Veri ve Ağ Güvenliği Ders Notları(içindekiler)

1 VERİ VE AĞ GÜVENLİĞİNE GİRİŞ(INTRODUCTION TO DATA AND NETWORK SECURITY)

Bilgisayarlaşmanın artmasıyla birlikte, dosyaları ve bilgisayarda saklanan diğer bilgileri korumak gerektiği açıktır. Özellikle, zaman-paylaşımlı ve halka açık iletişim sistemleri gibi paylaşılmış sistemlerde veri güvenliği daha da önemlidir. Veriyi korumak ve saldırganları engellemek için tasarlanmış olan sistem ve araçların genel adı Bilgisayar Güvenlik Sistemidir.

İkinci ana konu, dağıtık sistemler ve son kullanıcının terminali ile bilgisayar arasındaki veri taşıyan haberleşme olanaklarının güvenliğe etkileridir. Ağ güvenliği tedbirleri verinin iletimi sırasında onun korunmasını esas alır. Gerçekte ağ güvenliği kavramı, bütün iş yerleri, devlet ve akademik kuruluşlar veri işleme birimlerini birbirlerine iletişimi ağ ile bağladıkları için ortak bir ağ ortaya çıkar ki bunda birbirine bağlı ağlar adı verilir. Bu durumda koruma, ağ'daki bütün birimleri kapsar.

1.1 Bazı Güvenlik Tecavüzleri

• Kullanıcı A , Kullanıcı B' ye bir dosyayı transfer eder. Dosya, bozulmadan korumayı gerektiren hassas bilgileri(Ödeme bordrosu gibi) içermektedir. Dosyayı okumaya yetkili olmayan kullanıcı C, iletimi gözleyebilir ve iletim sırasında, dosyanın bir kopyasını alabilir.

• Bir ağ yöneticisi olan D, kendi yönetimindeki bilgisayar E' ye bir mesaj gönderir.Gönderilen mesaj, E' de bir grup kullanıcının bilgisayar erişim yetkilerinin güncellemesini içerir. Kullanıcı F, mesajı alıp,içeriğini değiştirerek, D'den geliyormuş gibi E' ye gönderir. E' de bu şekliyle kullanıcıların yetkilendirilmelerini günceller.

• Kullanıcı F, aldığı bir mesajı değiştirmek yerine kendi mesajını hazırlayarak sanki D'den geliyormuş gibi E' ye gönderir. E aldığı bu mesaja göre yetkilendirme dosyasını günceller.

• Farklı işlemler için ,müşteriden geliyormuş gibi borsa aracısına gönderilen bir mesaj ile para kaybı'na neden olunur ve müşterinin mesaj göndermesi engellenebilir.

1.2 Saldırılar servisler ve Mekanizmalar.

1. **Güvenlik saldırısı:** Bir kuruluşun bilgi güvenliği saygınlığını azaltır. Engelleme, Dinleme, Değiştirme ve yeniden oluşturma olarak 4 sınıf saldırı vardır.
2. **Güvenlik Mekanizması:** Bir güvenlik atağının anlaşılması, korunma veya onarımdır.
3. **Güvenlik Servisi:** Veri işleme sistemi ve kuruluşun bilgi iletim sisteminin güvenliğini artırma servisidir. Servis güvenlik saldırılarını engeller ve servis sağlamak için çeşitli güvenlik mekanizması kullanır.

Güvenlik Servis özellikleri aşağıda açıklanmıştır.

- **Gizlilik:** İletilen verinin pasif saldırılardan korunması. Diğer bir konu trafik akışının analiz edilmekten korunması. Bir saldırganın kaynak ve hedef arasında trafiği izlemesi önlenir.
- **Yetkilendirme**: Bu servis, haberleşmenin yetkili kişilerce yapılmasını sağlar. İkaz veya alarm gibi tek bir mesaj durumunda, yetkilendirme servisininin fonksiyonu, alıcıya mesajın kaynağı konusunda güven vermektir.
- **Bütünlük:** Mesajın bütünlüğünü sağlar. Mesajın tamamının değişmemesini temin eder.

- **İnkar edilememe**: Gönderici veya alıcının iletilen bir mesajı inkar etmemesini sağlar.
- **Erişim Denetimi:** Erişim denetimi ağ güvenliğinde, host sistemlere ve uygulamalara haberleşme bağlantıları ile erişimi sınırlandırır. Bu denetimi sağlamak için, her bir kişiye erişim hakkı verilmelidir.
- **Kullanıma hazırlık:** Saldırıların bir kısmı kullanılabilirliğin azalması veya kaybolmasına neden olabilir. Saldırıların bir kısamı iyi niyetli olabilir, oysa bir kısmı sistemin kullanılabilirliğini engeller. Bu servis kullanılabilirliğin sürekli olmasını sağlamaya yöneliktir.

Güvenlik mekanizmaları

Bilgi ve ağ güvenliğini sağlamak için birçok mekanizma mevcuttur. Bunlar kriptografik teknikler, şifreleme benzeri transformasyonlar sıkça kullanılan tekniklerdir.

Saldırılar

Bilgi sistemini saldırılardan korumak için saldırıları tanımak gerekir. Bu kapsamda tehdit(threat) ve saldırı(attack) termilerini kısaca açıklamak gerekir. **Tehdit**, belirli durum, yetenek, veya olay olduğu anlarda güvenlik foksiyonunun yerine getirilmesini engelleyen potansiyel bir güvenlik bozucusu olduğu halde; **saldırı**, sistemin güvenlik servislerini etkisiz hale getirmeyi amaçlayan akıllı bir tehditten üretilen ani bir hücumdur.
Bazı örnek saldırılar aşağıda verilmiştir.

Bilgilere yetkisiz erişimin elde edilmesi
Başka bir kullanıcının yetkilerini alarak onun yerine geçme
Saldırganın yasal lisansını genişletme
Saldırganın kendisini haberleşme yapan kullanıcıların arasına yerleştirmesi
Haberleşme hattının dinlenilmesi
Haberleşmenin engellenmesi
Saldırgan tarafından oluşturulan diğer bir kullanıcıya ait bilgilerin alındığını açıklamak
İletilen bilgilerin içeriğinin değiştirilmesi.

OSI Güvenlik Mimarisi

Bilgi güvenliğinde sistematik bir yaklaşım olarak X.800 OSI güvenlik mimarisi, yöneticilerin güvenlik oraganizasyonlarını düzenlemeleri için önemli bir yaklaşımdır. OSI yaklaşımı güvenlik servisleri, mekanizmalar ve saldırılara yoğunlaşmıştır.
Güvenlik Servisleri
Kimlik Doğrulama(Authentication)
Erişim Denetimi(Access Control)
Veri Gizliliği(Data Confideality)
Veri Bütünlüğü(Data Integrity)
İnkar edememe(Nonrepudation)

Güvenlik Mekanizmaları
X.800 OSI güvenlik mimarisinde mekanizmalar iki grupta toplanmıştır.,
Kendine özgü güvenlik mekanizmaları
Şifreleme, Sayısal imzalar, Erişim dentimi, Veri bütünlüğü, Kimlik doğrulama, Trafik analizini önleme, Yönlendirme denetimi ve noter makamı kullanılması

Kendine özgü olmayan güvenlik mekanizmaları
Güvenli fonksiyonellik, Güvenlik etiketi, Olay ortaya çıkartma, Güvenlik denetleme izleme, Güvenlik geri kazanımı

Güvenlik saldırıları

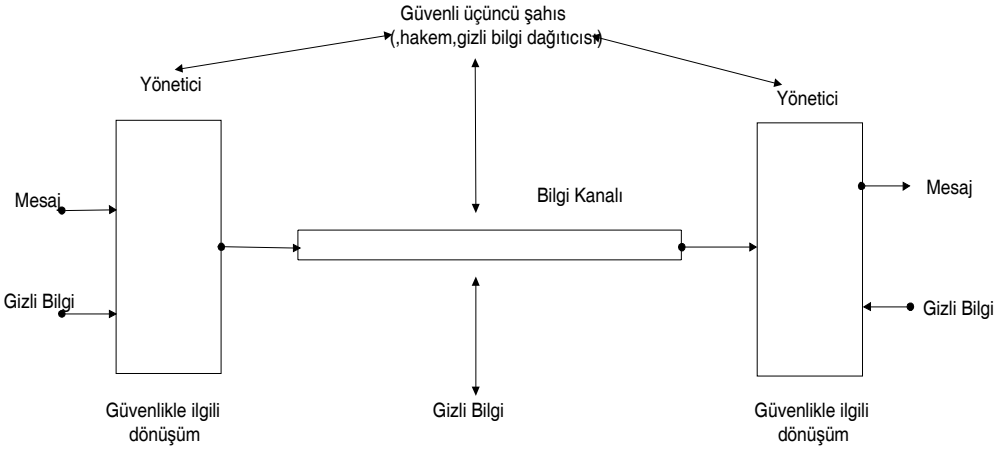
X.800 mimarisinde güvenlik saldırıları pasif ve aktif saldırılar olmak üzere iki türlüdür.
Pasif saldırılar, mesaj içeriğinin ifşa edilmesi ve trafik analizidir. Veri içeriği değiştirilmediği için pasif saldırıları ortaya çkartmak çok güçtür. Bu saldırılardan korunmak , anlamaktan daha uygun çözümlerdir.

Aktif Saldırılar, saldırganın kimliğini gizlemesi(masquarade), geri gönderme(replay), Mesajın değiştirilmesi(modification of message) ve servis durdurma(denial of service) dir.
Aktif saldırılar pasiflere göre zıt özelliktedirler. Aktif saldırılar tespit edilebilirler ve karşı önlem alınabilirler. Buna karşı aktif saldırıları tamamen önlemek çok zordur.

Ağ Güvenliği için bir model

Ağ güvenliğinde genel bir model şekil 1.1'de gösterilmiştir. Gönderici ve alıcı mesajları gizli olarak iletirken ,güvenli bir üçüncü şahıs gizli bilgilerin dağıtıcısı olarak hizmet vermekte, her iki taraf arasında noter görevi de görmektedir.
Bu genel güvenlik mimarisi, güvenlki servislerinin tasarımında dört temel işi gösterir.

1. Güvenlik ilişkili dönüşümler için bir algoritma tasarımı
2. Algoritma ile kullanılacak gizli bilginin üretimi
3. Gizli bilginin dağıtımı ve paylaşımı için yöntem geliştirme
4. Güvenlik algoritmasını ve güvenlik servisini sağlayacak gizli bilginin kullanımını sağlayacak bir protokol belirleme.



Şekil-1.1. Ağ Güvenliği için Model

2 GÜVENLİK GEREKLERİ VE KORUNACAK VARLIKLAR (Why Secure Your Network)

2.1 Giriş

Bilgisayar ağları, insanların bilgiye kolay ulaşımı, dolayısıyla çalışmalarındaki verimin artmasını sağlayan büyük bilgi ağlarıdır. Bilgiye kolay ulaşım için sunulan hizmetler (servisler, http, ftp, vs) aynı zamanda zarar verilebilme riski de taşımaktadır. Bilgisayar ağlarının sunduğu imkanlardan faydalanmak, fakat gelebilecek zararları en aza indirmek gerekir. Fakat bu tedbir birtakım şeylerden ödün vermemizi gerektirir. Güvenliği ön plana almak, hızı da aynı oranda azaltmak anlamına gelmektedir.

Alınabilecek güvenlik önlemlerini tartışmadan önce güvenlik konusunun neden gerekli olduğunun, nelerin korunması gerektiğinin anlaşılması daha faydalı olacaktır.

2.2 Korunacak varlıklar

Bir ağda güvenlik ile ilgili bir çalışma yapılmaya başlandığında ilk karar verilmesi gereken nelerin korunması gerektiğidir. Korunması gereken varlıklar üç ayrı ana başlıkta toplanabilir.

1. Veriler
2. Kaynaklar
3. Saygınlık

Bu varlıklar ayrı ayrı incelenecektir.

2.2.1 Veriler

Veriler, güvenlikle ilgili olarak üç özelliğe sahip olmalıdır;

- Gizlilik: Verilerin , başkaları tarafından öğrenilmesi istenmeyebilir.
- Bütünlük : Sahip olunan verilerin başkaları tarafından değiştirilmesi istenmeyebilir
- Kullanıma hazırlık: Verilerin istendiği zaman ulaşılabilir olup kullanıma hazır olması istenir.

Daha çok gizlilikle ilgili güvenlik üzerinde durulur. Gerçekten de bu konuda risk çoktur. Bir çok kişi ya da kuruluş için gizli bilgiler bilgisayar üzerinde tutulur. Bu bilgisayarların güvenliği de internet bağlantısı kopartılarak sağlanmaktadır. Bu şekilde bilginin gizliliği sağlanmış olabilir ama kolay ulaşılabilirlik ortadan kalkmış olur. Yani bir şekilde ağa bağlanılmalıdır. Bu durumda güvenlik politikaları belirlenerek, bilgilerin güvenliğinin sağlanması gerekmektedir.

2.2.2 Kaynaklar

Halka açık olan ağlara(İnternet'e) bağlanmakla riske atılacak ikinci şey, bilgisayar kaynaklarıdır. Başka insanların bir kuruluşa ait bilgisayardaki sabit diskte yer alan boş alanları kendi amacı için kullanmak istemesi her ne kadar mevcut verilere zarar vermeyecek bir şey olsa da istenecek bir durum değildir. Bunun gibi diğer kaynakların da (işlemci,bellek, ...) başkaları tarafından kullanılması, kabul edilebilir bir şey olamaz

2.2.3 Saygınlık

Her kişi ya da kurumun saygınlığının ağ üzerinde de korunması önemlidir. Meydana gelebilecek güvenlik problemleri kişi ve kurumların doğrudan aleyhine olup kötü reklamdır. ağ üzerinde

işlemler yapan bir kişinin, başka bir kişinin adını kullandığı düşünülürse, zarar verme durumunda doğrudan muhatap alınacak kişi saygınlığını kaybetme durumuyla karşı karşıya kalacaktır.

Genelde başka birinin hesabından girip sahte elektronik postalar atarak zarar verilir. Bunun sahte olduğunun kanıtlanması neredeyse imkansızdır. Böyle durumlarda, sahteciliği yapan kişinin kullandığı hesaba sahip kişi kadar kurum da zarar görür.

Halka açık ağlara(örn.internet) açılmayı düşünen kurumların eğitim ya da güvenlik politikası içinde, saygınlığın korunması için kişilere düşen güvenlik tedbirlerinin anlatılması gerekir. Ayrıca periyodik olarak takibinin yapılması şarttır.

2.3 Bilgisayar Ağına Saldırı

2.3.1 Giriş

Internet'in doğuşu ve gelişimi arasında aslında çok kısa bir zaman aralığı vardır. Bu kadar hızlı bir büyümenin olabileceği Internet'in doğuş yıllarında beklenmiyordu. Özellikle 1985 yılından sonra büyük yatırımlar yapıldı ve hızla yaygınlaştı. Ama bu hızlı gelişim birtakım konuların standartlarının tam olarak oluşturulmadan kullanıma geçirilmesinden dolayı bazı sorunları beraberinde getirdi. Özellikle de güvenlik sorunlarını ortaya çıkardı.

Güvenlik hemen her bilgisayar ağında öncelikli olarak düşünülmesi gereken bir konudur. Halka açık ağ(Internet) ortamında ise çok daha önemlidir. Birçok ticari firma ya da başka kuruluşlar ürünlerini ve hizmetlerini Internet ortamına aktarmak istemektedirler. Ancak bu birtakım risklerin de alınması gerektiği anlamına da gelir. Değişik güvenlik mekanizmalarının bir arada kullanılmasıyla bu riski azaltmak mümkündür.

2.3.2 Saldırganlar

Saldırgan (Hacker), ağ üzerindeki genelde bazı servisler veren makinalara hiçbir hakkı olmadan erişip zarar veren kişidir. Bilgi hırsızı olarak da tarif edilebilir. Fakat ev ya da banka soyguncularından çok farklıdırlar. İyi görünümlü, sistemler hakkında çok bilgisi olan insanlardır. Genellikle sistemin bilinen açıklıklarından ve sistem yöneticisinin bilgisizliğinden faydalanırlar.

İstatistiki raporlara göre saldırıların çoğunun firma içerisinden yapıldığı tespit edilmiştir. İçeriden gelen saldırı, sistem sadece dışarıya karşı korunmalı durumda ise çok zarar verebilir.

Saldırganların büyük firmaların ağına girdikleri ve büyük ölçekte sitemlere zarar verdikleri bilinmektedir. Bunu genellikle eğlence, kendini göstermek ya da sisteme zarar vermek için yaparlar.

Saldırganlar iki genel türde toplanabilir:

1. Kötü niyetli saldırganlar
2. Kötü niyetli olmayan saldırganlar

2.3.2.1 Kötü niyetli saldırganlar (Malicious hacker)

Sisteme gerçekten zarar vermek amacıyla girerler. Açığını buldukları sistemlere verebilecekleri en büyük zararı vermeyi amaçlarlar. Bu tür saldırganlar genelde ekip halinde çalışırlar. Kredi kartları kullanan sitelerden kart numaralarını ve parolalarını alıp kişi ve şirketlere büyük zararlar verebilirler.

Tablo2-1'de belirtilen bilgisayar korsanları, casuslar,teröristler ve profesyonel suçlular bu gruba girmektedir.

2.3.2.2 Kötü niyetli olmayan saldırganlar

Sistemlere genellikle eğlenmek için saldırıda bulunurlar. Çok fazla zararlı olmayan tiplerdir. Hatta sistem yöneticisi eksikliklerini ve sistemin zayıf noktalarını bu sayede görebilir. Bu tür saldırganlar, bir saldırgan grubuna üye değildir. Genellikle yaptıkları, kendilerine daha sonra kullanmak için hesap açmak ve sistemin zayıf gördüğü yerleri belirten notlar koymaktır. Bu işi zevk için yapan insanları bu kategoriye sokabiliriz. Bu gruba girenler aşağıdaki tabloda meraklılar olarak belirtilmiştir.

Saldırgan, kullandığı araçlar, sisteme erişim yolları ve amaçlarının ne olabilecekleri tablo 2-1'de özetlenmiştir.

Saldırganlar	Araçlar	Erişim	Sonuç	Amaç
Bilgisayar korsanları	Kullanıcı komutları	Gerçekleme zayıflıkları	Bilgi bozma	Finansal kazanç
Casuslar	Komut dosyası veya Program	Tasarım zayıflıkları	Bilgi çalma ya da açığa bilgi çıkartma	Politik kazanç
Teröristler	Araç takımı	Yapılandırma zayıflıkları	Hizmet çalma	Sosyal statüye meydan okuma
Meraklılar	Dağıtık araçlar	İzinsiz erişim	Hizmet önleme	Zevk için
Profesyonel suçlular	Veri dinleyici sistemler			

Tablo 2-1 Saldırganlar ve amaçları

2.3.3 Saldırı Türleri

Bu bölümde son yıllarda internette kullanılan saldırı yöntemlerine değinilecek ve sınıflandırılmaya çalışılacaktır. Saldırıların tanımları yapılacak ve sisteme verebileceği zararlar üzerinde durulacaktır. Saldırıya karşı alınabilecek önlemler güvenlik duvarı olmaksızın anlatılacak ve güvenlik duvarı düzeyinde yapılabilecekler açıklanacaktır.

Saldırganlar sisteme ağ üzerinden ulaşabilecekleri için, ağa bağlı cihazlar her zaman saldırıya açık durumdadır. Burada yapacakları, hedef makinaya ulaşmak, yazılım ve donanıma zarar vermek şeklinde olabilir. Şirkete ait veritabanına ulaşıp verilere erişebilir, değiştirebilir ya da silebilirler. Burada asıl olan, saldırganın ne yapmak istediğidir. İşine yarayan kayıtları, dosyaları alabilir ve sisteme (yazılım, donanım) zarar verebilir. Verilen hizmetleri servis dışı bırakabilir. Sadece Internet bağlantısına zarar verebilir. Truva atı türünde programları bir şekilde hedef makinaya yükleyerek kullanıcıyı takip edebilir.

2.3.3.1 Saldırıların Sınıflandırılması

Bilgisayar ve ağ saldırıları için değişik sınıflandırmalar yapılmıştır. Aşağıda süreçsel ve işlemsel sınıflandırmalar anlatılacaktır.

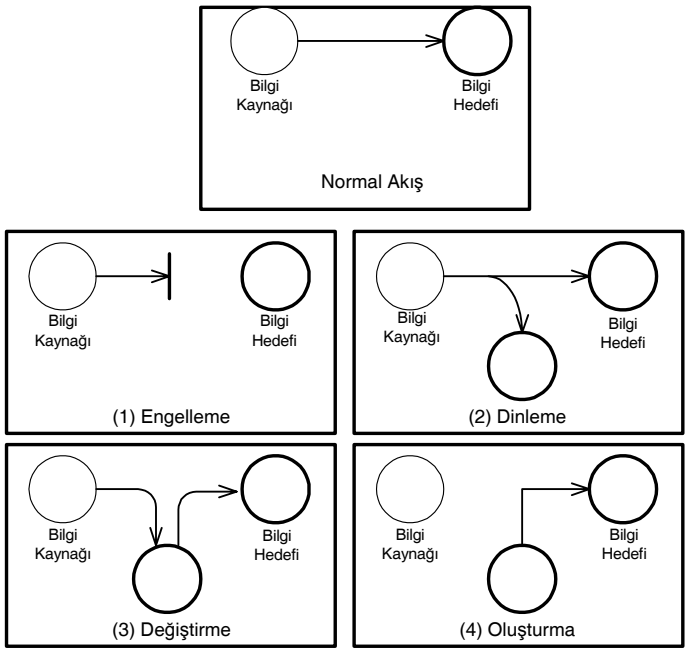
2.3.3.1.1 Süreçsel Sınıflandırma

Internet'te gerçekleştirilen veri transferiyle ilgili güvenlik sorunları dört kategoriye sokulabilir.

1. **Engelleme:** Sistemin bir kaynağı yok edilir veya kullanılamaz hale getirilir. Donanımın bir kısmının bozulması iletişim hattının kesilmesi, veya dosya yönetim sisteminin kapatılması gibi.

2. **Dinleme:** İzin verilmemiş bir taraf bir kaynağa erişim elde eder. Yetkisiz taraf, bir şahıs, bir program veya bir bilgisayar olabilir.Ağdaki veriyi veya dosyaların kopyasını alabilir
3. **Değiştirme:** İzin verilmemiş bir taraf bir kaynağa erişmenin yanı sıra üzerinde değişiklik de yapar. Bir veri dosyasının değiştirilmesi, farklı işlem yapmak üzere bir programın değiştirilmesi ve ağ üzerinde iletilen bir mesaj içeriğinin değiştirilmesi gibi.
4. **Oluşturma:** İzin verilmemiş bir taraf, sisteme yeni nesneler ekler. Ağ üzerine sahte mesaj yollanması veya bir dosyaya ilave kayıtlar eklenmesi.

Burada dinleme pasif bir saldırı türüdür. Engelleme, değiştirme ve oluşturma ise etkin bir saldırı türü olarak görülmektedir.



Şekil 2-1 Süreçsel Sınıflandırma

2.3.4 İşlemsel Sınıflandırma

Genel anlamda bir saldırı yöntemler, kullanılan yollar ve sonuçları açısından düşünülebilir. Bilgisayar ya da bilgisayar ağına saldıran kişi, istediği sonuçlara çeşitli adımlardan geçerek ulaşmak zorundadır. Bu adımlar aşağıdaki şekil 2-2 den de görüldüğü gibi araçlar,erişim ve sonuçlar şeklindedir.

Şekil 2-2 İşlemsel Sınıflandırma

2.3.5 Saldırıların Gruplandırılması

Saldırıları değişik açılardan değerlendirerek, değişik gruplamalar yapmak mümkündür. Saldırıda kullanılan yöntem, saldırının kullandığı yöntem, saldırının amaçladığı uygulamalar ve saldırı sonucunda oluşan zararlar gruplama için kullanılabilecek yöntemlerdir.

2.3.5.1 CERT Gruplandırması

(Computer Emergency Responce Team) tarafından yapılmış olan saldırı türleri ve açıklamaları tablo2-2'de listelenmiştir.

Probe,Scan,Scam	Bir sistemdeki açık ve kullanılan portların taranması ve bu portlardan hizmetlere yönelik saldırıları türüdür.
Prank	Kullanıcı hesaplarının yanlış oluşturulması sonucu oluşan açıklardan yapılan saldırı türleridir.
Email spoofing	Başka bir kullanıcı adına e-posta gönderilmesi...
Email bombardment	Bir e-posta adresine genelde farklı adresten çok sayıda e-posta gönderilmesi
Sendmail attack	Smtp portuna yönelik saldırılardır...
Break-in	Verilen hizmetlerin devre dışı bırakılmasına yönelik saldırı türüdür.
Intruder gained root access	Saldırganın normal kullanıcı olarak girdiği sistemde süper kullanıcı yetkisini kazanması.
Intruder installed trojan horse program	Saldırganın girdiği sisteme genelde daha sonra tekrar rahat girebilmesi ya da uzaktan yönetim için ajan program yerleştirimesi.
Intruder installed packed sniffer	Saldırgan tarafından hedef makinaya yönelik paket dinleyici yerleştirilerek yapılan saldırı türüdür. Bu şekilde bir yerel ağ korumasız bir konak üzerinden saldırılara açık hale gelebilir.
NIS attack	Ağ kullanıcı yönetim sistemine yönelik saldırı türüdür.
NFS attack	Ağ dosya yapısına yönelik saldırı türüdür. Genellikle ağ erişimini devre dışı bırakmada kullanılır.
Telnet attack	Uzaktan erişim protokolünün açıklarından faydalanılarak yapılan saldırı türüdür.
Rlogin or rsh attack	Uzaktan erişimde kullanılan servislerin açıklarına yönelik yapılan saldırı türüdür.
Cracked password	Kolay tahmin edilebilir parolaların tahmini ya da şifreli hallerine göre sözlük saldırısı yapma türüdür.
Anoymous FTP abuse	Anonim erişim izni verilen dosya aktarım sunucularına yönelik saldırılardır.
IP spoofing	IP adres yanıltmasıyla yapılan saldırı türüdür.
Configuration error	Çok kullanılan programdaki kullanıcılardan kaynaklanan konfigürasyon hatalarından doğan açıklıklardır.
Misuse of hosts resources	Konak kaynaklarının yanlış kullanımı sonucu ortaya çıkan açıklıklar.
Worm,Virus	Konaklarda kullanıcılardan habersiz çalışan zararlı programlar.

Tablo 2-2: Saldırı türleri

Yukarıda da belirtildiği gibi değişik gruplamalara gitmek mümkündür. Bazı saldırıları sadece bir gruba koymak mümkün değildir.

www.cert.org adresinde bu gruplandırılmış saldırıların ne kadar süredir var olduğu, ne tür zararlara yol açtığı ve yaygınlığı gibi bilgiler bulunmaktadır.

2.3.5.2 İletişim Protokollerini Kullanan Saldırılar

IP sahteciliği (IP spoofing)
TCP dizi numarası saldırısı (TCP sequence number attack)
ICMP atakları
Ölümcül ping
TCP SYN seli atağı (TCP SYN Flood Attack)
IP parçalama saldırısı (IP Fragmentation Attack)
Internet yönlendirme saldırısı (Internet Routing Attacks)
UDP sahteciliği ve Dinleme (UDP Spoofing and Sniffing)
UDP portunu servis dışı bırakma saldırısı (UDP Port Denial-of-Service Attack)
Rasgele port taraması (Random port scanning)
ARP saldırıları (ARP Attacks)
Ortadaki adam saldırıları

2.3.5.3 IP saldırıları

IPV4'te bulunan güvenlik eksikliklerinden faydalanılarak yapılan atak türleridir. Bazı örnekleri şunlardır: Out of Band Nuke, Land, Teardrop, Boink, Nestea, Brkill, ICMP Nuke, Jolt/Ssping, Smurf, Suffer3

Bu saldırılardan bir kısmı detaylı olarak anlatılacaktır.

2.3.5.4 İşletim sistemine özel saldırılar

Exploit olarak isimlendirilen bu saldırılar, sistem tabanlı olarak çalışırlar. Yani Unix için yapılan bir exploit MS Windows için çalışmaz.

Windows Null Session Exploit
PHF Exploit
ASP Exploit
Sendmail Exploit

2.3.5.5 Uygulama Katmanı Saldırıları

DNS,SMTP,MIME,NFS,NTP saldırıları
Uzaktan giriş ile saldırılar (Hacking and Remote Login)
Bilgi sızdıran saldırılar
URL sahteciliği (URL Spoofing)
CGI saldırıları
X-Windows sistem saldırıları
Kötü niyetli java ve AktiveX uygulamacıkları
Sistem log seli
Program ve ağ üstündeki virüsler

Sistem log seli güvenlik duvarına çok sayıda giriş yapılarak log dosyasının dolmasına ve sonuç olarak sistemin kapanmasına neden olan saldırı türüdür.

2.3.6 Bazı Saldırı Yöntemleri

Artık klasik hale gelmiş ve genelde iletişim protokollerinin deliklerinden yararlanılarak yapılan saldırılar anlatılacaktır.

2.3.6.1 IP Aldatması (IP Spoofing)

Aldatma saldırısının genelde yapılan türü IP aldatmasıdır. Sahtecilik olarak çevirmek mümkündür. IP paketlerinin kaynak IP' sini değiştirmekle sağlanmaktadır. Böylece paketi alan hostun, paketin geldiği kaynak adresini bilmesini engellenmiş olur. Host gelen paketin saldırgandan değil de kullanıcıdan geldiğini sanır.

IP adreslerine göre çalışan servisler üzerinde oldukça etkilidir. Sahte paketler üretme (fabrication) bu şekilde yapılabilmektedir.

Internet'e bağlanan bilgisayarlar birbirleriyle IP adreslerini kullanarak haberleşmektedir. IP paketleri üretildiği bilgisayardan hedef bilgisayara IP adreslerini kullanarak giderler. İletişimde bulunulan bilgisayarın IP numarasının bilinmesi güvenlik açısından oldukça önemlidir. İnternet'te servis veren bazı bilgisayarlar sadece belirli IP adreslerine hizmet verirler. Güvenlik duvarlarının kullandığı paket filtreleme mekanizması genelde bu adresler üzerinde yapılır. Paket filtreleme örneğinde de anlatıldığı gibi bazı IP adreslerine ait paketlerinin geçişine izin verilir ya da reddedilir.

Ayrıca güvenlik duvarı kullanılarak, bazı IP adreslerine verilecek hizmetlerin sınırlandırması da sağlanabilir. Gelen isteğin kaynak IP adresine bakılarak böyle bir işlem yapılır. Bunun anlamı kullanıcıya IP adresine göre yetki vermektir. IP adresine bakılarak yetki verilmesi çalışmaları rahatlatacaktır; fakat güvenlik açısından bazı riskler taşımaktadır.

Kaynak IP adresine göre yüksek yetki verilen bir kullanıcıya ait adres bilinmesi durumunda risk ortaya çıkmış olur. Saldırgan kaynak IP adresini değiştirmek suretiyle hakkı olmayan bir yetkiyle sisteme girebilir.

Saldırganın sahte IP paketleri kullanarak sisteme girmesi durumunda verebileceği zarar, IP adresine verilen yetkiyle orantılıdır. Bu şekilde yetkili kullanıcı olarak sisteme girebilen bir saldırgan sisteme çok kolay ve oldukça fazla zarar verebilir.

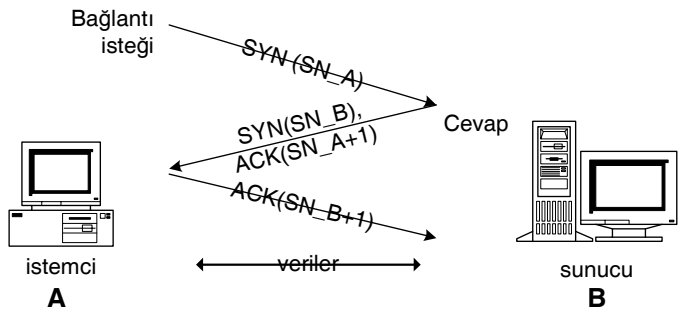
Böyle bir saldırıya karşı alınabilecek önlem yoktur. Ancak Kaynak IP yanında Hedef IP ve MAC adresine de bakılarak saldırı olduğuna karar verilebilir. Bunu iç ağın Internet'e açıldığı noktaya güvenlik duvarı kurmakla sağlamak mümkündür.

2.3.6.2 TCP SYN paketi akışı saldırıları

IP adresi kullanılarak gerçekleştirilen bir saldırı türüdür. Genelde TCP/IP servislerinin devre dışı bırakmak için kullanılır.

TCP bağlantı temelli bir protokoldür. Birbiriyle iletişim kuran iki bilgisayar, paketlerini kurulu bir hat üzerinden aktarırlar. Bunun için de iletişim başlangıç aşamasında bu hattın kurulması gerekir. Bu da bazı el sıkışma kurallarıyla mümkün olmaktadır. TCP protokolünün el sıkışma sistemi üç yollu el sıkışma (three way handshake) mekanizmasıdır. Üç yol denmesi, bu işlemin üç aşamada gerçekleşmesinden dolayıdır.

İlk olarak, bir sunucu bilgisayardan servis isteyecek diğer bilgisayar (istemci), bağlantı kurmak istediğini göstermek için SYN bayrağı kalkık(set) paketini, sunucu bilgisayara gönderir. Bu paketi alan sunucu SYN paketi aldığını ve bağlantı isteğini onayladığını yine SYN bayrağı kaldırılmış(set) paketi (SYN-ACK paketi) istemci bilgisayara gönderir. Üçüncü aşamada ise sunucu bilgisayarın gönderdiği SYN-ACK paketini alan istemci bilgisayar sunucuya bu paketi aldığını bildiren bir paket gönderir(ACK).



Şekil 2-3 TCP el sıkışma mekanizması

Bu mekanizmada saldırıya açık nokta, bir bilgisayarın istemci olarak bir bilgisayara el sıkışma mekanizmasını başlatacak SYN paketini göndermesi, buna karşılık sunucu bilgisayardan SYN-ACK paketini aldıktan sonra son paketi (ACK) göndermemesi ile oluşur. Böyle bir durumda sunucu tarafında açılmış fakat tamamlanmamış bir bağlantı isteği oluşacaktır. Bu bağlantı isteği uzun bir süre dolumuna kadar açık tutulacaktır. Bu tür bağlantılara yarı açık bağlantılar denir. Bu mekanizmanın kötüye kullanılabilecek noktası, arka arkaya belirtilen bu işlemlerin yapılmasıyla ortaya çıkar. Böyle bir durumda yarı açık birçok bağlantı oluşacaktır.

Herhangi bir hizmet bir port üzerinden verilmektedir. Buraya gelen istekler bir kuyruğa alınır ve istemciden üç yollu bağlantıdaki son paket gelene kadar kuyrukta tutulur. Dolayısıyla kuyruktaki tamamlanmayan bağlantı isteklerinin artması kuyruğun dolmasına sebep olacaktır. Kuyruk dolduğunda ise yeni gelen bağlantı isteklerine cevap veremeyecektir. Dolayısıyla servis kilitlenecektir. Bazı sistemlerde bellek taşmasına sebep olacağından bu durum sunucu bilgisayarı devre dışı da bırakabilir.

Bu saldırıyı önlemek için TCP protokolü üzerinde açıklıklarını kapatacak değişiklikler yapılmaktadır. Bu değişiklikler paket filtreleme düzeyinin üstünde TCP protokolü düzeyinde yapılmaktadır.

2.3.6.3 TCP sıra numarası tahmini yoluyla gerçekleştirilen saldırılar

Daha önce IP adresi yoluyla yanıltma yöntemi anlatılırken, IP adresine göre yetkilendirme yapan servislere karşı bu yöntemin kullanılması durumunda sistemin saldırıya karşı olduğundan bahsedilmişti. IP adresi yoluyla yanıltma tekniğinin birlikte kullanıldığı yöntemlerden biri TCP sıra numarası tahmini yoluyla yapılan saldırıdır. Bu TCP/IP protokolünün açıklıklarından olarak kabul edilir. IP adresine göre yetkilendirme yapan programlara saldırılarda bu yöntem kullanılır.
Bu saldırıyı anlamak için TCP protokolündeki üç yollu el sıkışma mekanizmasını detaylı incelemek gerekmektedir. TCP protokolü daha öncede bahsedildiği gibi bağlantı temelli bir protokoldür. Bunun anlamı bir oturuma ilişkin IP paketlerinin aktarılması sırasında verilen güvendir. Hedef uca uygun sırada ulaşmamaları durumunda, düzenlenmesi ve aradan paketlerin gelmemesi durumunda da tekrar o paketin istenmesi TCP katmanında yapılmaktadır. Bunları gerçekleştirmek için bazı mekanizmalar kullanılır. TCP sıra numarası (TCP sequence number), gönderilen paketlerin oturum içindeki sırasını gösterir. Bu değer kullanılarak doğru sırada alınmamış paketlerin sıraya konulması ve en son alınan pakete ilişkin bilgilendirme karşı tarafa yapılmaktadır. Bu sayede paketin hedefe ulaştığından emin olunması sağlanmış olur; aksi durumda paketin tekrar gönderilmesi işlemi yapılır.

Saldırıya açık kısmı ise, TCP üç yollu bağlantı şekli üzerinden açıklayalım. İstemci bilgisayar sunucu bilgisayara istekte bulunacağını bir SYN paketi göndererek ifade etmektedir. Bu pakette J

ile gösterilen, istemci bilgisayarın gönderdiği bilgilere verdiği sıra numarası bilgisidir. Bu paketi alan sunucu bilgisayar cevap olarak SYN-ACK paketi göndermektedir. Bu pakette de, K ile gösterilen,sunucu bilgisayarın gönderdiği pakete verdiği sıra numarası vardır. SYN(K) ile gösterebileceğimiz bu bilgiyle birlikte, haberleşmenin senkronize bir şekilde devam etmesini sağlamak üzere istemci tarafından gönderilen ve J sıra numarasını taşıyan paketin alındığına ilişkin bilgilendirmenin de yapılması gerekir. Bu amaçla da ACK(J+1) ile gösterebileceğimiz ve en son alınmış olan pakete ilişkin sıra numarası bilgisi de ACK olarak istemci bilgisayara gönderilir. Bu paketi alan istemci bilgisayar da, sunucunun göndermiş olduğu son paketi aldığını göstermek üzere ACK(K+1) paketini sunucuya göndererek, bağlantının kurulması işlemini tamamlar. Bağlantının kurulabilmesi ve daha sonra da devam edebilmesi için bu bilgilendirme ACK paketlerinin karşılıklı olarak aktarılması şarttır.

Saldırı yöntemi aşağıdaki örnekle açıklanmıştır

A,B ve C bilgisayarlarından oluşan bir sistem olsun. A bilgisayarının IP adresi yoluyla aldatma yöntemini kullanmak suretiyle kendisini C bilgisayarındaymış gibi göstererek, sunucu olan B bilgisayarına bağlanmaya çalıştığını düşünelim ve üç yollu el sıkışma mekanizmasında gerçekleşecekleri inceleyelim;

A bilgisayarı ilk SYN paketini gönderme konusunda bir zorluk yaşamayacaktır. Bu pakete kendi sıra numarasını (SN_A) ekleyerek ve C bilgisayarından geliyormuş gibi göstermek üzere 'kaynak adres' kısmını değiştirerek B bilgisayarına gönderecektir. Bu paketi alan B sunucu bilgisayarı, SYN(SN_B) ACK (SN_A+1) bilgilerini taşıyan paketi, kendisiyle haberleşmek istediğini düşündüğü C bilgisayarına gönderecektir. Üç yollu el sıkışma mekanizmasının tamamlanabilmesi için son paket olan ACK(SN_B+1) paketinin B bilgisayarına gönderilmesi gerekir. Oysa SN_B paket numarası bilgisini içeren paket, üç yollu el sıkışma mekanizmasını başlatan ve kendisini C bilgisayarı gibi gösteren A bilgisayarına değil de C bilgisayarına gönderilmiştir. Dolayısıyla A bilgisayarının kendisi kendisini C bilgisayarı gibi gösteren B sunucusuna bağlantıyı tamamlayabilmesi için, SN_B değerini belirlemesi ve ACK (SN_B+1) paketini yine C bilgisayarından geliyormuş gibi göstererek B bilgisayarına göndermesi gerekmektedir. Bunu başarabildiği anda üç yollu el sıkışma mekanizması tamamlanacak ve B sunucu bilgisayarı C bilgisayarı ile haberleştiğini düşünecektir.

Eğer bu saldırı, IP adresi ile yetkilendirme yapan bir servise yapılıyorsa, B sunucusunun C' ye güvendiği ve ona verdiği yetki oranında, A bilgisayarı B üzerinde işlemler yapacaktır.

A bilgisayarının B sunucusuna C bilgisayarıymış gibi bağlanma senaryosu tablo2-3'de özetlenmiştir;

Paket Üretici	Kaynak Adres	Hedef Adres	Paket
A	C	B	SYN(SN_A)
B	B	C	SYN(SN_B), ACK(SN_A+1)
A	C	B	ACK(SN_B+1)

Tablo 2-3 TCP el sıkışma mekanizması

Bundan sonra karşılıklı bilgi akışı başlar.

Görüldüğü gibi saldırının en kritik noktası, A bilgisayarının SN_B' yi belirlemesidir. Eğer A bu değeri doğru olarak belirleyebilirse, saldırıya başlangıç için büyük oranda başarılı olmuş demektir. Sıra numarası bilgisinin ne şekilde verildiğini incelememiz, bu konuya da açıklık getirecektir. Bir bağlantıda kullanılacak sıra numarası bilgisi için bir başlangıç değeri belirlenir; daha sonradan da her veri aktarımında bu değer, aktarılan veri miktarı kadar arttırılır. Başlangıç değeri belirlenirken de, bu işlem için kullanılan, 32 bitlik sayıcıdaki değer kullanılır. Bu değer belli aralıklar ve durumlarda arttırılarak düzenli bir çalışmanın yapılması garanti edilmeye çalışılır. Her saniye için belli bir sayı ve her gerçekleşen bağlantı içinde bir başka sayı sayıcıya eklenir.

Acaba böyle düzenlenen bir sayıcıdaki değerin, dolayısıyla gerçekleşecek yeni bir bağlantıya verilecek sıra numarasının (senaryoda SN_B idi), başka bilgisayarlarca (örnekte A) belirlenebilmesi, sayıcının düzenlenmesindeki algoritmanın ne kadar iyi olduğuna bağlıdır. Bu algoritmayla sıra numarasının tahmini kolaylaşmaktadır. Bunu yapacak saldırgan, hedef bilgisayara önce normal bir bağlantı gerçekleştirecek, hedef bilgisayardaki sıra numarası sayıcısının o andaki değerini belirleyecektir. Sonrasında da, sayıcının artış algoritmasını, hedef bilgisayarla aradaki mesafeyi ve diğer bazı unsurları göz önüne alarak, bir süre sonra kullanılacak sıra numarasını tahmin edebilecektir.

Bu tahminler yapılabildiği takdirde saldırı için gerekli zemin hazırlanmış demektir. Hedef bilgisayara güvenilir bir bilgisayar gibi ulaşılmış demektir.

Burada dikkat edilmesi gereken bir nokta daha vardır. Bağlantı kurulumu aşamasında B sunucu bilgisayarının, C bilgisayarına SYN (SN_B) ACK(SN_A+1) paketlerini göndermesi durumunda nelerin olacağının da göz önüne alınması gerekir. Böyle bir durumda, paketi C bilgisayarı algılarsa bağlantı isteğinde bulunmadığını gösteren RST paketini B bilgisayarına gönderecektir. Bu durumda B sunucu bilgisayarı üç yollu bağlantı işlemini kesecektir. Bu nedenle A bilgisayarındaki saldırgan ya C bilgisayarının devrede olmadığı bir anı gözleyecek ya da B bilgisayarının göndermiş olduğu paketin, C bilgisayarı üzerinden gideceği servise ilişkin portun SYN kuyruğunu doldurarak, bu paketin C bilgisayarı tarafından alınamamasını sağlayacaktır. Dolayısıyla C bilgisayarı cevap vermeyecektir.

Saldırıya ilişkin en kritik nokta, sıra numarasının tahmin edilebilir olmasıdır. Bu sayının tahmin edilemez hale getirilmesi durumunda saldırılar önlenecektir. Bunun için de sıra numarasını belirleyen sayıcının algoritmanın güçlendirilmesi gerekir.

2.3.6.4 IP Servis Durdurma Saldırısı (smurf)

Yanlış kaynak adresi bilgisiyle oluşturulmuş ICMP 'echo request" paketleri kullanılarak gerçekleştirilen, çoğu durumda hedef bilgisayarın kilitlenmesine sebep olan, ayrıca saldırıda hedef olarak kullanılan ağlarda önemli derecede performans sorunları yaratabilen bir saldırıdır. "smurf" adının verilmiş olması, saldırganların bu işlevleri yapan programlardan birisinin smurf olmasından dolayıdır.

Saldırı iki işlemden oluşmaktadır. Hedef alınan bilgisayarın IP adresinin "kaynak adres" olarak kullandığı sahte ICMP "echo request" paketlerinin hazırlanması ve bu paketlerin herkese yayınlanacak (broadcast) şekilde tüm bilgisayarlara yönlendirmesinin sağlanmasıdır.

ICMP (Internet Control Mesaj Protocol), ağ üzerindeki hataların belirlenmesi, bazı kontrol bilgilerinin karşılıklı değiştirilmesi, ağın belli açılardan gözetlenmesi imkanlarını sağlayan hizmetler verir. Bunlardan biri de, bir cihazın o anda açık olup olmadığını, belli fonksiyonları yerine getirip getirmediğini belirlemekte kullanılan hizmettir. ICMP bu işlemi gerçekleştirmek

için, denetlenmek istenen cihaza “echo request” paketi gönderir. Bunu alan cihaz ise, “echo reply” paketi ile, ağ üzerinde faal bir şekilde bulunduğunu bildirir. Bu sayede cihazların ulaşılabilir olup olmadığını, bu yolla da eğer bir sorun yaşanıyorsa sorunun nereden kaynaklandığını belirlemek mümkün olabilmektedir. Bu mekanizma çoğu işletim sistemi tarafından, genellikle de “ping” adı altında gerçeklenmektedir.

Saldırının ikinci unsurunu ICMP paketlerinin, bir ağın herkese yayın (broadcast) IP adresine yönlendirilmesi sonucu oluşturur. Bilindiği gibi çoğu durumda hazırlanan IP paketlerin “hedef adres” kısmında, paketin ulaşması gereken bilgisayarın IP adresi bulunur. Eğer hedef IP adres kısmında herkese yayın adresi varsa, bu paket tüm bilgisayarlara yöneltilecek demektir. Herkese yayın adresleri, IP adresinin konak kısımlarına ilişkin bitlerin tamamının ‘1’ olduğu adrestir. Örneğin C sınıfı bir IP adresi ağı için ağ IP adresi : 193.140.76.0 ise herkese yayın adresi : 193.140.76.255 olacaktır.

Saldırgan kendisine hedef olarak seçtiği cihazın IP adresini ‘kaynak adres’ kısmına yerleştirdiği ICMP ‘echo request’ paketlerini, yine ara hedef olarak seçtiği ve saldırısında basamak olarak kullanacağı ağın herkese yayın adresine gönderir. Böyle bir saldırıda saldırgan, ara hedef ve hedef olmak üzere üç nokta vardır. Şimdi belirtilen özellikteki paketlerin saldırgan tarafından üretilerek gönderilmesi durumunda olabilecek sonuçları inceleyelim.

Bilindiği üzere bu paketlerin ‘hedef adres’ kısmında, ara hedef ağın herkese yayın adresi bulunmaktadır. Dolayısıyla, eğer yol üzerinde veya ara hedef ağın internete açılan yüzünde bulunan yönlendiricide bu paketlerin filtrelenmesi yönünde bir çalışma yapılmamışsa, saldırgan tarafından üretilen paket, ara hedef olan ağa ulaşacaktır. Paket herkese yayın adresini taşıdığından, ağ üzerinde yer alan ve açık olan bütün bilgisayarlar tarafından alınacaktır. ICMP ‘echo request’ paketi olduğundan, paketin kaynak adres kısmında yer alan bilgisayara (hedef bilgisayar) ara hedef ağ üzerinde yer alan her bilgisayar ICMP ‘echo reply’ paketi gönderecektir. Bu paketler de ara hedef ağ trafiği üzerinde etkili olacak, performansı kötüleştirecektir. Saldırganın kullandığı paket boyu, gönderilme süresi ve ağda bulunan aktif bilgisayar sayısı arttıkça performans düşüşü daha fazla olacaktır.

Aslında asıl amaç ağa değil de hedef bilgisayara zarar vermektir. Bu da ağda yer alan bütün bilgisayarların ICMP ‘echo reply’ paketlerini hedef bilgisayara yöneltmekle gerçekleşmiş olur. Yoğun paket bombardımanına tutulan bilgisayar kilitlenir hatta yerel ağda da problemler çıkar. Saldırganlar bu yüzden birden fazla ara ağ kullanmaya çalışırlar.
Bu saldırı biçimi herkese yayın IP trafiğinin filtrelenmesi ve bilgisayarların herkese yayın IP kaynak adresli ICMP paketlerine cevap vermesinin engellenmesi yöntemleriyle engellenebilir.

2.3.6.5 UDP Portlarından Saldırı

Smurf saldırılarının benzeri olan, ICMP paketleri yerine UDP paketlerinin kullanıldığı saldırı türüdür. Bir bilgisayar üzerinde veya birkaç bilgisayar arasında, gerçek UDP portlarına yöneltilecek yoğun paket akışıyla gerçekleştirilen bu saldırılar, tek bir bilgisayar üzerinde gerçekleştiriliyorken bu bilgisayarın performansının düşmesine, birden fazla bilgisayar arasında gerçekleştiriliyorken ise,ağın performansının düşmesine sebep olacaktır.

Birbiriyle haberleşmekte olan iki UDP servisinden birisi veya her ikisi, üreteceği yoğun paket akışıyla,karşısındaki bilgisayarın servisini kilitlemeyi, bilgisayarın performansını kötüleştirmeyi başarabilir. UDP servisleri bağlantı temelli olmadıklarından, herhangi bir el sıkışma mekanizması ya da bazı kontrol bilgilerinin karşılıklı değiştirilmesi gerekmediğinden, bu tür saldırılara açıktır.

Örnekle açıklayalım;
7 numaralı portu kullanan UDP echo servisi, karşısındaki bilgisayardan (istemci) aldığı bilgileri olduğu gibi geri gönderir. 19 numaralı port üzerinden servis veren UDP 'chargen' servisi ise, istemci bilgisayardan her paket alışında, rasgele sayıdaki verilerden oluşan paketi geri gönderir. Bu iki servise ilişkin UDP portlarının aynı bilgisayar üzerinde veya değişik bilgisayarlar arasında birbirine bağlanması, sonsuz bir trafiğin oluşmasına sebep olacaktır. Bu hem servisi veren bilgisayarı hem de trafiğin aktığı ağı etkileyecektir.

Böyle bir saldırı sonucunda doğabilecek sonuçları şunlardır:
Saldırının yöneltildiği servisler kilitlenebilir. Bu servisleri veren bilgisayarların performansı düşebilir ve servisleri veren bilgisayarların bulunduğu ağın trafiğini arttırır.

Bu saldırı tipinden korunmak için alınabilecek önlemlerin başında saldırıda kullanılan servislerin bilgisayarların üzerinden kaldırmak gelir. Bu servislere ilişkin paketlerin güvenlik duvarı üzerinden filtrelenmesini sağlamaktır. Tabii bu yaklaşım kullanılıyorken, iptal edilecek servislerin ne kadar gerekli olduğu da önemlidir. Bazı servislerden vazgeçilmesi zordur (Örneğin UDP kullan DNS servisleri). Böyle bir durumda iyi hazırlanmış paket filtreleme kuralları ile, sadece belli bilgisayarların bu servislerden yararlanması sağlanıp diğerlerinin ulaşmaları reddedilebilir. Bu tür saldırılarda en çok kullanılan UDP servisleri chargen ve echo servisleridir. Bu servisler aslında neredeyse hiç kullanılmazlar. Dolayısıyla bu servislerin iptal edilmesi ya da güvenlik duvarı üzerinden filtrelenmesi, normal çalışmayı etkilemeyecektir.

Bir bilgisayar üzerinde çalışan UDP echo ve chargen servislerini iptal etmek için yapılacaklar her sistem için farklıdır. Unix sistemler için yapılması gereken, inetd.conf dosyası içerisinde, bu servislere ilişkin tanımlamaların yapıldığı satırların başına '#' koymak ve o satırın dikkate alınmaması sağlanır. Aktif olması için sistemin tekrar başlatılması gerekir. Aynı işlemler diğer UDP servisleri içinde uygulanabilir. Böylece bu servislerden gelebilecek saldırılar önlenmiş olacaktır.

Saldırıların daha çok hangi servislere yapıldığının tespiti için ağa saldırıları kontrol edip raporlayan (intrusion detection) programların kullanılması faydalı olacaktır.

2.3.6.6 NFS'e yönelik saldırılar

NFS (Network File System), ağ üzerindeki bilgisayarların dosyalarını birbirleriyle paylaşmalarını sağlayan bir protokoldür. Ancak bu protokolün açıklarının kullanılmasıyla, sistemi büyük zararlar verilebilecek bir saldırıya açmış olursunuz.

NFS uzun zamandır üzerinde çalışılan bir protokoldür ve saldırı programları internette yaygın olarak bulunmaktadır.

NFS'e yönelik saldırılar değişik sonuçlar doğurabilir. Saldırgan hedef bilgisayar üzerinde süper kullanıcı yetkisiyle işlemler yapabilecek duruma gelebilir.
Alınabilecek önlemeler;
Güvenlik duvarından NFS servislerine ait paketlerinin geçişi engellenebilir. Aynı şeklide internet üzerinden bu servislere ulaşım yasaklanabilir. Bu önlemeler NFS'e dışardan gelebilecek saldırılar içindir. İç ağdan gelebilecek saldırılara hala açıktır.

Güvenlik duvarı üzerinden alınabilecek önlemelerin yanı sıra /etc/exports dosyası üzerinde yapılacak bazı düzenlemelerle alınabilecek önlemlerde vardır. NFS ile ilgili yamaların takip edilip programa eklenmesi de saldırıların etkisini azaltacaktır.

2.4 Ağ güvenliği

Sistemlerin büyümesi ve sistem içerisindeki birimlerin farklı özelliklere sahip olması durumunda her bir düğümün (makine, bilgisayar) güvenliğinin sağlanması oldukça zor olacaktır. Bu da ağın güvenliğinin sağlanması çalışmalarına yönelmeye zorlamaktadır. Bu yaklaşımdan yola çıkılarak, ağda hizmet veren makinalara ve ağa erişimlerin tamamının kontrol edilmesi gerekir. Her ağa, güvenlik delikleri sayesinde içeriden ya da dışarıdan izinsiz erişimler olabilmektedir. Ağın önemli ve hassas bilgiler barındırması sebebiyle içerdeki verilerin ve hizmetlerin korunması önemlidir. Önemli verilerin sadece iç ağdaki kullanıcılara değil aynı zamanda dışarıdan girebilecek kişilere karşı da korunmuş olması gerekir.

En iyi güvenlik çözümü ağ bağlantısını kesmektir. Ancak bu tür bir çözüm bilgisayar haberleşmesi teknolojisini kullanan organizasyonların zararına olacaktır. Dıştaki güvenilmez ağ ile içteki güvenilir özel ağ arasında koruma sağlayan güvenlik duvarları, ağ bağlantısını kesmek yerine kullanılabilir.

Güvenlik duvarlarının kullanılması, komple güvenlik çözümünü oluşturan esaslar olan;
1. Güvenlik politikasının belirlenmesi,
2. Fiziksel güvenlik,
3. Erişim kontrol,
4. Kimlik onaylama
5. Şifreleme
6. Takip

fonksiyonlarının sadece bir parçasını oluşturacaktır.

Güvenlik duvarı kullanarak çok büyük yerel alan ağları korunabilir.

2.4.1 Fiziksel Güvenlik

Ağ güvenliği fiziksel güvenlikle bağlantılıdır. Ağ makinesinin boyutu ve şeklinin yanı sıra ağın ihtiyaçtan dolayı ve karşılıklı güven ilişkilerine dayalı olarak bir binayı, kampüsü, ülkeyi ya da dünyayı sarabilme ihtimali vardır. Fiziksel güvenlik politikasının, ağ güvenliği politikası oluşturulurken yenilenmesi veya dikkate alınması gerekebilir.

2.4.2 Erişim Kontrol

Erişim kontrol, gelen her ağ paketinin içeriye alınıp alınmayacağına ve pakete karşı yapılacak davranışa karar verir. Bir güvenlik duvarı, paketin veya oturumun tanımlanmış güvenlik politikasına uygunluğunu belirler. İyi tasarlanmış güvenlik duvarı detaylı güvenlik politikalarını gerçekleştirebilir. Ayrıca güvenlik duvarları özel bir ağı uzaktan erişim zayıflıklarına karşı koruyan en iyi çözüm olarak kabul görmüşlerdir.

Ağ protokolleri, yazılım ve konfigürasyondaki yanlışlıklar ve problemlerden kaynaklanan uzaktan erişim zayıflıkları, saldırganların yetki alarak dışarıdan sisteme girişlerini kolaylaştırmaktadır.

2.4.3 Kimlik Onaylama

Kimlik onaylama yetkili personel ve bölümlerin serbestçe haberleşmelerini sağlarken izinsiz erişimi engellemektedir. Kullanılan onaylama yöntemi kullanıcının nereden ve nasıl onaylandığına bağlıdır. Internet ve öteki uygulamalar için en popüler onaylama yöntemleri, “Neredeler”, “Neleri var” ve “Neler Biliyorlar” dır. Ancak IP adres onaylaması veya “Neredeler” yöntemi, IP adres sahtekarlığı saldırı yöntemi kullanılarak geçilebilir.

2.4.4 Şifreleme

Şifreleme veri bütünlüğünü garantileyebilir ve güvenli hatlardan yollanan bilgiyi koruyabilir. Önemli şirket bilgilerine uzaktan erişimde veya organizasyon intranetine erişimde korumanın sağlanabilmesi için şifreleme kullanılabilir.

Ancak şifrelemede önemli olan anahtarların hangi yoldan gönderileceği ve nasıl yönetileceği konularıdır. Anahtarlar verinin şifrelenmesi ve açılmasında kullanılır. Otomatik anahtar yönetimi bir çok konağı bulunan ağ için şarttır. PKI bu alandaki çalışmaları içermektedir.

2.4.5 Takip

Güvenlik politikası uygulanmaya başladıktan sonra, bütün sistem parçaları ve personelin güvenlik politikasına uygunluğunun periyodik olarak kontrol edilmesi gerekmektedir. Yeterli denetimin olmaması durumunda, bir güvenlik ihlali sonrası takip için yeterli delil olmaması durumunda, bir güvenlik ihlali sonrası takip için yeterli bilgi olmayabilir. Denetimin yapılması, problemleri önceden tespit ederek güvenlik boşluklarına dönüşmelerini engelleyebilir. Günlük kayıt ve anında uyarı mesajının yollanması, kısa sürede önlem alınmasını ve atak kaynağının tespitini kolaylaştırır.

2.5 Elektronik Posta Güvenliği

Ağ üzerindeki elektronik postaların güvenli bir şekilde gönderici ve alıcı arasında yol alması amacıyla değişik uygulamalar değişik protokolleri, bu protokoller de farklı şifreleme ve imzalama algoritmalarını kullanmaktadırlar. Bunlardan biri olan PGP protokolünde X.509'a benzer bir sertifikasyon yapısı vardır. PGP protokolünde Her kullanıcı aynı zamanda bir sertifikasyon otoritesidir(CA). Bunun anlamı ise her kullanıcı kendine ait bir gizli anahtar seçip bu anahtara uygun bir açık anahtar oluşturacak ve bu anahtarı kimlik bilgisiyle ağ üzerinde ortak kullanılan bir sunucuya aktaracaktır. Kendisine ait gizli anahtarı uygun bir yerde saklayan kullanıcı haberleşeceği adresin açık anahtarını ise Public-Key ring adı verilen bir soyada toplayacaktır. PGP, açık anahtarlı algoritma olarak RSA, gizli anahtarlı algoritma olarak IDEA ve özetleme fonksiyonu olarak MD5 algoritmasını kullanmaktadır. Kendi simetrik algoritmasına ait üretilen gizli anahtarla mesajı şifreleyen kullanıcı, gizli anahtarı'da alıcı kişinin açık anahtarlı algoritmasına ait açık anahtarla şifreleyecek ve bütün bu şifreli kısımları da kendine ait gizli anahtarla imzalayacak ve alıcıya gönderecektir. Alıcı ise kendi açık anahtarlı algoritmasının gizli anahtarıyla, şifrelenmiş anahtarı açacak ve buradan elde edilen anahtarla da şifrelenmiş mesajı açacaktır. Mesajın imzasını ise gönderenin açık anahtarıyla kontrol edecektir.

2.5.1 Ağ Yönetim Güvenliği

Birbirine bağlı ağların kullanımının artmasıyla birlikte ağların yönetim sistemlerindeki güvenlik probleminin çözülmesi gerektiği de önem kazanmıştır. Ağ yönetim protokollerinden SNMPv1 sadece ulaşım kontrolü vardı. Güvenlikle ilgili eklemeler yapıldı ve ikinci sürümü çıkartıldı. SNMPv2 ulaşım kontrolünün yanında kimlik doğrulama ve gizlilik fonksiyonlarını da içermektedir. SNMPv3'te güvenlik ön plana çıkmıştır.

2.5.2 İşletim Sistemlerinin Güvenliği

İşletim sistemi denildiğinde akla ilk gelenler UNIX ve Windows türevi sistemlerdir. İşletim sistemi seçilirken;

- Kurulum kolaylığı
- Donanım gereksinimleri, sürücü edinebilme
- Kullanım ve yönetim
- Güvenilirlik
- Güvenlik
- Uyumluluk
- Fiyat

- Destek

gibi özelliklere bakılarak seçilir. Bu özelliklerden güvenlik eğer sistem ağa açılacaksa çok büyük önem kazanacaktır. İşletim sistemlerinin güvenilirliği sürekli olarak tartışılmakta ve çıkan her yeni sürümde güvenlik delikleri kapatılmaktadır. Burada Windows NT ile UNIX işletim sistemlerinin güvenlik üzerine sundukları teknolojilerden kısaca bahsedilecektir.

Windows NT'nin Güvenlik Bileşenleri;

Giriş süreçleri (Logon Process): Kullanıcıların giriş isteklerini kabul eder. Kullanıcının ismi ve parolası kontrol edildikten sonra tanımlanan haklara göre hareket etmesini sağlayan sistemdir. Yakından ya da ağ üzerinden giriş yapılabilir.

Yerel Güvenlik makamı (Local Security Authority): kullanıcının sisteme erişim iznini denetler. Bu bileşen güvenlik alt sisteminin çekirdeğidir. Erişim jetonlarını üretir, yerel güvenlik prensiplerini yönetir ve etkileşimli kullanıcı onaylama hizmetlerini sağlar. Yerel güvenlik makamı aynı zamanda kayıt denetimi prensiplerini de denetler ve güvenlik kayıt mesajlarını kaydeder.

Güvenlik hesap yöneticisi (SAM): Kullanıcı hesapları veritabanına bakarak kullanıcı yönetimini sağlar. Veritabanında tüm kullanıcı ve grupların hesapları vardır. SAM yerel güvenlik makamı tarafından kullanılan kullanıcı geçerli kılma hizmetlerini sağlar.

Güvenlik Başvuru İzleyicisi (Security Reference Monitor) : Kullanıcının bir nesneye erişim izninin olup olmadığının kontrolü ve yaptığı işlemleri denetler. Bu bileşen SAM tarafından tanımlanmış olan erişim iznini geçerli kılma ve kayıt hesabı üretim prensiplerini gerçekler. Hem çekirdek hem de kullanıcı kiplerine, bir nesneye erişmek isteyen kullanıcı ve süreçlerin gerekli izinlerinin olduğunu denetleyen hizmetler sunar. Bu bileşen gerektiğinde kayıt hesabı mesajları da üretir.

UNIX;

Unix'te NT gibi sistem yöneticisine dayalı olarak kullanıcı hesap prensipleri belirleyebilmesi için birtakım özellikler sağlar. UNIX'te kullanıcı adları hangi gruba ait oldukları /etc/passwd dosyasında tutulur. NT'de ise kullanıcı bilgileri kayıt dosyalarında tutulur. Kayıt dosyaları(registery), sadece öncelikli çekirdek rutinleri tarafından erişilebilen, korunan ve şifrelenmiş veritabanıdır.

2.6 Güvenlik Seviyeleri

Güvenlik konusunda olabilecek yaklaşımları gördükten sonraki konu, sistemlerin sahip oldukları güvenlik seviyelerini belirlemek ve yükseltmek olabilir. Sistemlerin içerdikleri donanım ve yazılımlara göre güvenlik seviyeleri özellikleri belirlenmiş ve standartları oluşturulmuştur. Güvenlik seviyelerinde çeşitli fiziksel korumalar, işletim sistemini güvenli hale getirme gibi işlemleri içerir.

1985 yılında DoD tarafından yayınlanan TCSEC yayınında, dört güvenlik seviyesi ve alt sınıfları belirtilmiştir.

2.6.1 D Seviyesi

2.6.1.1 D1 Seviyesi

Mevcut en düşük güvenlik olanaklarını sunar. Bu seviyede bir güvenliğe sahip sistem, bütün olarak güvensizdir. Donanım elemanları için herhangi bir koruma mekanizması yoktur. İşletim sistemi kolaylıkla geçilebilir ve istenen amaçlara uygun şekilde kullanılabilir. Sistem kaynaklarına

yetkili kişilerin ulaşmasını denetleyecek bir erişim kontrol sistemi yoktur. MS-DOS, MS-Windows 3.1/95/98 ve Apple Macintosh bu sınıftandır.

2.6.2 C Seviyesi

C1 ve C2 olmak üzere iki alt güvenlik seviyesine ayrılmıştır. Bu seviye güvenlikte kullanıcı için hesap tutulur(account) ve izleme(audit) yapılır.

2.6.2.1 C1 Seviyesi

Sınırlı bir güvenlik koruması vardır. Daha çok kullanıcı hatalarından sistemi korumak gerekli tanımlar bulunur. Dışardan gelecek saldırılara karşı koruma mekanizmaları yoktur.

Unix işletim sisteminin sunduğu güvenlik gereklerini içerir. Ayrıca donanım elemanları için bazı güvenlik mekanizmalarını da içerir. Donanım elemanlarının istenmeyen kişiler tarafından ulaşılması zorlaştırılmıştır. Sistem kaynaklarına ulaşmak isteyen kullanıcıların erişim kontrolü yapılmaktadır. Erişim kontrolü, kullanıcı adı ve parolasına göre yapılmakta ve sonuçta kullanıcının sisteme erişim hakkı varsa sisteme alınmaktadır. Kullanıcı sisteme girdikten sonra kendisine verilmiş haklar ve sınırlamaların dışına çıkamaz.

Kullanıcı adı ve şifresinin belirlediği erişme hakkı, sistemdeki dosya ve dizinlere ilişkin izinlerdir. Dosya ve dizinlere erişim hakkı o dizin sahibi ya da sistem yöneticisi tarafından verilebilir. Böylece istenmeyen kişilerden korunma sağlanır. Sistem yöneticisi için bir sınırlama olamaz.

UNIX ve IBM MVS bu sınıfa örnektir.

2.6.2.2 C2 Seviyesi

C1 seviyesine göre daha güvenli hale getirilmiştir. C2 seviyesinde kaynaklara kontrollü erişim sağlanabilmektedir. Bunun anlamı, bir kullanıcının bir dosya veya dizine ulaşması sırasında sadece haklarına bakılarak izin verilip verilmemesine karar verilmez. Bununla birlikte bir yetkilendirme mekanizması da geliştirilerek, kullanıcının belirtilen dizine ulaşmaya yetkili olup olmadığına veya bir komut koşturmak için gerekli yetkiye sahip olup olmadığına bakılarak, istediği işlemi yapması sağlanır ya da reddedilir. Yetkilendirmenin dışında bu seviye güvenlikte yapılan işlemlerin kontrol edilmesi gerekir. Bunun için de sistemde yapılan her iş ile ilgili bir kayıt tutulur.

C1 güvenlik seviyesindekilere ek olarak yapılan işlemlerin kontrol ve kaydedilmesi, C1 seviyesinde yaşanan güvenlik problemlerini ortadan kaldıracaktır. Yapılan fazladan kontrol ve kayıt işlemleri, sistemin işlemci zamanını ve diskten alan alacaktır.

C2 güvenlik seviyesine örnek sistemler Windows NT 4.0 ve Digital Equipment VAX/VMS 4.x gösterilebilir.

Güvenlik arttıkça kaynaklara erişimdeki hız düşmektedir.

2.6.3 B seviyesi

Üç alt güvenlik seviyesine (B1,B2,B3) ayrılır. Zorunlu erişim denetimi kullanılır. Sistemdeki her nesnenin güvenlik seviyeleri tanımlanır.

2.6.3.1 B1 seviyesi

Çok katmanlı güvenlik yapısı kurulmasını sağlar (gizli,en gizli vb..). Sistemde, güvenliği sağlanacak nesnelerin diğerlerinden kesinlikle ayrılması gerekmektedir. Bu nesneler diskette ya da diskte saklanacak türdendir.

Bu sisteme örnek olarak OSF/1, AT&T V/MLS, IBM MVS/ESA sistemleri verilebilir.

2.6.3.2 B2 seviyesi

Bu seviyedeki güvenlik için sistemdeki bütün nesnelerin (birimlerin) etkilenmesi gerekmektedir. Diskle, teypler veya terminaller, bir veya daha fazla olabilecek güvenlik seviyesi ile ilişkilendirilebilirler. Güvenlik düzeyi yüksek olan bir cihaz ile güvenlik düzeyi düşük cihazın haberleşmesinde problemler çıkacaktır, bunlara dikkat edilmesi ve çözülmesi gerekir.

Bu güvenlik seviyesine örnek olarak Honeywell Information Systems'in Multics Sistemi, Trusted XENIX verilebilir,

2.6.3.3 B3 Seviyesi

Güvenliği, donanımların uygun kurulumlarıyla sağlamaya çalışan yöntemi içerir. B2 seviyesine göre daha sağlam, ciddi bir sistem tasarımı vardır. Güvenlik yönetimi, güvenli kurtarma ve saldırıların ya da oluşan zararların sistem yöneticisine hemen bildirilmesi gibi özellikleri içerir.
Bu seviyeye örnek olarak Honeywell XTS-200 verilebilir.

2.6.4 A Seviyesi

Tek sınıf içermektedir. En üst güvenliği sunan güvenlik seviyesidir. Donanım ve yazılım açısından dizayn, kontrol ve doğrulama işlemlerini içerir. Daha önce bahsedilen güvenlik seviyelerindeki bileşenleri içermektedir. Bir sistemin dizayn,geliştirme ve gerçekleme aşamalarında güvenlik isteklerinin sağlanması istenir. Her aşamayla ilgili isteklerin dokümana uygun olarak yerine getirilmesi gerekmektedir.

2.6.4.1 A1 seviyesi

Dizaynın sağlamlığının matematiksel olarak incelenip,test edilmesi ve doğrulanması gerekmektedir. B3 sınıfına ek olarak güvenli dağıtım (trusted distrubition) özelliği eklenmiştir. Güvenli dağıtım ilkesi uyarınca, sisteme ilişkin yazılım ve donanım bileşenleri üzerinde, güvenlik sistemini etkileyecek değişikliklerin, sistemlerin aktarılması aşamasında tekrar güvenliğin sağlanması gerekir.
Sadece bir güvenlik seviyesi içerir. En yüksek düzeyde güvenlik seviyesidir.
Güvenlik seviyeleri tablo2-4'de özet olarak verilmiştir.

Güvenlik Seviyesi	Alt Seviye	Özet Bilgi
D	D1	En düşük düzeyde güvenlik
C	C1	İsteğe(Kullanıcıya) bağlı güvenlik
	C2	Kontrollü erişim
B	B1	Etiketli güvenlik
	B2	Yapısal güvenlik
	B3	Güvenlik Alanlı koruma
A	A1	En yüksek düzeyde güvenlik

Tablo 2-4 DoD TCSEC'de tanımlanmış güvenlik seviyeleri

3 NE KADAR GÜVENLİK GEREKLİ (HOW MUCH SECURİTY DO YOU NEED)

Ağ güvenliğinin seviyesine karar vermeden önce, yapılabilecek olan korumanın seviyesine karar verilmelidir. Bunun için ağ'ın güvenlik analizinin yapılması gereklidir.

3.1 Risk Analizi

Risk analizi korunması istenilen varlıkların ve onlara karşı olan potansiyel saldırıların belirlenmesi sürecidir. Doğru risk analizinin yapılması önemli bir adımdır. Biçimsel bir risk analizi aşağıdaki sorulara cevap vermelidir.

Ne tür varlıkları korumak gereklidir.
Bu varlıkları nelerden korumalıyız.
Ağ'a kim tehlikeli saldırı yapabilir ve ne kazanabilir.
Bir tehdit'in varlıklarımızı bozma olasılığı ne kadardır.
Eğer bir tehlikeli saldırı olursa bunun ivedi maliyeti ne olacaktır.
Bir atak veya bozulmanın geri kazanma maliyeti ne olacaktır.
Bu varlıklar, etkin maliyet ile nasıl korunabilir.

3.2 Korunacak varlıklar

Bir ağda güvenlik ile ilgili bir çalışma yapılmaya başlandığında ilk karar verilmesi gereken nelerin korunması gerektiğidir. Korunması gereken varlıklar üç ayrı ana başlıkta toplanabilir.

- Veriler
- Kaynaklar
- Zaman
- Saygınlık

Bu varlıklar ayrı ayrı incelenecektir.

3.2.1 Veriler

Veriler, güvenlikle ilgili olarak üç özelliğe sahip olmalıdır;

Gizlilik: Verilerin , başkaları tarafından öğrenilmesi istenmeyebilir.

Bütünlük : Sahip olunan verilerin başkaları tarafından değiştirilmesi istenmeyebilir

Kullanıma hazırlık : Verilerin istendiği zaman ulaşılabilir olup kullanıma hazır olması istenir.

Daha çok gizlilikle ilgili güvenlik üzerinde durulur. Gerçekten de bu konuda risk çoktur. Bir çok kişi ya da kuruluş için gizli bilgiler bilgisayar üzerinde tutulur. Bu bilgisayarların güvenliği de Internet bağlantısı kopartılarak sağlanmaktadır. Bu şekilde bilginin gizliliği sağlanmış olabilir ama kolay ulaşılabilirlik ortadan kalkmış olur. Yani bir şekilde ağa bağlanılmalıdır. Bu durumda güvenlik politikaları belirlenerek, bilgilerin güvenliğinin sağlanması gerekmektedir.

3.2.2 Kaynaklar

İnternet'e bağlanmakla riske atılacak ikinci şey, bilgisayar kaynaklarıdır. Başka insanların bir kuruluşa ait bilgisayardaki sabit diskte yer alan boş alanları kendi amacı için kullanmak istemesi her ne kadar mevcut verilere zarar vermeyecek bir şey olsa da istenecek bir durum değildir. Bunun

gibi diğer kaynakların da (işlemci,bellek, ...) başkaları tarafından kullanılması, kabul edilebilir bir şey olamaz

3.2.3 Saygınlık

Her kişi ya da kurumun saygınlığının İnternet üzerinde de korunması önemlidir. Meydana gelebilecek güvenlik problemleri kişi ve kurumların doğrudan aleyhine olup kötü reklamdır. İnternet üzerinde işlemler yapan bir kişinin, başka bir kişinin adını kullandığı düşünülürse, zarar verme durumunda direk muhatap alınacak kişi saygınlığını kaybetme durumuyla karşı karşıya kalacaktır.

Genelde başka birinin hesabından girip sahte elektronik postalar atarak zarar verilir. Bunun sahte olduğunun kanıtlanması neredeyse imkansızdır. Böyle durumlarda, sahteciliği yapan kişinin kullandığı hesaba sahip kişi kadar kurum da zarar görür.

İnternet'e açılmayı düşünen kurumların eğitim ya da güvenlik politikası içinde, saygınlığın korunması için kişilere düşen güvenlik tedbirlerinin anlatılması gerekir. Ayrıca periyodik olarak takibinin yapılması şarttır.

3.3 Kaynaklar Kimlerden korunmalı

Ağın yapısına bağlı olarak saldırganlar değişebilir. Saldırılarının büyük çoğunluğu iç ağdan gelmektedir. Ağa açılan bilgisayarların verdiği hizmetlere göre, ne tür saldırılara uğrayacağı ve saldırgan türleri de ortaya çıkabilir. Risk analizi sırasında bu saldırı kaynaklarının belirlenmesi gereklidir
Potansiyel saldırı kaynakları aşağıda belirtilmiştir.

Dahili Sistemler
Çevre ofis erişim noktaları
Bir iş ortağına olan geniş alan ağ bağlantısı üzerinden
Internet bağlantısı üzerinden
Modem havuzu üzerinden
Henüz kimlerin saldırı yapacağını belirlemeden, saldırı kaynaklarını belirlemek gerektiğini akılda tutmalıyız.

3.4 Ağ'a kim tehlikeli saldırı yapabilir.

Potansiyel saldırı yapabilecek kişilerin belirlenmesi gereklidir.

- Çalışan İşçiler
- Geçici veya Danışman Personel
- Rakipler
- Organizasyonun görüş ve maçlarından çok farklı düşünceye sahip olan şahıslar.
- Organizasyona düşmanlığı olan şahıslar veya onları personeli
- Sizin Organizasyonunuzun halka açık görüntüsünden dolayı şöhret kazanmak isteyen kişiler.

Kuruluşun yapısına göre bu listeye yeniler eklenebilir.Önemli olan başarılı bir saldırı sonunda ağ'a zarar verebilecek potansiyel saldırganları belirleyebilmektir.

En çok görülen saldırı tiplerinden biri, sisteme davetsiz misafirlerin girmesidir. Bunlar sisteme girdikten sonra çeşitli saldırılar yaparlar. Genelde yapılan, verilerin servislerin kilitlenmesine yönelik saldırılardır.

3.5 Bir Saldırı İhtimali nedir.

Kaynakları ve olabilecek saldırı türlerini belirlemek gereklidir,kuruluşun saldırılara karşı potansiyel risklerinin değerlendirilmesi gereklidir. Yalıtılmış bir ağa mı sahip veya ağ birçok noktadan geniş alan Ağı'na mı bağlı, modem havuzu var mı, veya VPN ile mi bağlı. Bütün bu bağlantı noktaları güçlü yetkilendirme sistemlerine sahip mi ? Yoksa güvenlik duvarı ile mi korunuyor, ve bazı alarmlar var mı? Saldırı ihtimalinin değerlendirilmesinde farklı görüşler olabilir.

3.6 Acil Maliyet Nedir.

Saldırı sonucunda fonksiyonunu yapamayacak olan her bir varlık için acil maliyetin hesaplanması gereklidir. Nakliye gibi Uzun süreli etkiler bunun içinde olmamalıdır. Örneğin bir sabit disk bozulmasından dolayı sunucunun kapalı kalmasının kabaca dakikada 14.50 dolarlık bir ivedi maliyeti olacağı söylenebilir.

Bazen ivedi maliyetin hesabı oldukça güç olabilir. Örneğin, bazı rakiplerin çalacağı şema,çizim, ve yeni üretilecek parçaların projelerinden dolayı maliyet daha fazla olacaktır. Bu ise rakiplerin daha gelişmiş ürün tasarlamalarına neden olacaktır. Böyle bir kayıp çok daha yıkıcı olabilecektir.

3.7 Bir atak veya bozulmanın geri kazanma maliyeti ne olacaktır.

Bozulma veya zararlı saldırının başlangıç maliyetini hesapladıktan sonra bu bozulmanın getireceği toplam maliyetin hesaplanması gereklidir. Örneğin şirket bilgisini saklayan bir sunumcu bozulmasındaki maliyetler için;

- Bütün kullanıcıların bağlantılarının kesilmesinin ani maliyeti ne olur.
- Yapılan saldırının hangi kaynakları ne kadar süre erişilemez yaptığının maliyeti nedir.
- Silinen veya bozulan kritik dosyaların onarım maliyeti nedir.
- Her bir donanım elemanının onarın maliyeti nedir.
- Bütünüyle bir sunumcunun onarım maliyeti nedir.
- Bilgi çalınmış ve hırsız bulunamamış ise bunun maliyeti ne olacaktır..

3.8 Bu varlıklar, etkin maliyet ile nasıl korunabilir.

Ağ ortamını korumanın bir maliyeti olacaktır. Ancak bu maliyetin en az olmasına dikkat edilmelidir. Bu nedenle koruncak olan varlıkların risk analizlerinden korumanın seviyesi belirlenmiş olacaktır. Bazı güvenlik seçimlerinde güçlüklerle karşılaşabiliriz. Örneğin Internet bağlantısında paket filtreleme yeterlimidir.? Yoksa bir güvenlik duvarı yatırımı yapılmalımıdır.? Bir güvenlik duvarı yeterli midir. Bunlar güvenlik uzmanlarının düşünüp çözüm bulacakları önemli sorulardır.

Örneğin bir sunumcunun devre dışı kalmasının günlük maliyeti 14.000 $ olur ise bir RAID disk yatırımı gerekli olacaktır. Bunun yanında bazı gizli maliyetlerde olabilecektir. Örneğin kullanıcıların bu sürede çalışmamaları ve atıl kalan işgücünün maliyetinin hesabı oldukça zordur.

3.9 Güvenlik Önlemlerinin Bütçesinin Çıkartılması

Uygulanacak Güvenlik önlemlerinin maliyetinin çıkartılarak tahmini bütçenin ne olduğunun belirlenmesi gereklidir. Bunlar Sunumcu donanımı güvenlik duvarı ve güvenli bölgelerin kurulumunu ve güvenlik personeli, testler, ve sistem bakımını içerebilir. Burada hiçbir zaman "*bütün yumurtaları aynı sepete koyma*" sözünü unutmamak gerekir.

3.10 Bulunanların yazılı olarak dökümante edilmesi.

Bu çalışmalar sonucunda elde edilen bulguların yazılı olarak raporlanması gereklidir. Çünkü bu doküman daha sonraki güvenlik önlemlerinin geliştirilmesinde temel kaynak olacaktır. Ayrıca daha sonra yapılan işlemlerin günlük olarak kayıtlarının tutulması gereklidir.

3.11 Güvenlik Politikasının Geliştirilmesi

Çoğu yöneticinin ilk soracağı soru, Neden bir güvenlik politikasına ihtiyaç duyuyoruz. Şeklinde olmalıdır. Güvenlik politikası aynı zamanda kuruluşun tamamının güvenlik hedeflerini açıklamalıdır.
İdeal güvenlik, ağ tasarımı, bilginin gizlilik derecesini ve kullanıcı hakları ile uygulama sınırlamalarını hesaba katan sağlam bir güvenlik politikası ile başlar. Politika, güvenliğin temelini oluşturur. Kurumun önemli gördüğü ve korunması gereken bilgiler ile bu bilgileri tehdit eden hareketleri belirler. Güvenlik politikasının oluşturulmasında sorulacak anahtar sorular şunlardır.

1. Kime, nereye, ne zaman, nereden ve hangi yetkiyle izin verilebilir ?
2. Hangi aktiviteler tehdit olarak görülür ve güvenlik riski yaratırlar ?
3. Ne tip gözden kaçmalar ve dikkatsizlikler olabilir?
4. Güvenlik politikasının gerçekleştirilmesinde kim, ne yetki ve sorumluluğa sahiptir?

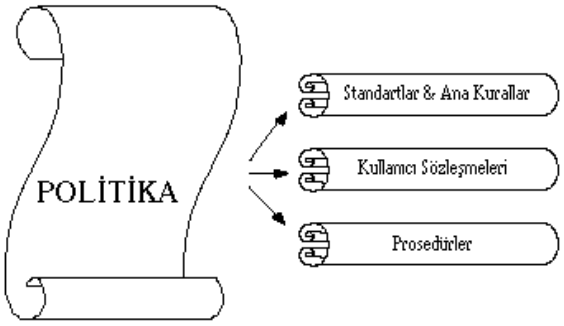
3.12 Güvenlik Politikası Temelleri

Politika, farklı tiplerdeki bilgilere erişim için kişilere yetki sağlar. Ayrıca ne tür ve ne kadar güvenlik zorunluluğu ve ölçülerine uyulması gerektiğine bakarak kuralları ve standartları belirler. Prosedürler, politikayı sağlayan standart ve kuralların(guidelines) uygulanması için metotları sağlar. Neredeyse bütün kurumların bir bilgi güvenliği politikası vardır. Fakat bazı kurumlarda politika açıkça yazılmamıştır.

Politika yazılmazsa, organizasyon çalışanların yanlış anlamalarından dolayı risk altındadır demektir. Ayrıca bir güvenlik problemi olması durumunda cezanın boyutu da belirsiz olacaktır. Bir politika yazmak, organizasyonun kararlılığının başlangıcıdır. Ayrıca ana kuralların belirlenmesi ve onların uygulamaya konulması açışından da önemlidir.

3.12.1 Güvenlik Politikası Yazılması

Bir bilgi güvenliği politikası bir vakum içinde yazılmaz. O kurumun ihtiyaçlarıyla direk olarak ilişkilidir. Bütün kurumlara tam olarak uyan genel bir güvenlik politikası yoktur.



Şekil 3-1 Güvenlik politikası oluşturmak için işlemler

Bir organizasyonun güvenlik politikası oldukça kısa olmalıdır. Yaklaşık olarak beş sayfa olabilir. Platform bağımlı terimler olmamalı, genel olmalıdır. Yapı ve teknolojideki değişimlere göre esnek olarak hazırlanmalıdır. Birkaç yıllık bir ömrü olmalıdır.

Güvenlik politikası dokümanı aşağıdaki bilgileri içeren dokümanlarla ilişkili olmak zorundadır.
1. Standartlar ve ana kurallar
2. Kullanıcı sözleşmeleri

3. Prosedürler

Bunlar bilgisayar platformu, teknolojisi, uygulamaları, kullanıcı güvenirliliği ve organizasyon yapısıyla ilgili özel bilgileri içeren dokümanlardır. Politika, güvenliğin uygulanması için beyannamedir ve ilgili dokümanlar uygulama metotlarını sağlar.

3.12.1.1 Politika Esasları

Güvenlik politikası minimum aşağıdaki özellikleri sağlamalıdır.

- Kuruluşun diğer politikaları ile uyumlu olmalıdır.
- Uygun seviyedeki yöneticiler kadar network destek personeli tarafından da kabul edilmelidir.
- Mevcut ağ cihaz ve prosedürlerini kullanarak uygulanabilmelidir.
- Yerel yönetim, devlet kanun ve yönetmelikleriyle uyumlu olmalıdır.

Üç temel güvenlik amacına dayanır.

1. Gizlilik : Hassas bilgilerin sadece yetkili kişiler tarafından okunduğundan emin olma ve yetkili olmayan kişilere bilgilerin ifşa edilmemesi.
2. Bütünlük : Yazılım ve verilerin bozulmamasının sağlanması.
3. Kullanılabilirlik : Sistem, ağ, uygulama ve verilere yetkili kullanıcılar istediklerinde erişip işlem yapabilmelerinin sağlanması.

Gizlilikte seviye isteyen farklı uygulama tipleri için, bütünlük ve kullanılabilirlilik değişecektir. Örneğin nükleer silah araştırma sistemi yüksek seviyeli gizlilik ister fakat, birkaç saatlik sistemin kapalı tutulmasına dayanabilir. Genel bilgi verilen sistemlerde çok düşük seviyeli gizlilik yeterlidir, fakat yüksek seviyede bütünlük ister. Telefon anahtarlama sistemlerinde yüksek seviyeli kullanılabilirlik istenmektedir.

Ayrıca yukarıdaki amaçların tam olarak sağlanması için politika esaslarının aşağıdaki özellikleri de içermesi gerekmektedir.

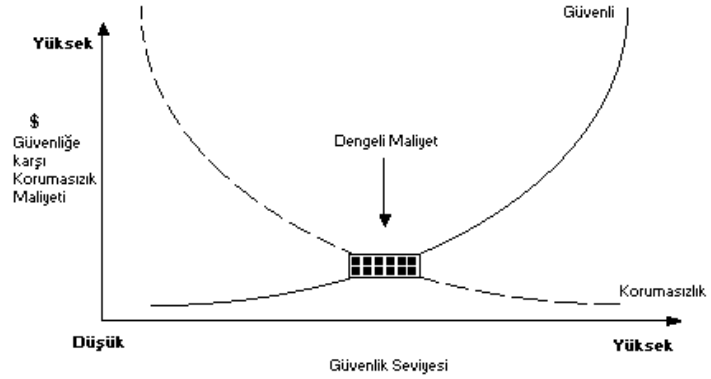
1. Sorumluluk: Kimin neler yaptığını anlayabilme yeteneğidir.
2. Kaynak Kontrol: Bilgisayar ekipmanlarını kazalardan, doğal ve kasıtlı olabilecek zararlardan korumak ve yetkisiz kişilerin bu birimlere erişimini sınırlamak gerekir.

3.12.1.2 Risk Yönetimi

Politika tanımlarken, bilgi sistemlerinizin risk ve tehditlerini bilmeniz gerekir. Tehditler potansiyel güvenlik problemlerinin kaynağıdır. Tehditler insan ve doğal kaynaklıdır. Doğal kaynaklı olanlar yangın,su,deprem, insan kaynaklı olanlar ise kazara ya da kasıtlı olarak yapılan tehditlerdir. İnsan kaynaklı tehditlerin bazıları terör ve savaş durumları gibi toplumsaldır. Diğerleri de içerideki kullanıcılar ya da dışarıdaki saldırganlardan kaynaklanır. Son incelemelere göre içerideki kullanıcıların sistemlere saldırganlara (dışarıdan gelen) göre daha fazla zarar verdikleri görülmüştür. Buradan içerideki kullanıcıların büyük sistemlere erişimi sevdiklerini ve çok hassas aynı zamanda önemli bilgilerin nerelerde bulabileceklerini bildikleri söylenebilir.

Risk değerlendirmesi için bir metot “en kötü durum” senaryosuna göre bir maliyet saptanmaktır.

Risk yönetimi, risk & korunmasızlık maliyetine karşı koruma maliyetini dengeleyen süreçtir. Şekil3-2 de temel teori gösterilmiştir. Koruma ve korunmasızlık maliyetinin neredeyse aynı olduğu nokta gölgeli olarak gösterilmiştir. Bu alan dengelenmiş ve mantıklı güvenlik ölçülerini göstermektedir. Yoksa, güvenlik için gereğinden fazla harcama yapabilirsiniz ya da daha az harcama ile işinizi korumasız bırakarak riske atmış olursunuz.



Şekil 3-2 *Güvenlik-Korunmasızlık Maliyetinin Dengelenmesi*

Risklere karşı üç temel seçim vardır.

1. Kabul : Eğer korunmasızlık çok küçük boyutlarda ve onu koruma altına almak büyük maliyet getiriyorsa, politikanız riski kabul edebilir.
2. Devretme : Bazı durumlarda riske karşı direk olarak koruma almaktansa onun için birini görevlendirmek daha az maliyet getirebilir.
3. Kaçınma :Güvenlik olaylarının neredeyse hiç olmayacağı yerleri korumaya almak maliyet getireceğinden bundan kaçınılmalıdır.

Güvenlik riskleri içeriden veya dışarıdan gelebilecek saldırılardan kaynaklanır. Güvenliğin sağlam olması için yapılması gerekenler şunlardır;

1. Dışarıdan içerideki özel ağa izinsiz erişimi engellemek için Dış Güvenlik (Internet ya da modem bağlantıları),
2. Hassas bilgilerin içeriden izinsiz erişimini engellemek için İç Güvenlik.

Dış ve İç güvenlik için problem yaratan ağ sistemi zayıflıkları üç ayrı kategoride özetlenebilir. :

1. **Protokol**, bilgisayarlar ve ağlar arasındaki iletişimi yöneten ana kurallar. Bir organizasyon ağı içteki ağ için bir ya da birden fazla protokol, ve İnternet ile haberleşmek için başka bir protokol kullanabilir. Yapıları gereği, bazı protokoller saldırganların kullanabileceği güvenlik deliklerine sahiptir. Bir güvenlik duvarı içteki ağı bir çok protokol sorunlarından koruyabilir.
2. **Yazılım,** işletim sistemleri ile bilgisayar ve ağların kendi aralarındaki iletişimi sağlayan ağ iletişimi uygulamaları. Yazılım zayıflıkları genelde güvenli olmayan sürümlerin kullanılmasından kaynaklanır.
3. **Konfigürasyon**, ağdaki donanım ve yazılımın kullanıcı tarafından parametrelerinin düzenleme kuralları. Konfigürasyon zayıflıkları donanım ve yazılımın güvenli olarak nasıl kurulacağının bilinmemesinden ve etkili güvenlik politikasının olmamasından kaynaklanabilir.

3.12.1.3 Güvenlik Sorumluluğu

Politika, güvenlik için kimlerin sorumlu olduğunu belirtmek zorundadır. Basit anlamda, bütün kullanıcılar ilk koruyucu aynı zamanda da en büyük tehdit olduklarından, "herkes" sorumludur. Politika bütün kullanıcılardan sahip oldukları sistem ve veriler için, güvenlik bilgi ve sorumluluklarının anlaşılmasını ve **sözleşme** yapılarak imzalanmasını ister.

Sözleşmeyle ilgili konular;

- Kurumun sistem ve verileri vardır
- Kullanıcılar yetkilerinin olmadığı veri ve yazılım kopyalarına erişmemeyi kabul etmelidirler
- Kullanıcılar parolalarını uzun olarak seçmeli ve gizli yerlerde saklamayı kabul etmelidirler
- Kullanıcılar güvenlik için kurum haklarını koruduklarını bilmelidirler

Politika yayınlanmalı ve bütün kullanıcılara açık olmalıdır. Güvenlik politikasına sadakat çalışanın performans değerlendirmesinin bir parçası olmalıdır.

Bireyler güvenlik sorumluluğu ile ilgili olarak direk olarak görevlendirilirken sadece fonksiyon ve unvanlarına bakılmalıdır. Genel olarak görevler parçalanabilir.

1. Güvenlik yöneticileri güvenliği izlemekle sorumlu olmalıdırlar.
2. Sistem yöneticileri ve BT müdürleri güvenliğin uygulanmasına yardımcı olmalıdırlar.
3. Bilgi sistemleri hesap tutucuları periyodik olarak bilgi sistemlerinin güvenliğini gözlemlemelidirler. Böylece yönetim sağlanmış ve politika izlenmiş olur.

Organizasyonun yapısına ve büyüklüğüne bağlı olarak, güvenlik işleri değişebilir. Fakat politika bunu açıkça belirtmelidir. Kesinlikle aynı kişi güvenliği izleme,denetim ve uygulama işlerini yapmamalıdır. Böyle bir politikada kontrol ve denge olmaz.

3.12.1.4 İtaat

Politika kurallara uyumdan emin olmak için bir prosedür belirtmelidir. Bu periyodik olarak izleme ya da otomatik olarak politika hatalarının sistem tarafından bildirilmesi demektir. Bir hata bulunduğu zaman, aşağıdaki aksiyonlar oluşabilir.

1. Yetkili uyarılır
2. Problem düzeltilebilir
3. Olay kaydedilebilir
4. Dikkate alınmayabilir

3.12.2 Güvenlik Politikası Yönetimi

3.12.2.1 Büyük Sistemlerin Güvenlik Yönetimi

Enterprise ağın gelişiyle birlikte güvenlik politikalarının tanımlanması ve yönetimi birbirlerine bağlı UNIX,PC ler, PC LANlar, Windows NT ve mainframe sistemler için yapılması zorunludur. Güvenlik prosedür ve kurallarının bilgisayar platformuna bakılmaksızın sağlanması gerekir.

3.12.2.2 Tanımlanmış Politikaya Karşı Gerçek Performansın Ölçülmesi

Bir yer için politika tanımlandıktan sonra onun izlenip izlenmediğinin belirlenmesi gerekir. Bir güvenlik problemi oluştuğunda tekrarlanabileceği için yetenekleri değerlendirilmelidir. Bir organizasyon sıkı bir güvenlik ile dünyanın en büyük saldırganlarına karşı korunabilir. Fakat çok pahalıya mal olur.

Devamlı olarak, gerçek güvenlik performansının ölçülmesi ve daha önceden tanımlanmış hedef kriterlerle karşılaştırılması gerekir.

3.12.2.3 Politika Kategorileri

Bilgi güvenliği politikaları birkaç güvenlik kategorisi içinde gruplanabilir. Bu kategorilerin her biri kullanıcı hesap ve yetkileri, ağ ve sunucu ayarları, dosya sistemi ve dizinler için bir grup güvenlik kontrolleri sunar. Bu kategoriler politika problemlerini belirlemenizi sağlar ve zayıflıkları, potansiyel güvenlik tehditlerini gösterir. Kategoriler;

1. Kullanıcı Hesapları ve Yetkileri

Hesap doğruluğu, giriş parametreleri,parola yapısı,kullanıcı dosyaları.

2. Ağ ve Sunucu Ayarları

Sistem denetçisi, sistem posta yöneticisi, ağ üniteleri, sistem kuyrukları, başlangıç dosyaları.

3. Dosya Sistemleri Ve Klasörler
4. Dosya erişimi,dosya özellikleri

3.13 İyi bir Güvenlik politikası nasıl olmalıdır.

İyi bir güvenlik politikası minimum olarak aşağıdaki özelliklere sahip olmalıdır

- Kuruluşun bütün üyeleri tarafından kolaylıkla erişilebilmelidir.
- Güvenlik hedeflerini açıkça tanımlamalıdır.
- Politikada açıklanan her bir konu doğru bir şekilde tanımlanmalıdır.
- Her bir konuda kuruluşun konumunu açıkça göstermelidir.
- Her konu hakkındaki politikanın savunulmasını açıklamalıdır.
- Ne koşullarda konseptin uygulanabileceğini açıklamalıdır.
- Kuruluş üyelerinin Görev ve sorumlulukları, açıklanan sonuçlarda belirtilmelidir.
- Açıklanan politikaya uymayanların durumu hecelenerek açıklanmalıdır.
- Açıklanan konseptin sonraki detaylarının veya açıklamalar için başvuru bilgisi içermelidir.
- Kullanıcıdan beklenen gizliliğin seviyesini tanımlamalıdır.
- Tanımlanmayan konulardaki kuruluşun tutumunu içermelidir.

3.14 Bir Güvenlik Politikası Örneği

Bir Internet tabanlı Web sunumcu kaynaklarının erişim müsadesi iş ilişkili görevlerin yapılması amacıyla verilecektir. Web erişimi bir personel tarafından sürekli olarak gözlenerek ihlaller önlenecektir. Şimdi bu politikadaki ayrıntıları inceleyelim.

- Bu politika özel olarak, "Internet tabanlı Web sunumcu kaynaklarına erişim" i amaçlar
- Kuruluşun konumu, "iş ilişkili olan görevlerin yapılmasında kullanılacaktır" şeklinde açıklanır.Web browsing sadece iş ilişkili aktivitelerde kullanılacaktır.
- Bu politika sadece ağ kaynaklarının etkin ve verimli bir şeklide kullanımını amaçlar.
- Politika bütün çalışanlara eşit olarak uygulanacaktır. Bu politika üretimde ve üretim dışındaki zaman periyodunda kullanılacaktır.
- Politikada ağ personeli web sunumcuyu gözleyecek, Ayrıca her bir çalışan web erişimi için yöneticisinden izin alacaktır.Bunun anlamı her yöneticinin web erişimi için izin verme yetkisi olacağıdır.
- Bu politikaya uymayanların yazılı olarak ikaz edileceğinin belirtilmesi gereklidir.
- Daha fazla bilgi için lütfen doğrudan ağ yöneticiniz ile irtibata geçiniz.şeklinde olacaktır.
- Bütün web erişimleri ağ personeli tarafından izlenecektir. Böylece personeli gizlilik seviyesi sıfırdır.

3.15 Kurumsal Güvenlik Standardı(ISO 17799 Bilgi Güvenliği Yönetimi)

Organizasyonların bilgi varlıklarının bütünlük, gizlilik ve kullanılabilirlik amaçlarının sürekli olarak açıklıklardan kaynaklanan tehditlere karşı korunabilmesi için organizasyonda bir bilgi güvenliği yönetim sistemi kurulması ve bu sistemin işletilmesi için uluslararası kriterler ISO 17799'da tanımlanmıştır. ISO 17799 standardının uygulama adımları aşağıda açıklanmıştır.

1. **Bilgi güvenliği politikasının tanımlanması**; Oluşturulan güvenlik politikası ile bilgi güvenliği için yönetimin yönlendirilmesinin ve desteğinin amaçlanmaktadır. Yönetim organizasyon için geçerli olacak, ve bilgi güvenliğine ilişkin açık bir politikanın ortaya koyulduğu ve bu politikaya desteğini ve bağlılığını göstereceği bir güvenlik politikası hazırlamalı ve bütün çalışanları politika konusunda bilgilendirmeli ve gerekli eğitimleri vermelidir.
2. **Bilgi güvenliği yönetim sisteminin kapsamının belirlenmesi ve bu sistemin kurulması**; Bu sistem ile organizasyonda bilgi güvenliğinin yönetilmesi amaçlanmaktadır. Bilgi güvenliği gereksinimlerini uygulamak ve kontrollerini gerçekleştirmek bu yönetim

sisteminin sorumluluğundadır. Ayrıca bu sistem oluşturulan güvenlik politikasının onaylanmasını, güvenlik rollerinin ve sorumluluklarının tanımlanmasını ve varlıkların sınıflandırılmasının detaylarını bu yönetim sistemi mekanizması tanımlamalıdır.

3. **Risk değerlendirmesinin gerçekleştirilmesi**; Bilgi güvenliği yönetim sisteminin belirlediği bilgi varlıklarına gerçekleştirilebilecek olan tehditlere karşı organizasyon içerisinde bir risk değerlendirmesi gerçekleştirilmelidir. Risk değerlendirmesi sonuçları raporlanmalı ve incelenmelidir.
4. **Risk yönetiminin gerçekleştirilmesi**; Risk değerlendirmesi sonuçları dikkate alınarak hedeflenen garanti düzeyine ve organizasyonun risk yönetimi yaklaşımlarına uygun olarak risk yönetimi gerçekleştirilmelidir.
5. **Kontrol objelerinin seçilmesi ve uygulanması**; Gerçekleştirilen risk yönetiminin ardından riskin kabul edilebilir seviyeye indirilebilmesi için ISO 17799'da tanımlanan kontrol objelerinden gerekli olanlar tespit edilmeli ve standardın önerdiği şekilde organizasyona uygun olarak uygulanmalıdır.
6. **Uygunluk iddiası**; ISO 17799'a uygunluk için bilgi güvenliği yönetimi gereksinimleri organizasyon için uygulanmalıdır. Dikkat edilmesi gereken nokta bu işlemin bir kerelik yapılmadığı ve bir süreç olduğudur. Yani belirlenen aralıklarda risk değerlendirmesi tekrarlanmalı ve risk yönetimi tekrar gerçekleştirilmelidir. Sonuçlara uygun olarak organizasyonda uygulanan kontrol objeleri güncellenmelidir.

3.15.1 ISO 17799 Denetim Nesneleri

ISO 17799 standardının tanımladığı denetim nesneleri ve bu nesneleri amaçları aşağıdaki gibidir. Organizasyonlar gerçekleştirdikleri risk yönetimi sonuçlarına uygun olarak bu nesnelerden olabildiğince çok miktarda seçmeli ve uygulamalıdır;

1. **Güvenlik politikası**; Bilgi güvenliğinin sağlanması için yönetimin yönlendirmesini ve desteğini sağlamak.
2. **Güvenlik organizasyonu**; Bilgi Güvenliğini organizasyon çapında yönetmek, kurumda bilginin işlendiği ve üçüncü şahısların erişebildikleri ortamların güvenliğini sağlamak ve kurumun bilgi sistemi dış kaynaklarla idare ediliyorsa gerekli güvenlik önlemlerini sağlamak.
3. **Varlıkların sınıflandırılması**; Kurumun bilgilerini uygun seviyede korumak, ve kurum bilgilerinin yeterli ve uygun bir seviyede korunduğunu garanti etmek.
4. **Personel güvenliği**; İnsan hataları, hırsızlık ve kötüye kullanımlardan kaynaklanacak riskleri en aza indirmek, kullanıcıları tehditler konusunda bilgilendirmek, ve bu tür kazalardan oluşacak etkileri en aza indirmek.
5. **Fiziksel güvenlik**; Kurum için değerli olan varlıklara yetkisiz erişimi engellemek, bu varlıkları olası hasarlardan korumak, ve bilgiyi çalınmalara ve değişikliklere karşı korumak.
6. **İletişim ve işlem güvenliği**; Bilgi işlem ve kayıt sistemlerinin doğru ve güvenli çalışmalarını sağlamak, sistem hata risklerini azaltmak, yazılımların ve bilginin bütünlüğünü korumak, iletişimin ve bilginin bütünlüğünü ve kullanılabilirliğini sağlamak, varlıkları hasarlara karşı korumak, iş eylemlerini kesintilere karşı korumak, kurumlar arası bilgi değişimlerini kayba, değiştirilmelere ve kötüye kullanıma karşı korumak.
7. **Erişim kontrolleri**; Bilgiye erişimi kontrol etmek, bilgi sistemlerine yetkisiz erişimleri

engellemek, ağ servislerinin güvenliğini sağlamak, yetkisiz bilgisayar erişimlerini engellemek, ve yetkisiz aktiviteleri tespit etmek.

8. **Sistem geliştirilmesi ve bakımı**; İşlevsel sistemleri gerekli güvenlikle tasarlamak, uygulama sistemlerinde kullanıcı bilgilerini kayba, değiştirilmeye ve kötüye kullanıma karşı korumak, bilginin gizliliğini ve bütünlüğünü korumak ve doğrulamak, uygulama yazılımlarının ve donanımların güvenliğini sağlanmak.
9. **İş devamlılık planı**; İş aktivitelerini kritik ve büyük hasarlı kazalardan sonrada devam ettirmek.
10. **Uygunluk**; Güvenlikle ilgili yasalara aykırı davranmamayı, ve sistemlerin güvenlik politikasına ve standartlara uyguluğunu sağlamak.

4 AĞ SİSTEMLERİ NASIL HABERLEŞİR (Understanding How Network Systems Communicate)

Bu bölümde, bir ağ sisteminde verinin a noktasından B noktasına nasıl iletildiği açıklanacaktır.

4.1 Bir veri paketinin Anatomisi:

Veri ağ üzerinden iletilirken dağıtım zarfı şeklinde paketlenir ve bu paketlere çerçeve denilir. Çerçeveler topolojiye göre değişebilir. Ethernet çok popüler bir topoloji olduğu için detayları açıklanacaktır.

4.1.1 Ethernet Çerçeveleri

Bir ethernet çerçevesi 64-1518 byte arası büyüklükteki sayısal darbelerden meydana gelir ve dört bölüm içerir.

Başlangıç(preamble) : 8 Byte lık her istasyonun hazır olduğunu gösteren haberleşme darbeleri(Başlangıç için gönderilen veriler paketin büyüklüğüne dahil edilmezler.)

Başlık(Header): Başlık bilgisi veriyi kimin gönderdiğini ve kime gideceğini tutar. Aynı zamanda çerçevenin büyüklüğü de tutulur. Eğer alan istasyon farklı büyüklükte çerçeve alırsa, yeni bir çerçeve gönderilmesini talep eder. Büyüklüğü her zaman 14 Byte'dır. Gönderen ve alacak olan istasyonların adresleri mac adreslerdir. Eğer broadcast adresi olur ise mac numarası ff-ff-ff-ff-ff-ff şeklinde olacaktır.

Veri(data): Büyüklüğü 46-1500 byte arasında olabilen ve iletilecek olan veriyi içeren kısımdır. Eğer iletilecek veri 1500 byte'dan büyük ise , parçalara ayrılarak dizi numarası verilir. Eğer 46 byte'dan küçük ise bu defa verinin sonuna 1 dizisi koyularak iletilir.

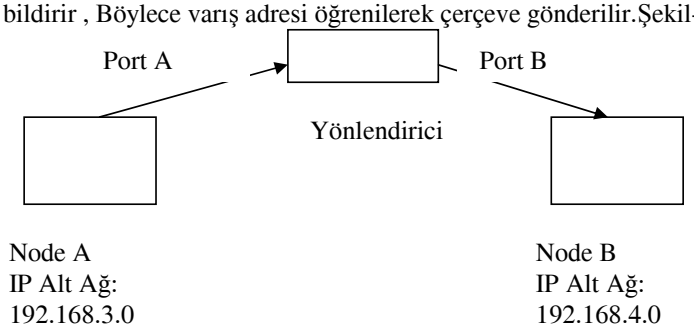
Çerçeve Denetim Dizisi(Frame Check Sequence): Çerçeve Denetim Dizisi alınan verinin gönderilen olup olmadığını denetlemek için kullanılır. Bunun için kullanılan algoritmaya Periyodik fazlalık denetimi (Cyclic Redundancy Check) adı verilir. Bu alanın uzunluğu 4 byte'dır.

4.2 Adres Çözümleme Protokolü(Address Resolution Protocol)

Gönderilmek istenilen verinin gideceği istasyonun mac adresinin bilinmesi gereklidir. Bu ise kart tarafından tutulmaz. Böyle bir durumda ARP paketi gönderilerek IP'den Mac adrese dönüşüm yapılır. ARP fonksiyonu IPX,IP,NetBEUI protokollerinde farklıdır. Eğer bir sistem varış adresini öğrenmek istiyorsa ARP kullanılır.

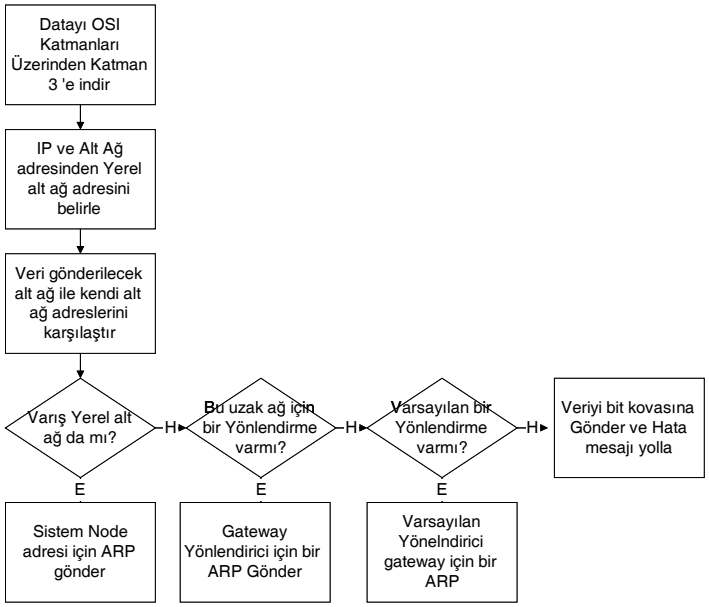
ARP ancak yerel haberleşmede kullanılır. Aşağıdaki örnekte olduğu gibi Node A , Node B'ye bir çerçeve göndermek istediği zaman, node B'nin IP numarası farklı olduğu ve yönlendirme tablosunda da varsayılan yönlendiricinin PortA'sı olduğu için portA'nın adresini ARP paketi göndererek bulur. Paketi Yönlendiriciye gönderir. Yönlendirici , Node B 'nin adresini(MAC) öğrenmek için Prot B'si aracılığı ile ARP gönderir. Node B ARP sorgusuna cevap vererek adresini Port B'ye bildirir , Böylece varış adresi öğrenilerek çerçeve gönderilir.Şekil-4.1 ve 4.2

Silinmiş: <sp>



Şekil-4.1. A ve B sistemlerinin Yönlendirici üzerinden Haberleşmesi

Bütün sistemler ARP ile öğrendiği adresleri belli süre saklama yeteneğine sahiptir.



Şekil-4.2 ARP adres çözümleme protokolünün algoritması

4.3 Bir Protokolün İşi

Bir sistem diğerine bir çerçeve göndermek istediği zaman, node adresinin çerçeve başlığındaki varış adresine koyulduğu bir çerçeve gönderir. Ancak bu iletişim aşağıdaki sorulara cevap vermelidir.

- İletim sistemi çerçevenin tek bir parça olarak iletildiğini kabul etmelimidir.?
- Varış sisteminin "Sizin çerçevenizi aldım, teşekkürler" cevabı göndermesi gereklimidir?
- Eğer cevap gönderilir ise, her bir çerçeve için ayrı ayrı mı, yoksa çerçevelerin tamamı için bir ad. Cevap mı gönderilmelidir.?
- Eğer varış sistemi aynı ağ da değil ise veriyi göndereceğimiz adresi nasıl öğreneceğiz.
- Eğer varış sisteminde e-posta,dosya transferi ve web sayfaları gezintisi var ise bu datanın hangi uygulama için olduğunu nasıl anlayacak?

Protokolün işi, bu soruların cevaplarını vererek veriyi iletmektir. Topolojilere göre protokoller de özellik gösterir. Örneğin Ethernet üzerinde çalışan TCP/IP protokolü, servisleri Token ring veya ATM'de kullanılamayacaktır.

4.4 OSI Modeli

1977'de Uluslar arası Standartlar Kuruluşu(ISO), farklı satıcı sistemlerinin birbirleriyle haberleşmelerine yardımcı olmak amacıyla Açık Sistem Bağlantı Kaynak Modeli (OSI) yi geliştirdi.

OSI Modelinde 7 katman bulunmaktadır. Her bir katman, iletişimin nasıl yapılacağını ve diğer katmanlar ile etkileşimi açıklar. Bu ise bir satıcının ürününde bulundurması gereken minimum standartları belirlemiş olur.

Bu katmanlar aşağıdan yukarıya doğru,

1. **Fiziksel Katman :** İletim ortamı, konnektörler ve işaret darbelerinin özelliklerini açıklar. Bir tekrarlayıcı veya Hub fiziksel ortam cihazlarıdır.Veri Birimi bittir
2. **Veri Bağlantı Katmanı(Data Link Layer):** Yerel sistemler arasındaki topoloji ve haberleşme özelliklerin tanımlar. Paket başlıklarını ve checksum dizilerin hazırlar. Datagramları çerçevelere paketler. Hataları anlar. Veri akışını düzenler. Donanım adreslerini dönüştürür.(FDDI,Ethernet,T1), Network Interface Kartları, Veri birimi **çerçevedir**.
3. **Ağ Katmanı(Network Layer):** Ağ katmanı, farklı ağ segmentlerinde bulunan sistemlerin birbirlerini nasıl bulacaklarını açıklar, aynı zamanda ağ adresini de tanımlar.Çoklu ağ segmentlerinin bağlantılarını yönlendirir. (network routing) veri birimi **Pakettir.**
4. **İletim Katmanı (Transport Layer):** Verinin gerçek hareketi ile ilgilenir ve ağ üzerinden iletime hazırlar. Eğer veri çerçeveden büyük ise iletim katmanında küçük parçalara ayrılarak sıra numarası verilir.Alt ağlar arasındaki mesaj haberleşmesini yönetir. Veri birimi se**gmenttir**.
5. **Oturum Katmanı (Session Layer):** İki veya daha fazla sistem arasındaki ulaştırmanın sağlanması ve devamını sağlar. Eğer http ile bağlantı kurulmuş ise bu paketlerin e-posta olarak değerlendirilmemesini sağlar. Birim **Segmenttir**.
6. **Sunum Katmanı(Presentation Layer):** Gönderici ve alıcının Veri biçimlerini dönüştürür. Aynı zamanda kripto lama yapar. Veri sıkıştırma çevirme ve şifreleme yapar. (Translation)
7. **Uygulama Katmanı(Application Layer):** Uzak bir sistem tarafından sağlanan program isteklerinin karşılanması için gerekli program taleplerini karşılar. (Ftp,Nfs, Mhs, Netware Requester, bUygulama Protokolleri ve Programlar)

4.5 OSI Modeli Nasıl Çalışır

Bu katmanların nasıl çalıştığını bir örnek üzerinde açıklayalım. Bir kelime işlem programı kullanıldığını ve bu programın resume.txt adındaki dosyayı uzaktaki sunucunun home katalogundan almak istediğini varsayalım.Bu durumda işlem adımları aşağıdaki şekilde olacaktır.

- Uygulama katmanı bir istek ile resume.txt dosyasının istendiğini analar ve sunun katmanına bunu iletir.
- Sunum katmanı bu isteğin kriptolu olup olmadığını ve bir veri tipi dönüşümü olup olmadığını belirler. İhtiyacı olan bilgiyi ekleyerek paketi oturum katmanına iletir.
- Oturum katmanı, dosyanın getirilmesi için hangi uygulamanın ve uzak sistemin hangi servisinin kullanılacağına karar verir. Uzak sistemin servis bilgisini ekleyerek paketi iletim katmanına gönderir.
- İletim katmanı uzak sistem ile garantili bir bağlantının olmasını ve eğer birden fazla çerçeve gerekli ise paketi çerçevelere ayırma işlemine hazırlar. Çerçevelere sıra numarasını ekleyip ağ katmanına iletir.
- Ağ katmanı aldığı çerçeveye kendi ve diğer sistem adreslerini ekler ve veri bağlantı katmanına iletir.
- Veri bağlantı katmanı, blokları bağımsız çerçevelere ayırır. Ethernet paketlerinin başlık kısımlarına MAC adreslerini yerleştirir. Çerçevenin sonuna denetim dizisini koyar. Topolojinin yapısına göre bu düzenlemeyi yapar.
- Fiziksel katman veriyi kaynaktan hedef sisteme sayısal darbeler halinde iletir.

4.6 Diğer sistemde verinin alınması

- Uzak sistemdeki Veri bağlantı Katmanı iletilen çerçeveyi okur. Varış adresinin kendisi olup olmadığına bakar. Eğer kendisi ise CRC denetimini yaparak uygun ise Network katmanına transfer eder.

- Network katmanı çerçeveyi analiz ederek varış adresinin kendisi olduğunu anlar. Bu analizden sonra bu seviyedeki bilgiyi ayırır ve kalanı iletim katmanına gönderir.
- İletim Katmanı, kaynak sistem tarafından kaydedilen bilgiyi analiz ederek,bir sıra numarası bulursa veriyi kuyruğa atarak, bütün bilginin tamamlanmasını bekler. Eğer alınamayan veri var ise sıra numarasını kullanarak kaynak sistemin yeniden göndermesini sağlar. Daha sonra veriyi oturum katmanına iletir.
- Oturum katmanı alınan veriyi alır ve geçerli bir bağlantıdan geldiğini kontrol eder. Daha sonra sunum katmanına iletir.
- Sunum katmanı alınan verideki dönüşüm ve çözümleme işlemini yaparak, sunum katmanı bilgisini ayırır ve uygulama katmanına iletir.
- Uygulama katmanı sistemde çalışan doğru sürecin işlem yapmasını garanti eder.Bu bir dosya isteği olduğu için dosya erişiminde sorumlu olan sürece görevi devreder.

4.7 Yönlendiriciler

Yönlendiriciler, IP dünyasında gateway olarak adlandırılır ve mantıksal ağları birbirine bağlamakta kullanılırlar. Yönlendiricilerin her iki tarafında da tek ağ adresi olması gerekir. Bu nedenle sistemler her iki tarafta bulunan mantıksal ağların ne olduğunu öğrenmelidirler. Bunu ise yönlendirme tabloları ile yaparlar. Yönlendirme tabloları,ya bilginin gideceği yolu tanımlayan statik olarak programlanır yada, özel olarak kullanılan ve bilgileri bilinen ağlar arasında aktaran bir dinamik yönlendirme protokolü kullanırlar.

4.7.1 Yönlendirme Tabloları

Yönlendirme tabloları bir yol haritası gibi düşünülebilir. Bir yol haritası şehirler arasındaki bütün yolları gösterdiği gibi yönlendirme tabloları da benzer olarak düşünülebilir. Bir ağdan diğerine üç türlü yönlendirme bilgisinin olması mümkündür.

4.7.1.1 Statik Yönlendirme

Statik yönlendirme tabloları en basit yöntemdir. Çoğunlukla IP ağlarda özel ağı belirten bir gösterici olarak tanımlanır. Yönlendirme bilgisini değiştirme ihtiyacını hissetmez. Ancak statik yönlendirme tablolarının kolay kullanımı yanında sabit yol tanımlamasından dolayı, arıza durumlarında kendisini güncellemez ve optimum yol uzunluğunu kullanmaz. Bunun yerine dinamik yönlendirme için uzaklık vektörü veya bağlantı durumu yönlendirme tabloları kullanılır.

Statik yönlendirme tabloları yüksek seviyede güvenlik sağlar. Aynı zamanda kendi yönlendirme tablolarınızı belirlediğiniz için en güvenli yöntemdir.Dinamik yönlendirme, tabloları dinamik olarak güncellediği için, saldırgan, yönlendiriciye yanlış yönlendirme bilgisi vererek ağın fonksiyonunu yapmasını engeller. Her bir taraftaki yönlendirici kendi yönlendirme tablosunu korumakla yükümlüdür. Bu yüzden eğer, bir saldırı olurda yönlendirici etkisiz kalırsa, diğer yönlendiriciler bundan etkilenmezler.

4.7.1.2 Mesafe Vektörü Yönlendirme(Distance Vector Routing)

Mesafe vektörü yönlendirme en eski ve en popüler yönlendirme tablosu oluşturma yöntemidir.Yönlendirme Bilgisi Protokolü(RIP) öncelikle kullanılan dinamik yönlendirme protokolüdür. Bu tip yönlendiriciler kendi yönlendirme tablolarını , bağlı oldukları yönlendiricilere bakarak dinamik şekilde oluştururlar. Her bir yönlendirici için hop değerine bir eklerler. Mesafe vektörü ile her bir yönlendirici kendi yönlendirme tablosunu dakikada bir kere güncelleme yapacaktır.
Bu yöntemde her bir yönlendirici diğer ağlara ulaşmak için hop sayma bilgisini yakınındaki yönlendiricilerden alacaktır. Ancak aldığı bu bilgiler her zaman gerçeği yansıtmayabilir. Bu nedenle bazı durumlarda yanlış yönlendirme ve hop sayma bilgisi oluşabilir.

Yönlendirme bilgisi ikinci el bilgi olduğu için bu bilginin doğruluğu hiçbir zaman kanıtlanamayacaktır.Bu ise bir güvenlik açığı anlamına gelmektedir. Dolayısı ile çoğu kuruluş statik yönlendirme tablosu veya, bağlantı durumu protokolü kullanır.

4.7.1.3 Bağlantı Durumu Yönlendirme(Link State Routing)

Bağlantı durumlu yönlendiriciler, birkaç önemli fark dışında mesafe vektörüne benzer fonksiyon yaparlar. Bu yönlendiriciler öncelikle tabloları güncellerken birinci el bilgiler kullanırlar. Bu sadece yönlendirme hatalarını elimine etmez, buluşma zamanını azaltarak sıfıra yaklaştırır.

Bağlantı durumu yönlendirmede, Yönlendirici A açıldığı zaman, bir RIP paketi olarak *hello* mesajı gönderir. Bu mesaj her porttan gönderilir. A yönlendiricisi B ve C'den cevap aldığında bir bağlantı kurulur. Bu bağlantı aşağıdaki bilgileri içerir.

- Yönlendiricinin adı veya kimliği
- Bağlı olduğu ağ'lar
- Her bir ağa erişim için gerekli hop sayısı veya maliyet
- Onun *hello* çerçevesine cevap veren her ağdaki diğer yönlendiriciler

Yönlendirici A'nın *Hello* mesajını alan diğer yönlendiriciler bu mesajı diğer yönlendiricilere kopyalarlar. Böylece ağdaki her aktif yönlendiricini cevabı A' ya gelerek bir bağlantı kurulur.

Bağlantı durumlu ağ faal olarak çalışırken, B ve C yönlendiricileri yeniden yönlendirme tablolarını oluşturmak yerine , A'dan bir bölüm kopyalarlar. Böylece zamandan tasarruf edilmiş olur.

Eğer C yönlendiricisi normal olarak kapatılırsa, B' ye bir çerçeve gönderir. Bunun üzerine B, kendi tablosundan C'nin bilgisini siler ve A'yada bu bilgiyi gönderir. Eğer C arızalanır ise, B'nin bunu anlaması için bir gecikme olur. Bundan sonra B tablosundan C' yi siler ve durumu A' ya bildirir. Her bir yönlendiricinin yönlendirme tabloları doğru ve şebekemiz güncelleme için minimum zaman gerektirir. Bağlantı durumunun maksimum büyüklüğü 127 olabilir.

Çoğu bağlantı durumlu yönlendirme protokolü, dinamik yönlendirme güncellemenin yapacağı kaynak için bir yetkilendirme seviyesi sağlar. Böylece bir şifre ve kullanıcı adı ile yönlendirme protokolü daha güvenli hale gelir.

4.8 Bağlantısız ve Bağlantı kaynaklı Haberleşmeler

A noktasından B noktasına veri iletilirken, sistemlerin aynı mantıksal ağ da olmasına bakılmaz. Ancak veri iletilirken iletim katmanında iletim ile ilgili kurallar uygulanır. Bu kapsamda iki türlü ağ iletişim kuralı vardır.

4.8.1 Bağlantı temelli İletişim.:

Bağlantı temelli iletişimde, veri iletiminden önce el sıkışma denilen kontrol bilgileri iletilir. Ulaştırma katmanı bu el sıkışma bilgilerinden varış sisteminin bilgi almaya hazır olduğunu anlar. Bağlantı esaslı değişim aynı zamanda verinin orijinal sırasında gönderilip alındığını sağlar. Bu işlem IP' de iletim katmanında bir bayrak ile gösterilir. IPX' de bağlantı kontrol alanı ile gösterilir.

Bağlantı temelli haberleşme için TCP' deki üç fazlı yapı daha önce anlatılmıştı. Ancak biraz bulanık olan bu yapıyı daha iyi açıklayabilmek için aşağıdaki örnek uygundur.
Bir arkadaşınızı cumartesi akşamında ağ sallanma partisine davet edecek ve diz üstü bilgisayarı ile gelmesini isteyeceksiniz.

- Arkadaşınızın telefon numarasını çevirin(SYN=1,ACK=0)
- Arkadaşınız telefona cevap verir ve "Merhaba" der(SYN=1,ACK=1)
- Merhaba Ahmet, ben Mehmet diyerek cevap verirsiniz(SYN=0, ACK=1)

Daha sonra parti ile ilgili bilgileri Mehmet'e aktarırsınız. Konuşma bittikten sonra, vedalaşıp bağlantıyı sonlandırırsınız.
Bağlantı esaslı iletişimin amacı, güvenli haberleşme sağlamaktır.

4.8.2 Bağlantısız İletişim(Connectionless Communication):

Bağlantısız iletişim, başlangıçta el sıkışmaya ihtiyaç duymaz. Bu iletişimde en iyi performans sağlanır, ancak katmanların kararlılığı önemlidir. NFS oturumu bu tip haberleşmeye örnektir. Bu yapıdaki haberleşmeye örnek olarak yine cumartesi günkü partiye davet edeceğimiz arkadaşımızın durumuna bakalım.
Arkadaşımızı partiye çağırmak için telefon ile aradık. Ancak kendisi yerine bilgisayarı cevap verir ve partinin yeri zamanı hakkında detaylı mesaj bırakırsınız. Ancak bundan sonra arkadaşınız ile ilgili aşağıdaki durumlara bağlı olacaksınız.
Çevirdiğiniz telefon numarasının doğru olup olmadığı
Telefon şirketinin sizin mesajınızın yarısında telefon bağlantısını düşürmesi
Cevap makinasının bırakılan mesajı doğru kaydedip etmediği
Arkadaşınızın kedisinin telefon ile iplik topu arasındaki farkı ayırt edebilme yeteneği
Güç bozulmasının olup olmadığı
Arkadaşınızın bu mesajı parti saatinden önce alıp almadığı
Görüleceği gibi bu mesajların hiç birinin tam doğrusu bulunmaktadır.:

Bu yöntemlerden hangisi daha iyidir? Sorusunun tam bir cevabı bulunmamaktadır. Bunu uygulama katmanı belirler. Eğer Telnet TCP isterse bunu UDP yapamazsınız.

Güvelik önlemleri bağlantı tabanlı servisler ister. Örneğin Güvenlik duvarları bağlantı tabanlı servislerdir. Bağlantının özelliğine göre onu kabul veya ret eder.
Örneğin içerdeki kullanıcılar Internet'e çıkacak, fakat dışarıdan içeriye ulaşılamayacak şeklinde bir politika belirlenirse bu nasıl gerçekleştirilecektir.

Bu işlem TCP protokolündeki bayrak ile yapılabilir. TCP protokolünde herhangi bir harici kullanıcının içeriye bağlantı yapması önlenir. TCP' deki SYN bayrağı1 yapılıp diğer bütün bayraklar 0 olarak el sıkışma sırasında ayarlanır. Bu sırada bağlantı önlenirse, kullanıcının içeriden veri alıp göndermesi de önlenmiş olur.

4.9 Ağ Servisleri

Servis, karşı sistemde çalışan bir süreç olup, ağ kullanıcısına bazı hizmetler sağlar. E- posta , dosya ve yazıcı paylaşım gibi. Servislere özel port ve soketler ile ulaşılır.Port, sistemdeki sanal bir posta dilimidir. Her bir servis için ayrı bir port numarası tasarlanır. Kullanıcı bir servise erişmek istediği zaman oturum katmanı bunun için doğru port numarasını sağlamaktan sorumludur. Internet'te standart hale gelmiş bazı servisler vardır. Bunların dışında, firmaların kendilerine özel servisleri de olabilir. Bu bölümde çokça karşılaşılan standart servisler anlatılacaktır. Bu servislerin her birinin kendilerine özgün güvenlik delikleri vardır.

4.9.1 FTP

Internet üzerinden dosya transferi sağlayan bir servistir. File Transfer Protocol (FTP), bu amaçla kullanılan standart bir protokoldür.Kullandığı port numarası 20,21 dir.

Dosya transferinde güvenliğin sağlanabilmesi için, dışarıdaki bir FTP sunucusuna bağlanan kullanıcının yüklediği dosyanın içeriğinin kontrol edilmesi ve yerel FTP sunucuya bağlanan kullanıcıların, sistemin diğer kısımlarına ulaşmalarının engellenmesi gerekmektedir.

Web browser üzerinden kullanılan pasif ftp 21 nolu port ile haberleşir.

Dosya transferi ile ilgili olarak kullanılan diğer protokoller;

1. TFTP (Trival File Transfer Protocol)
2. UUCP (Unix To Unix Copy)
3. FSP (File Service Protocol)
4. rpc

4.9.2 DHCP(Dynamic Host Configuration Protocol)

Ağdaki host lara IP adresi vermek için üç ad yöntem vardır..
Manuel : Kullanıcı manuel olarak herbir host'u konfigüre eder.
Otomatik : Bir sunumcu , hostun çalışmaya başlatılması esnasında otomatik olarak Ip adresi verir.
Dinamik : Bir sunucu hostun çalışmaya başlaması sırasında dinamik olarak bir IP havuzundan adres atar.
DHCP otomatik ve dinamik adres atamasını destekler. Ancak dinamik adres atanması, ağ broadcast trafiğini artırması ve sunumcunun devre dışı kalması gibi dezavantajları vardır.

4.9.3 DNS

Domain Name Server (DNS), bilgisayar isimlerini IP adresine dönüştüren servistir. Kullanıcılar doğudan kullanmazlar. SMTP, FTP ve Telnet gibi servisler tarafından kullanılır. Hiyerarşik bir yapısı vardır.

4.9.4 HTTP

HTTP, web tarayıcı ve Web sunumcu arasında haberleşir. Genellikle 80 no'lu portu kullanır. World Wide Web (www) tamamen internet için geliştirilmiş bir servistir. SMTP, FTP, telnet, usenet gibi standart servisleri de kullanarak HHTP servisi üzerine inşa edilmiştir.

www, HHTP sunucularının bir araya gelmesiyle oluşmaktadır. HTTP, kullanıcıların www üzerinde yer alan dosyalara ulaşmasını sağlamaktadır. HHTP protokolü detaylı olarak ele alınacaktır.

www çok fazla servisi içermesi esnek olarak tasarlanmış olmasından kaynaklanmaktadır. Çok fazla servisi sunabilmesi aynı zamanda, bu servislerin de güvenlik problemlerini taşıması anlamına gelmektedir.

4.9.5 POP(Post Office Protokolü)

POP tipik olarak bir UNIX shell hesabından posta almak için kullanılır.POP3 ile kullanıcı POP sunumcuya, hem uzaktan görülmesi için posta bırakabilir(online posta) hemde,kendi sistemine postaları alıp görebilir(ofline posta).

4.9.6 IMAP4(Internet Message Access Protocol, version 4)

IMAP POP'nun geliştirilmesiyle elde edilmiştir.POP nin özelliklerini taşırken ilave bazı özellikleri de vardır.

4.9.7 NFS

Bazı protokoller vasıtasıyla başka bilgisayarlar üzerindeki sabit sürücüdeki dosyalara ulaşmak mümkündür. Network File System(NFS), bu tür hizmet verilebilecek bir servistir. Bu servis, kendisine ulaşan bilgisayarlara güvendiğinden herhangi bir kullanıcı tanıma mekanizması kullanmaz. Bu nedenle de güvenlik konusunda dikkatli olmak gerekir. Özellikle internet üzerinden bu servis verilecekse, değişik güvenlik sistemleriyle birlikte kullanılması gerekmektedir.

Aynı işlevi yerine getiren başka bir serviste Andrew File System (AFS) dir. Bu servisin kullanıcı tanıma mekanizması ve eğer isteniyorsa bilgilerin aktarımında şifreleme işlemine imkan vermesi, NFS'e göre avantajlı duruma sokmaktadır.

4.9.8 NNTP(Network News Transfer Protocol)

NNTP haberleri ağ üzerinde dağıtmak amacıyla kullanılır.

4.9.9 SMTP

Simple Mail Transfer Protokol (SMTP), elektronik mektup göndermek ve almak için kullanılan standart bir protokoldür.
Elektronik posta en popüler servislerdendir. Bu servisle ilgili güvenlik problemleri bulunmaktadır. Çok karmaşık olmasa da posta yoluyla virüs gelebilmektedir.

4.9.10 SNMP(Simple Network ManagementProtocol)

SNMP, ağ elemanlarını görüntülemek ve denetlemek için kullanılır. Kontrol ve denetleme istasyonuna SNMP yönetim istasyonu denir. Ağ elemanlarının denetimi için SNMP etmenlerinin çalışması gerekir.

4.9.11 Telnet, rlogin, rsh

Bu servisler uzak bir sisteme bağlanmayı sağlar. Sisteme doğrudan bağlı bir terminal gibi çalışmanızı sağlayan bir servistir.
Telnet, uzaktaki sistemlere bağlanma servisi olarak, standart hale gelmiş çok kullanılan bir protokoldür. Kullanıcıların sisteme bağlanabilmeleri için kullanıcı adı ve parolası istediği için güvenli sayılabilir. Fakat, sunucu ile istemci arasındaki iletişim açık olarak yapılmaktadır. Hattı dinleyen birisi kullanıcı adı ve parolası başta olmak üzere ne tür işlemler gerçekleştirildiğini gözleyebilir. Bu güvenlik açısından büyük bir problemdir.
rlogin ve rsh uzak sistemlere erişim ve komut yürütme işlemlerini sağlayacak diğer servislerdir. Güvenlik önemli olduğunda internet üzerinden bu servislerin kullanımı oldukça zordur.

4.9.12 Usenet News

SMTP bire bir ya da birden çoğa haberleşme sunarken, usenet news çokça çok bir haberleşme ortamını sağlayan bir servistir. Haber gruplarından yararlanmak için kullanılır. Haber grupları, sayıları çok fazla olan kullanıcıların, her kullanıcının yazdığı mektubu birlikte okuyabilmeyi sağlayan bir servistir.

Bu servisle ilgili olarak karşılaşılabilecek güvenlik sorunları, elektronik posta için geçerli olanlar burada da geçerlidir.

4.9.13 Bilgi tabanlı diğer servisler

Internet üzerinde bilgi temelli olan www dışındaki diğer servisler arasında şunlar da sayılabilir.

- Gopher
- WAIS
- Archie

Gopher, karakter tabanlı ve menüler şeklinde dizayn edilmiş, internet üzerinde bilgi araştırmasına yardım eden bir servistir.

Wide Area Information Service (WAIS), kullanıcının vereceği anahtar kelimeleri kullanarak internet üzerinde sorgulama yapan ve bu anahtar kelimelerin bulunduğu sayfaları kullanıcıya bir liste olarak sunan servistir.

Archi, verilen bir dosya veya dizin adını, genel kullanıma açık ftp sunucularında arayan bir servistir. Özel istemci Archie programlarının yanında bu servisten yararlanmak için Telnet veya elektronik posta da kullanılabilir.

5 TOPOLOJİ GÜVENLİĞİ(Toplogy Security)

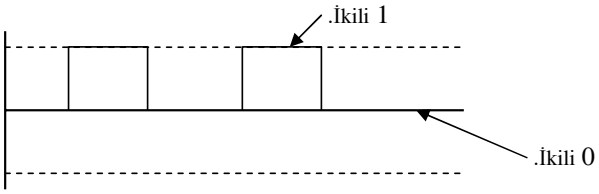
5.1 Ağ iletiminin anlaşılması

Sayısal İletişim

Sayısal iletişim, ,ilk olarak telgraf ta kullanılan mors koduna benzerdir.Değişik karakterleri temsil etmek üzere farklı darbe dizileri kullanılır. İkili sistemde iletilen bu bilgilerin yapısı şekil 5.1'de gösterilmiştir

Gürültülü iletişim de darbelerin şekilleri bozulacaktır. Buna rağmen sayısal iletişim analog iletişimden daha verimlidir. Çünkü analog iletişimde gürültüyü ayırt etmek için daha fazla işlem yapmak gereklidir. Ancak iletişimde bu gerilim seviyeleri değiştiği için bir başka problem ortaya çıkar, bu da elektromanyetik gürültüdür.

Silinmiş: <sp>



Şekil-5.1 Sayısal veri iletimi

Elektromanyetik Parazit

Elektromanyetik gürültüyü değişken akım taşıyan iletişim devreleri üretir. Eğer bu manyetik alan bir iletken tarafından kesilirse, bu iletkende alanın gücü ile orantılı bir elektriksel işaret indüklenir. Ayrıca üretilen bu alan dinlenir ise iletim devresinden geçen elektriksel işaret aynı şekilde elde edilmiş olur. Böylece hat dinleme ile bilgiler elde edilebilir. Çoğunlukla fiyatının düşük olması nedeniyle haberleşme hatlarında ekransız bükülü kablo kullanılır.(Unshilded Twisted pair) EMI açısından güvensiz bir iletişim hattı elde edilmiş olur. Eğer güvenli bir iletişim isteniyor ise bu kabloların üreteceği EMI minimum olacak şekilde tesis edilmelidir.

5.1.1 Fiber Optik Kablo

Fiber optik kablo teknolojisi ile bilgi ışığa çevrilerek iletilir. Bu sayede:EMI üretmez ve bundan etkilenmez. Ayrıca iletim bat genişliği bakır iletkene göre fazladır.

5.1.2 Sınırlı ve Sınırsız iletişim ortamları

Atmosfer sınırsız iletişim ortamıdır ve haberleşme devresinin sınırları belirli değildir. İşaret belirli bir yoldan gitmeye zorlanmaz. Bükülü çift bakır kablo ve fiber optik kablo, işaret kablodan gitmeye zorlandığı için sınırlı iletişim ortamına örnektir..Sınırsız ortamın bu niteliği nedeniyle güvenlik problemlerini beraberinde getirir. Atmosfer değişik tipte işareti iletime yeteneğine sahiptir.

5.1.3 Işık iletimi

Atmosferden Işık iletimi, ağ işaretlerini gönderip almak için lazer kullanır.Bu cihazlar cam ortamsız olan fiber kablo gibi çalışır. Atmosfer ışığı iletmede bazı sınırlamalar getirir. (mesafe gibi) Sınırsız ışık iletimi çevresel koşullara karşı duyarlıdır. Yoğun sis ve kar yağışı gibi olaylar iletimi etkiler.

5.1.4 Radyo Dalgaları

Ağ iletişimi amacıyla kullanılan radyo dalgaları, tipik olarak 1-20 Ghz aralığında mikrodalga işaretleri olarak adlandırılır. Sabit frekansta olan işaret taşıyıcı olarak kullanılır. Bu taşıyıcının frekansı modüle edilerek veriler iletilir. Diğer tarafta demodüle edilir. Eğer , taşıyıcının frekansı aralıklı olarak değiştirilirse, yayılmış frekanstaki işaretler taşıyıcı olarak kullanılmış olur. Bu yöntem ile bilginin başkalarının eline geçmesi önlenmiş olur.

Bu iletişim ya karaya yerleştirilen iletim kuleleri üzerinden veya uydu aracılığı ile yapılır. Karadaki bağlantı birimlerinin bazı sınırlamalarını ortadan kaldıran uydu teknolojisi elbette daha geniş aralıkta haberleşmeyi sağlayacaktır.

5.1.5 İletim ortamının Seçimi

Ağ iletimi için ortam seçilirken bir seri güvenlik konusunu düşünmek gereklidir. Bunun için aşağıdaki hususlar göz önüne alınmalıdır.

- Datamız ne kadar değerlidir.
- Hassas veriyi hangi ağ dilimleri taşıyacaktır.
- Yabancını haberi olacak mı
- Omurga dilimleri ne erişilebilir mi ?

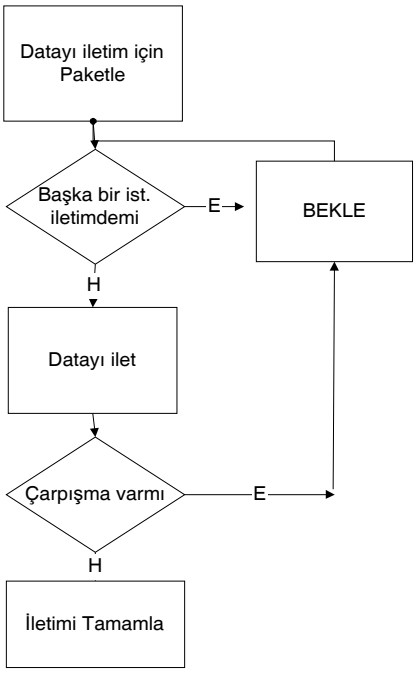
5.2 Topoloji Güvenliği

Buraya kadar iletim ortamının özellikleri açıklandı. Bundan sonra bu ortamın ağ olarak çalışması için nasıl konfigüre edildiği üzerinde durulacaktır. Topoloji, ağ ortamındaki fiziksel bağlantı ve iletişim için kuralları tanımlar.Her topoloji iletişim ve konuşma için kendi kurallarını ayarlar.

5.2.1 Ethernet İletişimi

Daha önce Ethernet çerçevesinin içerdiği verinin yapısı incelenmişti. Şimdi ethernetin bilgiyi nasıl bir sistemden diğerine ilettiği üzerinde durulacaktır.
Ethernet en popüler yerel ağ topolojisidir. Değişik kablo türleriyle çalışabilmesi,düşük maliyetli donanım ve tak çalıştır özelliği onu diğer topolojilere göre daha üstün hale getirmiştir. Ethernetin haberleşme protokolü CSMA/CD(Carrier Sense Multiple Access/ Collision Detect) dir. Algoritması Şekil-5.2'de gösterilen bu protokolün açıklaması aşağıda verilmiştir.

Taşıyıcı Anlama(Carrier Sense): Ethernette her bir istasyon, bir iletim olup olmadığını anlamak için hattı dinler. Bunun anlamı her bir istasyon hattı gözleyebilmektedir. Bunun nedeni hattın boş olduğu bir anda veri göndermektir.
Çoklu Erişim(Multiple Access): Basitçe birden fazla istasyonun aynı ağa bağlanmasıdır. Bu yapıda ağ istasyonlar tarafından paylaşılarak veri iletiminde kullanılır. Ayrıca ilave istasyon kolayca bu yapıya eklenebilir.
Çarpışma Bulma(Collision Detection): Eğer iki istasyon aynı anda veri göndermiş ise ne olduğunun anlaşılmasıdır. Eğer gönderilen veriler ağ üzerinde karşılaşmış ise çarpışma olacak, dolayısı ile veriler bozulacaktır.
Ethernetin yukarıda belirtilen özelliğinden dolayı, güvenliği zayıf olan bir topolojidir. Çünkü ağdaki her istasyon ağı dinleyebildiği için iletilen verileri elde edebilir. Bunu önlemek için ağ segmentlere bölünür. Segmentlere ayırma işlemi köprü, anahtar veya yönlendiriciler ile yapılır.



Şekil-5.2 Ethernet CSMA/CD protokolünün çalışma algoritması

5.3 Geniş Alan Ağ Topolojileri

Geniş alan ağa topolojileri, yerel alan topolojilerinin aksine veriyi uzak mesafelere taşımak amacıyla tasarlanır. Çoğunlukla noktadan noktaya iletim olarak kurulur. Eğer çoklu noktaya iletişim gerekiyor ise iletilen düğümün arkasına yerel alan şebekesi kurulur.

5.3.1 Özel Devre Topolojileri

Kiralık devreler iki düğüm arasında analog veya sayısal iletişim amacıyla kurulurlar.Hızları klasik kiralık devrede 56 Kbps iken, TDM(Time division Multiplexing) sisteminde 64 Kbps'den 1.544 Mbps'e kadar olabilir. Bu topoloji daha güvenli bir yapı sağlar. Ancak saldırgan yinede devreyi dinleyerek görüntüleyebilir.

5.3.2 Frame Relay ve X.25

Frame Relay ve X.25 paket anahtarlamalı devreler olduğu için ağ, verileri herhangi bir devre üzerinden iletebilir. Eğer sürekli aynı devre üzerinden iletim istenirse PVC(Permanent Virtual Circuit) olarak ayarlanmalıdır. WAN ortamında frame relay, atanmış devreden daha verimlidir. Aynı WAN üzerinden çoklu PVC'ler tanımlanabilir.

Bağlantılar DLCI(Data Link Connection Identifier) kullanılarak FR//X.25 bulutu üzerinden tanımlanır. Her bir yönlendiricinin kendine ait tek bir DLCI' vardır. Herkes kendi DLCI'sini kullandığı sürece mutludur. Eğer birileri yanlışlıkla veya saldırı amacıyla kendi yönlendiricisine sizin DLCI'nizi atarsa aynı ağa girmiş olur. Bu işlemin gerçekleşmesi için aşağıdaki olayların olması gereklidir.

- Saldırgan aynı yerel değiştirme taşıyıcısına(local exchange carrier) bağlanmalıdır.
- Saldırgan aynı fiziksel anahtara bağlanmalıdır.
- Saldırgan sizin DLCI'nızı bilmelidir.

Anlaşılacağı gibi bunlar oldukça zor gerçekleşecek olaylardır.

5.4 Temel Ağ Donanımı

Ağdaki güvenlik ihlallerini iyi analiz etmek için temel bağlantı elemanlarının çalışmasının bilinmesi gereklidir. Bu elemanlar Tekrarlayıcılar(Repeaters), Hublar, Köprüler(Bridges), Anahtarlar(Switches), Yönlendiriciler(routers) dir.

5.4.1 Tekrarlayıcılar(Repeaters),

Tekrarlayıcılar basit işaret kuvvetlendiricilerdir. Fiziksel düz kanal topolojisinde mesafeyi artırmak için kullanılırlar. Herhangi bir veri segmentleme yapmazlar, sadece veriyi bir taraftan diğerine iletirler.

5.4.2 Hublar(hubs)

Yıldız topolojisinde bükülü çift kabloyu destekleyen çok portlu tekrarlayıcı olarak çalışırlar. Her Bir port işareti diğer bütün portlara kuvvetlendirerek gönderir. Tekrarlayıcıda olduğu gibi hublarda elektrik seviyesinde çalışırlar. Ağ trafiğini kontrol etmezler.

5.4.3 Köprüler(Bridges)

Köprüler, iki ağ segmentini birbirine bağlarlar. Segmentler arasında tekrarlayıcı gibi çalışırlar. Ancak, MAC adres seviyesinde yönlendirme yaparlar. Segmentleri çarpışma(collision) alanlarına ayırırlar. Bir bakıma MAC adres seviyesinde yönlendirici gibi çalışırlar. Bu işlemi MAC adreslerine göre düzenlenmiş olan yönlendirme tabloları ile yaparlar.

Ağı iki çarpışma alanına ayırmak güvenliği artıran bir yöntemdir. Çünkü her çarpışma bölgesi kendi alanındaki trafiği dinleyerek iletişim yapar.

5.4.4 Anahtarlar(Switches)

Anahtarlar hub ve köprü teknolojilerinin evliliğidir. Hub gibi RJ45 portu ile ethernet kartlarına bağlanır. Her port bir tekrarlayıcı ve köprü özelliğini taşır. Gelen trafiği, varış adresine göre yönlendirir. Bu teknoloji ile ağdaki performans artırıldığı gibi güvenlik de artırılmış olur.Eğer herhangi bir sistemin güvenliğini tehdit eden bir husus var ise ancak kendi oturumu sırasında onu dinleyebilir. Bu özelliğinden dolayı bütün ağ'ı izlemek için bir monitör portu bulunur. Bu port, hub benzeri olarak bütün ağ trafiğini kopyasını içerir. Eğer, bir saldırgan bu porta ulaşırsa ağı dinleyebilir. Köprü ve anahtarlar ağ performansını geliştirmek amacıyla tasarlanmış elemanlardır.

5.4.5 VLAN Teknolojisi

Anahtarlama teknolojisi sanal LAN oluşturmayı mümkün hale getirmiştir. Anahtarların portları kendi aralarında gruplandırılarak sanal LAN'lar oluşturulabilir. Böylece elde edilen sanal LAN lar arasında iletişim sağlanır. Ancak bu yöntemin güvenlik açısından bazı sakıncaları vardır. Eğer bir saldırgan anahtarı ele geçirirse(Yönlendiriciden daha kolay olur.) kendini her hangi bir VLAN!ın görüntüleme portuna bağlayıp ağı gözleyebilirler.

5.5 Yönlendiriciler(Routers)

Yönlendiriciler çok portlu olan ve OSI katman 3(Ağ katmanı)'da ağ adresine göre veriyi portları arasında transfer eden cihazlardır. Çalışırken veriyi protokol ve topoloji özelliğine göre ilettiği için protokol bağımlı ağ cihazı olarak bilinirler. Bu nedenle ileteceği protokollerin önceden yönlendiriciye belirtilmesi gereklidir. Ayrıca portlarına gelen ve varış MAC adresi ff olan broadcast mesajlarını iletmedikleri için ağı alt ağlara bölmekte ideal elemanlardır.

Bazı yönlendiriciler IP seviyesinde paket filtreleme yapabilirler. Bu şekliyle firewall gibi ağ trafiğini kontrol edebilir. Yönlendiriciler ile anahtarlayıcıların birbirlerine göre özelliklerinin karşılaştırılması Tablo-5.1'de verilmiştir.

Köprü(Switch) Özelliği	Yönlendirici(router) Özelliği
Bütün portlar aynı ağ adresini kullanırlar	Her bir portun ağ adresi farklıdır.
Yönlendirme tablosu MAC adrese göre düzenlenir.	Yönlendirme tablosu Ağ adresine(IP) göre düzenlenir.
Trafik MAC bilgisine göre filtrelenir	Trafik ağ veya host bilgisine göre filtrelenir.
Broadcast trafiğini iletir.	Broadcast trafiğini iletmez.
Trafiği bilinmeyen adrese iletir	Trafiği bilinmeyen adrese iletmez
Çerçeveyi düzenlemez	Çerçeveye yeni başlık ve son bilgisi ekler
Çerçeve başlığına göre trafiği iletir	Trafiği iletmeden önce kuyruğa koyar

Tablo5-1 Köprü ve Yönlendiricinin Karşılaştırılması

5.5.1 Katman 3 'te anahtarlama

Buraya kadar anahtar ile yönlendirici arasındaki fark açıklandı. Ancak Anahtarlamalı yönlendirme (Switching Router) veya katman3'te anahtarlama kavramı son yıllarda çok kullanılan bir terim olup üzerinde durulması gereklidir. Katman3 anahtarlama, anahtar yönlendirici veya Yönlendirici anahtar aynı cihazın isimleridir.

Bu cihaz tipik olarak bir yönlendiricinin fonksiyonunu yapar. Bir veri çerçevesi alındığı zaman tampon belleğe koyulur,ve CRC testi yapılır. Sonra protokol özelliği çerçeveden alınır. Klasik yönlendiricide olduğu gibi yönlendirme tablosuna göre iletim yapar. Klasik yönlendiriciden farkı sorusunun cevabı ise cihazın başlığındadır Veri işleme ASIC bir donanım tarafından yapılır. Standart yönlendiricide, bütün işlemler tekbir RISC işlemcide yapılır. Oysa, anahtar yönlendiricide, yönlendirme sürecindeki özel işlerin her birini yapmak için sabit elemanlar vardır. Bu ise performansı artıran bir faktördür. Ancak bu husus güvenlik açısından o kadar iyi bir durum olmayabilir. Elbette performans, kazaen geçen trafiğin engellenmesi ile ilgilenmez. Anahtar yönlendiricinin hedefi performansı artırmak olduğu için, iletilen veriler hakkında klasik yönlendiriciler gibi kılı kırk yaran bir yapısı yoktur.

Bu nedenle eğer anahtar yönlendirici kullanılan bir ağın yöneticisi iseniz güvenlik politikası daha titiz hazırlanmalıdır. Ancak standart anahtarlara göre daha iyi bir güvenlik sağlayacağı kesindir.

5.5.2 Katman 4 'te anahtarlama

Katman 4 OSI Modelinin İletim (Taransport) katmanıdır. İletim katmanı kaynak ile varış arasında uçtan uca haberleşmeden ve kaynak ile varış arasındaki koordinasyondan sorumludur Bu katmanda TCP(Transmission Control Protocol) ve UDP (User Datagram Protocol) gibi IP protokolleri yer alır. Katman 4'te TCP ve UDP başlıkları uygulama protokollerini(HTTP, SMTP, FTP, vs.) belirten port numaralarını içerir. Uç sistem bu bilgiyi paketteki veriyi yorumlamakta kullanır, bir anlamada port numarası alınmış olan IP paketinin tipini ve hangi üst katman yazılımına transfer edileceğini belirler.Port numarası ve cihazın IP numarası kombinasyonuna çoğunlukla ***soket*** denilir.

Port numaraları 1- 255 arasında olur ve iyi-bilinen numaraları bu aralıktadır. Tablo5.2 örnek port numaralarını gösterir..Bu katmanda yönlendirme MAC adrese göre yönlendirmeye benzer.

Uygulama Protokolü	Port Numarası
FTP	20 (data) 21 (control)
TELNET	23
SMTP	25
HTTP	80
NNTP	119
SNMP	161 162 (SNMP traps)

Tablo-5.2: İyi Bilinen Port Numaraları

6 KRİPTOSİSTEMLER VE SİMETRİK ŞİFRELEME/DEŞİFRELEME(Cryptosystems and Symmetric Encryption/Decryption)

Kimlik doğrulama ve şifreleme, verinin emniyetini sağlamaya yarayan birbiriyle bağlantılı iki teknolojidir. Kimlik doğrulama, haberleşmede her iki tarafta bulunanların ne söylüyorlar ise onun doğru olmasını sağlama sürecidir. Şifreleme ise iletişim sırasında verinin hem güvenliğini sağlamak hem de değiştirilmesini önlemeye yönelik işlemlerdir.

6.1 Güvenliğin geliştirilmesi ihtiyacı.

1970'li yıllarda IP version4 Internet'te kullanılmaya başlanınca ağ güvenliği ön planda bir konu değildi. Bu nedenle IP, bütün veriyi açık metin şeklinde gönderir. Bunun anlamı, eğer gönderilen paketler dinlenirse hem içeriği öğrenilebilir hem de değiştirilebilir. Ağ analizi yapan bir uç noktadaki saldırgan bu analizler sonucunda, hem oturumları öğrenebilir, hemde veri paketlerinin içeriklerini değiştirebilir. Aşağıdaki protokoller açık metin(Clear text) ileten protokollerdir.

- FTP Doğrulama açık metindir.
- Telnet Doğrulama açık metindir
- SMTP posta mesajlarının içeriği açık metin olarak dağıtılır.
- http Sayfa içeriği ve formlardaki bilgilerin içeriği açık metin olarak gönderilir.
- IMAP Doğrulama açık metindir
- SNMPv1 Doğrulama açık metindir

6.2 Ağ Üzerinde Yapılan Saldırı Türleri

1. İfşaat(Disclosure) Mesaj içeriğinin herhangi birisine verilmesi veya Uygun kriptografik anahtara sahip olmama

2.Trafik Analizi: Ağdaki trafik akışının analiz edilmesi.Bağlantı esaslı uygulamalarda, bağlantının sıklığı ve süresi. belirlenebilir. Bağlantı esaslı veya bağlantısız ortamda, bağlantılardaki mesajların sayısı ve uzunluğu belirlenebilir.

3. Gerçeği gizleme (Masquerade) Hileli bir kaynaktan ağ'a mesaj ekleme. Bu işlem muhalif tarafından yetkili bir kullanıcıdan geliyormuş gibi görünen mesajların oluşturulmasını içerir.

4.İçerik Değiştirme(Content Modification): Ekleme, silme, sırasını değiştirme veya içeriğini değiştirme yöntemleriyle mesajın değiştirilmesi.

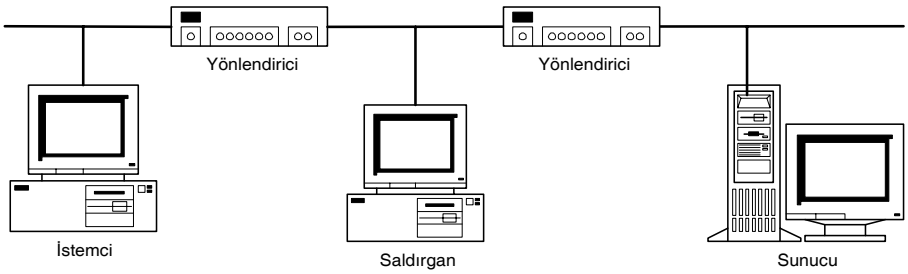
5.Sıra Değiştirme(Sequence Modification): Ekleme silme ve yeniden sıralama ile mesajın sırasında değişiklik yapma.

6.Zamanlamayı Değiştirme(Timing Modification): Mesajları geciktirme veya yeniden yollama. Bir bağlantı orijinli uygulamada bütün oturum veya mesajların bir kısmı ya önceki geçerli bir oturumun bir tekrarlanan sırası veya sıradaki kısmi mesajlar olarak geciktirilebilir veya tekrar gönderilir.

7.İnkarcılık (Repudiation): Alınan mesajın varış tarafından inkarı veya gönderilen mesajın kaynak tarafından inkarı.

6.3 İyi Doğrulama Gereklidir.

İyi doğrulama gerektiği açıktır. Açık metin olarak logon bilgisini ileten bir protokol ile sunucuya erişen bir istemcinin logon ve password bilgisini bir saldırgan elde edebilir. Bu ise saldırganın o birim yerine geçmesi demektir. İyi doğrulamanın bir başka sebebi bir servise erişen kaynak istemcinin veya sunumcunun doğrulanmasıdır. Aynı zamanda hostun iletişim oturumu sırasında değişmediğinden emin olunması gereklidir. Bu tip bir atağa oturum korsanlığı adı verilir.



Şekil 6.1. Oturum Korsanlığı

6.3.1 Oturum Korsanlığı

Şdkil 6.1'deki ağ üzerinde bir istemci, sunumcu ile haberleşme yapmaktadır. İstemci sunumcu tarafından doğrulanmış ve erşimi yönetici seviyesinde sağlanmıştır. Kendini istemci ile sunumcu arasındaki ağ segmentinde gizlemiş bir saldırgan oturumları gözlemleyebilir. Bu saldırgana haberleşme yapan uçların port numaraları ve sıra numaralarını öğrenme imkanı verir. Bunları öğrenen saldırgan yöneticinin oturumunu kullanarak yönetici seviyesinde yeni hesap açmayı gerçekleştirebilir.(man in the middle attack)

6.3.2 Varışın Doğrulanması

Kaynağın iletişimden önce ve sonra doğrulanması gerektiği açıktır. Ancak varışın(sunucu) doğrulanması da gereklidir.

C2MYAZZ, Sunucu aldatması için kullanılan iyi bir yardımcıdır. Windows95'in kullanıcı doğrulanması sırasında pasif olarak bekler. Bir logon işlemi olduğunda,istemciye LANMAN doğrulama bilgisi gönderir. İstemci ise bilginin sunucudan geldiğini sanarak logon ve şifre bilgisini gönderir. Böylece kullanıcı şifresi öğrenilmiş olur.

DNS Poisoning

DNS te bir hostun adresi yerine rastgele başka adres bilgisinin yayınlanması işlemidir. Saldırgan trafiği böylece başka sunumcuya yönlendirir.Sayısal sertifikalar kullanılmadığı sürece istemci ve sunumcuların yerine bir saldırganın geçebilmesi mümkün olabilmektedir. Bunu önemenin en emin yolu verileri şifreleyerek iletmektir.

6.4 Kriptolama

Bilgisayar ağlarının ve haberleşme sistemlerinin güvenliğinin sağlanması için kullanılan en önemli işlem, verilerin şifrelenerek anlamsız hale getirilip hedefe gönderilmesi ve hedefte tersi işlem yapılarak tekrar eski hale getirilmesidir.

Bir şifreli haberleşme için;
1. Şifreleme algoritması (E)
2. Deşifreleme algoritması (D)
3. Bir anahtar bilgisine(K),

ihtiyaç vardır.

6.4.1 Terminoloji ve Notasyon

Kriptoloji, latince gizli anlamına gelen *kryptos* ve yine latince sözcük anlamına gelen *logos* kelimelerinin birleşiminden oluşan gizli ve güvenli haberleşme bilimidir. Kriptoloji temelde iki

kısımda incelenir; bunların birincisi kritik bilgilerin yetkisiz kişi ve/veya kurumlardan korunması amacıyla geri dönüşümü ümkün olarak anlaşılmaz hale getirilmesi yani şifrelenmesi için kripto sistemlerinin tasarlanması demek olan **kriptografi** bilimidir. İkinci kısım ise kodlanmış veya şifrelenmiş olan gizli bilgilerin bulunmasına yönelik çalışmaların yapılması demek olan **kript analiz** bilimidir.
Kriptolojide daha çok bilginin güvenliği ve gizliliği üzerinde durulacaktır. Bunun yolu genellikle bilgilerin veya mesajların bir takım transformasyonlara tabi tutulmasıyla olur. Daha sonra bu bilgi topluluğunun tekrar elde edilebilmesi için şifreli metne aynı transformasyonların tersi uygulanır. Orijinal mesaj burada kısaca **m** harfiyle, mesajı transformasyona tabi tutma işlemi **şifreleme** adıyla, ortaya çıkan anlaşılmaz metin ise kısaca **c** harfi ile gösterilecektir**.** Ters transformasyon işleminin şifreli metne uygulanıp tekrar orijinal mesajı elde etmeye yönelik yapılan işleme ise **deşifreleme** adı verilir.

6.5 Temel Kavramlar

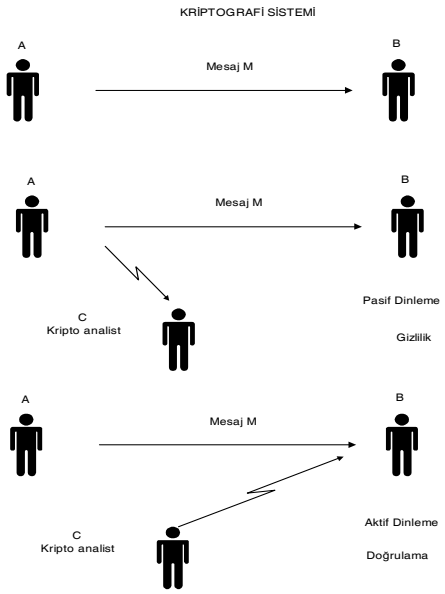
Kriptografi(cryptography): Anlaşılır bir mesajı anlaşılmaz şekle dönüştürme ve mesajı tekrar eski orijinal haline geri dönüştürme prensipleri ve yöntemlerini içeren sanat veya bilimdir.
Açık metin(plaintext): Anlaşılır orijinal metin
Şifreli metin(ciphertext) : Dönüştürülen metin
Şifreleyici(cipher) : Anlaşılır bir metni, yerlerini değiştirme ve/veya yerine koyma yöntemlerini kullanarak anlaşılır bir metni anlaşılmaz şekle dönüştürmek için kullanılan bir algoritma.
Anahtar(key) : Sadece gönderici ve alıcının bildiği şifreleyici tarafından kullanılan kritik bilgiler
Şifreleme(encipher (encode)) : Açık metni bir şifreleyici ve bir anahtar kullanarak şifreli metne dönüştürme süreci
Deşifreleme(decipher (decode)): Şifreli metni bir şifreleyici ve bir anahtar kullanarak açık metne dönüştürme süreci
Kriptoanaliz(cryptanalysis) : Bilgi ve anahtar olmaksızın anlaşılmaz mesajı anlaşılır mesaj olarak geri dönüştürme prensipleri ve yöntemleridir. Aynı zamanda kod kırma(**codebreaking**) olarak da adlandırılır.
Kriptoloji(cryptology) :Kriptografi ve kriptoanalizin her ikisi(şekil 6.2)
Kod(code): Anlaşılır bir mesajı bir kod kitabı kullanarak anlaşılmaz şekle dönüştürme için bir algoritma

Şifreleme(Encryption) $c = E_K(m)$

Deşifreleme(Decryption) $m = D_K(c)$

E_K, kriptografik sistem olarak bilinen transformasyon ailesinden seçilir.
Anahtar denilen K parametresi anahtar uzayından seçilir

Diğer bir deyişle, şifreleme işlemi $E_K(m)=c$ fonksiyonunu sağlayan bire-bir, bir fonksiyondur. E_K fonksiyonunun tersi olan D_K fonksiyonu ise, $D_K(c)=m$ şartını sağlayan deşifreleme işlemini gerçekleştirir. Burada yer alan bütün transformasyon işlemleri tersinir olduğundan dolayı açık bilginin şifreli bilgiden direkt olarak elde edilmesini önlemek için E ve D algoritmalarının gizli tutulması düşünülebilir. Şifreleme ve deşifreleme algoritmalarının herhangi bir şekilde yetkisiz kişilerin eline geçmesine karşı yalnızca mesajlaşacak kişilerin bilebileceği bir **anahtar** bilgisi, K, kullanılmalıdır. Dolayısıyla, mesajlaşmada önemli olan kriter kullanılan anahtarın gizliliği olacaktır. Sonuçta anahtar gizli tutulduğu halde algoritmalar açık olabilir.



Şekil6.2. Kriptografi Sistemi

6.6 Kripto sistemler

Kripto sistemlerinde kullanılan başlıca terimler kısaca şunlardır; ***A*** ile gösterilen **Alfabe** kavramı sonlu sayıda elemanlar kümesidir. Örneğin $A=\{0,1\}$ sık kullanılan ikili (binary) bir alfabedir. ***P*** ile gösterilen **Açık Metin Uzayı** (Plaintext Space) ise alfabeden alınmış sonlu sayıda eleman dizilerinden oluşur. Örneğin *P*, 0 ve 1 ler den meydana gelen bit dizilerini içerebilir. ***C*** ile gösterilen **Şifreli Metin Uzayı** (Ciphertext Space) ise yine *A* alfabesinden alınmış fakat *P* den farklı bir diziliş gösteren elemanlardan oluşur. ***K*** ise daha önce bahsettiğimiz **Anahtar Uzayını** (Key Space) ifade eder. Anahtar yine ***A*** alfabesindeki elemanların belli uzunluklarda bir araya gelmiş elemanlarından oluşur.

Tanım : Bir kriptosistem aşağıdaki şartları sağlayan (P,C,K,E,D) beşlisinden oluşur. Burada *E* şifreleme, *D* ise deşifreleme fonksiyonu veya algoritmasını gösterir.

$\forall\ k \in K$, $D_k \in D$ fonksiyonuna uyan bir $E_k \in E$ fonksiyonu vardır. Öyle ki;

$\forall\ E_k :\ P \rightarrow C$ ve $\forall\ D_k : C \rightarrow P$ ve her $x \in P$ için $D_k(E_k(x)) = x$

Kriptosistemler genel olarak aşağıdaki üç bağımsız özelliğe göre sınıflandırılırlar.

1. **Şifresiz metinden şifreli metne dönüşüm için kullanılan işlemlerin tipi:** Bütün şifreleme algoritmaları yerine koyma(substutition) ve yerini değiştirme(transposition) olmak üzere iki genel prensibe dayanır. Yerine koymada, şifresiz metindeki her bir eleman diğer bir elemana dönüştürülür, yerini değiştirme de ise, şifresiz metindeki elemanların yerleri değiştirilir.

2. **Kullanılan anahtarın sayısı:** Gönderici ve alıcı aynı anahtarı kullanırsa buna simetrik (tek anahtarlı, gizli anahtarlı, veya geleneksel) şifreleme, eğer gönderici ve alıcının her biri farklı anahtar kullanırsa buna asimetrik(iki anahtarlı, veya açık anahtarlı) şifreleme denir.

3. **Şifresiz metnin işleme yöntemi:** Eğer giriş verisi, herbir adımda blok olarak işlenerek çıkış blok olarak elde edilirse blok şifreleme, giriş verisi dizi olarak sürekli şekilde işlenirse dizi şifreleme adı verilir.

6.6.1 Kriptolama güvenliği ve Kriptoanaliz.

Şifrelenen metnin ne kadar güvenli olduğu ve çözümlenmesi için yapılacak saldırı tiplerinin neler olduğunun bilinmesi önemlidir. Geleneksel şifreleme yöntemlerine saldırı için iki adet genel yaklaşım mevcuttur.

Kriptoanaliz: Kriptoanalitik saldırılar, algoritmanın özelliği, şifresiz metnin genel karakteristiği hakkındaki bilgilere ve şifresiz metin–şifreli metin çiftinin bazı örneklerine dayanır. Bu saldırı sonucunda kullanılan anahtar veya şifresiz metin, algoritmanın eksikliklerine dayanılarak elde edilmeye çalışılır.
Deneme-Yanılma(Brute-Force Attack) saldırsı: Saldırgan mümkün olan bütün anahtar kombinasyonlarını, şifresiz metin elde edilene kadar şifreli metni çözmek için dener. Ortalama olarak bütün anahtar kombinasyonlarının yarısı başarılı bir saldırı için denenmelidir.

Şifreli metin için güvenlik bir sonraki paragrafta açıklanmıştır. Tablo 6.1'de ise Şifrelenen mesajı çözmek için yapılan saldırı tipleri ve kripto analistin neler bildiği gösterilmiştir.

Saldırı Tipi	Kriptoanalist'in bildiği
Sadece Şifreli Metne (ciphertext only)	Kriptolama algoritması Kodu çözülecek şifreli metin (istatistiksel Saldırı, brute force)
Bilinen Düz metin (known plaintext)	Kriptolama algoritması Kodu çözülecek şifreli metin Gizli anahtar ile şifrelenen bir veya daha fazla düz-şifreli metin çifti(Şifreye saldırı için kullanılır.)
Seçilen Düz metin (chosen plaintext)	Kriptolama algoritması Kodu çözülecek şifreli metin Kriptoanalist tarafından seçilen açık metin, bununla birlikte açık metnin gizli anahtar ile üretilen şifreli hali
Şeçilen Şifreli metin (chosen ciphertext)	Kriptolama algoritması Kodu çözülecek şifreli metin Kriptoanalist tarafından seçilen kuvvetle muhtemel şifreli metin ve karşılığı olan, gizli anahtar ile üretilen çözümlenmiş açık metin.
Şeçilen metin (chosen text)	Kriptolama algoritması Kodu çözülecek şifreli metin Kriptoanalist tarafından seçilen açık metin, bununla birlikte açık metnin gizli anahtar ile üretilen şifreli hali Kriptoanalist tarafından seçilen kuvvetle muhtemel şifreli metin ve karşılığı olan, gizli anahtar ile üretilen çözümlenmiş açık metin.

Tablo 6.1: Şifrelenen mesaja karşı yapılan saldırı Tipleri

6.6.2 Mutlak ve hesaplama güvenliği

İki farklı temel yöntem ile şifreler güvenli olabilir.

Mutlak güvenlik

- Bilgisayar gücü ne kadar fazla olursa olsun şifre hiçbir şekilde kırılamaz.

Hesaplamaya bağlı güvenlik

Bir şifreleme algoritması aşağıdaki kriterleri sağlıyor ise hesaplamaya bağlı güvenli(computationally secure) dır.

- Şifrenin kırılmasının maliyeti şifrelenmiş bilginin değerinden fazla ise
- Şifreyi kırmak için gereken zaman, bilginin yaralı ömründen fazla ise.

Hesaplamaya bağlı güvenlikte verilen bilgisayar gücü sınırları(örn. Evrenin yaşından daha fazla hesaplama zamanı gerekir gibi), içinde şifre kırılamaz.

Hesaplamaya bağlı güvenlik için şifreleme algoritması ve kullanılan anahtar uzunluğu önemlidir. Şifreleme algoritmasının kriptoanalist tarafından bilindiği kabul edilerek şifre uzunluğu ve bilgisayarın hesaplama gücüne bağlı olarak şifrelerin çözümleme süreleri Tablo 6.2'de gösterilmiştir. Çözümleme süresi için gerekli olacak zaman hesabı ortalama olarak alternatif şifre sayısının yarısı kadardır. Bilgisayar hesaplama gücünü ise paralel mimarili tasarım ile artırmak mümkün olmaktadır.

Anahtar Uzunluğu(bit)	Alternatif Anahtar Sayısı	1 çözümleme/µs hızında gereken zaman	10^6 çözümleme/µs hızında gereken zaman
24	$2^{24} = 1.6 \times 10^7$	2^{23} µs = 8.4 saniye	8.4 µsaniye
32	$2^{32} = 4.3 \times 10^9$	2^{31} µs = 35.8 dakika	2.15 milisaniye
48	$2^{48} = 2.8 \times 10^{14}$	2^{47} µs = 4.46 yıl	2.35 dakika
56	$2^{56} = 7.2 \times 10^{16}$	2^{55} µs = 1142 yıl	10 saat
128	$2^{128} = 3.4 \times 10^{38}$	2^{127} µs = 5.4×10^{24} yıl	5.4×10^{18} yıl
168	$2^{168} = 3.7 \times 10^{50}$	2^{167} µs = 5.9×10^{36} yıl	5.9×10^{30} yıl
26 karakter permutasyonu	$26! = 4 \times 10^{26}$	2×10^{26} µs = 6.4×10^{12} yıl	6.4×10^6 yıl

Tablo 6.2. : Anahtar uzunluklarına göre hesaplamaya bağlı güvenlik

6.7 Kriptografinin kısa Tarihçesi

6.7.1 Çok Eski(Ancient) şifreleyiciler

- En az 4000 yıl öncesine dayanır.
- Eski mısırlılar anıtlara yazdıkları resimli yazılarını şifrelemişlerdir.(Şekil 6.3)

Hieroglyphic encipherments of proper names and titles, with cipher hieroglyphs at left, plain equivalents at right

Şekil 6.3.

- Eski ibraniler kutsal kitaplarındaki belirli kelimeleri şifrelemişlerdir.
- 2000 sene önce Jul Sezar, şimdi Sezar şifresi olarak bilinen basit bir yerine koyma şifresi kullandı
- Roger Bacon 1200 lerde birkaç yöntem açıkladı.
- Geoffrey Chaucer çalışmalarında birkaç adet şifre kullandı
- Leon Alberti 1460 larda bir şifre tekerleği kullandı ve frekans analizinin prensiplerini açıkladı.

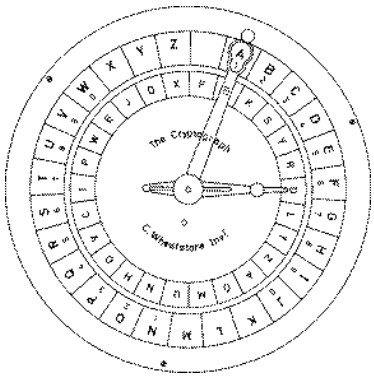
- Blaise de Vigenère 1855 de kriptoloji üzerine bir kitap yayınladı ve çoklu alfabe değiştirme sifresini açıkladı.
- Kullanımı ülkelerde özellikle diplomasi ve savaşlarda artmaktadır.

6.7.2 Makina Şifreleri

- 1790 larda geliştirilen **Jefferson cylinder**, herbiri rastgele alfabeli 36 adet disk ten oluşmaktaydı, disklerin sırası anahtarı oluşturmaktaydı, mesaj ayarlanınca diğer satır şifreyi oluşturmaktaydı.(Şekil 6.4)

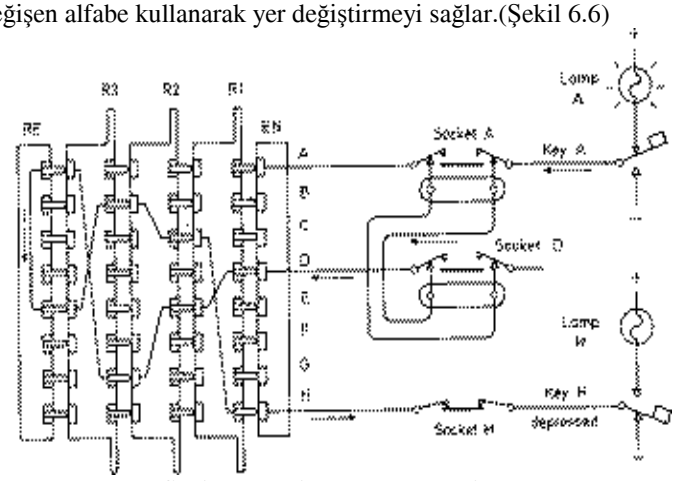
Şekil 6.4. Jefferson Cylinder

- **Wheatstone disc**, orijinal olarak 1817'de Wadsworth tarafından icat edildi, fakat 1860 da Wheatstone tarafından geliştirildi. Çoklu alfabeli şifreyi oluşturmak için merkezi olarak kullanılan tekerleklerden meydana gelmekteydi. (Şekil 6.5)



Şekil 6.5. Wheatsone Disk

- **Enigma Rotor makinası**, ikinci dünya savaşı sırasında çok kullanılan şifre makinalarının önemli bir sınıfını teşkil eder, içinde çapraz bağlantılı, bir seri rotordan meydana gelir, sürekli değişen alfabe kullanarak yer değiştirmeyi sağlar.(Şekil 6.6)



Şekil 6.6. Enigma Rotor Makinası

6.8 Sayı Teorisine Giriş

Bu bölümde kriptolama algoritmalarının matematik modellemesinde kullanılan modüler aritmetik kavramları üzerinde kısaca durulacaktır.

Grup Teorisi

Tanım(Grup): Her bir elemanın tersinin olduğu monoide (G, *) **grup** denir. Yani (G, *) çifti şu dört şartı sağlar:
(G_1) *, Kapalılık, Eğer a ve b $\in$ G ise a*b $\in$ G dir.
(G_2) *, G üzerinde birleşme özelliğine sahiptir. $\forall$a,b,c $\in$ G için, a*(b*c) = (a*b)*c dir.
(G_3) bir etkisiz eleman mevcuttur. $\forall$a $\in$ G için, a*e = e*a =a dır.
(G_4) G' nin her bir elemanının tersi mevcuttur.$\forall$a$\in$ G için,G'de bir a' vardır ve a*a'= a'*a =e dır.

Bu bölümde ve bundan sonraki bölümlerde belirtilmemiş ikili işlemler içeren ifadeler yazarken * simgesini göz ardı edeceğiz. Sadece yanlış anlamalara imkan verecek iki ikili işlemi birbirinden ayırt etmek için kullanacağız. Örneğin x*y yerine xy yazacağız (ancak çarpma işlemi ile karıştırmamalıyız). Ayrıca aşağıdaki gibi x' in üslerini tanımlayacağız.

$n\in Z^+$ olmak üzere $x^n=x*x*\ldots*x$ (n tane)

ve $x\in Z^-$ olmak üzere $x^n=(x^{-1})^{|n|}=x^{-1}*x^{-1}*x^{-1}*\ldots*x^{-1}$.(n tane)

Ayrıca etkisiz elemanı da şu şekilde tanımlarız: $x^0=e$.
Herhangi bir (G,*) grubun en belirgin özelliği büyüklüğü yani grubun temelini oluşturan G kümesinin eleman sayısıdır. Buna (G,*) grubunun order'ı denir.
Tanım: (G,*) grubunun order'ı G kümesinin kardinalitesidir ve |G| şeklinde gösterilir.

Eğer bir grup, sonlu sayıda elemana sahipse sonlu grup, ve grubun order'i gruptaki eleman sayısıdır. Diğer durumda grup sonsuz gruptur.
Eğer bir grup aşağıdaki ilave koşulu sağlıyor ise **abealian** grup adı verilir.

(G_5) Komutatiflik. $\forall$a,b $\in$ G için, a*b = b*a dır.

Eğer H grubu G grubunun bir alt grubu ise $|H|$ değeri $|G|$ değerini böler. Böylece eğer G grubunun *düzeni* bir asal sayıysa G' nin tek alt grubu kendisidir. Bu durumda G grubu çarpmalı olarak yazılabilir.

Eğer G grubu çarpmalı olarak yazılabilirse ve $g \in G$ olmak üzere g sayısı G grubunun düzeni ise bu g sayısı $i\in \mathrm{N} \cup \{\infty\}$ ve $g^i = 1$ şartını sağlayan en küçük i değeridir. Burada $\forall\, j, l \in Z$:

$$g^j = g^l \quad \Leftrightarrow \quad j \equiv l \mod ord(g)\text{' dir.}$$

Tablo 6.3'deki Cayley tablosu ile tanımlanmış grubu ele alalım:

*	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

Tablo 6.3

Her bir elemanı n bir tamsayı olmak üzere a^n biçiminde yazabileceğimizden bu grup için a^1=a, a^2=b, a^3=c ve a^4=e 'dir. Verilen herhangi bir eleman için bu gösterim aynı değildir. Örneğin,

$b=a^2=a^6=a^{-2}$ vs. yazabiliriz. Aslında kümenin her bir elemanını a' nın kuvvetleri biçiminde göstermek için sonsuz sayıda yol vardır. {e,a,b,c} 'nin her elemanı a^n biçiminde yazılabilir ve bu duruma a grubun bir üretecidir (generator) denir.

G grubunun altgrubu olan tüm gruplar *g* elemanının bir üssüdür ve $<g>$ ifadesiyle gösterilirler. Eğer $<g> = G$ ise *g* sayısı *G* grubunun **üreteci** (jeneratörü) olur. Bir üreteci olan tüm gruplara **devirli grup** (cyclic group) adı verilir.

G grubunun düzeni *p* asal sayısı ise grup içerisinde yer alan 1 dışındaki tüm sayılar *G* grubunun üreteci olur. Diğer bir deyişle $<g>$ nin düzeni 1 veya *p* sayısı olur.

Doğal olarak, diğer başka elemanlar da grubun üretecimidir? sorusu aklımıza gelir. c elemanının da bir üreteç olduğunu fakat n çift ise $b^n=e$ ve b tek ise $b^n=b$ olduğundan b 'nin bir üreteç olmadığını söyleyebiliriz. En az bir tane üretece sahip gruplara halka denir.

Halkalar: {R,+,X) ile gösterilen bir *R* halkası, $\forall a,b,c \in R$ için aşağıdaki aksiyomları toplama ve çarpma ikili işlemleriyle sağlayan bir elemanlar kümesidir.
(G_1-G_5) R, toplama altında bir abelian grup tur.

(H_1) Çarpma altında kapalılık, Eğer a ve b $\in$ R ise ab$\in$ R dir.
(H_2) Çarpma ile birleşme özelliğine sahiptir. $\forall a,b,c \in R$ için, a(bc) = (ab)c dir.
(H_3) Dağılma kuralı, $\forall a,b,c \in R$ için, a(b+c) = ab + ac , (a+b)c = ac +bc dir.

Eğer bir halka aşağıdaki koşulu sağlıyor ise komutatif halkadır.
(G_4) Çarpmada Komutatiflik. $\forall a,b \in R$ için, ab = ba dır.

Eğer bir komutatif halka aşağıdaki aksiyomları sağlıyor ise integral domain dir.
(H_5) Çarpımsal etkisiz eleman. $\forall a \in R$ için, a1 = 1a =a dır.
(H_6) Sıfır bölen olmaması $\forall a,b \in R$ ve ab=0 ise ya a=0 veya b=0 dır.

Alanlar(Field) : {F,+,X) ile gösterilen bir *F* alanı, $\forall a,b,c \in F$ için aşağıdaki aksiyomları toplama ve çarpma ikili işlemleriyle sağlayan bir elemanlar kümesidir.
(G_1-H_6) F, G_1 den G_5 'e ve H_1den H_6 ya aksiyomları sağlayan bir integral domain dir.
(H_7) Çarpımsal invers . $\forall a \in F$ için (sıfır hariç) F'de bir a^{-1} vardır ve $aa^{-1}= (a^{-1})a =1$dir.

Esasında bir **alan**, kümenin dışına çıkmaksızın, toplama çıkartma çarpma ve bölme yapılabilen bir kümedir. Bölme $a/b = a(b^{-1})$ kuralı ile tanımlanır.

Modüler Aritmetik

Modüler aritmetik "saat aritmetiğidir"

Tanım *a, r* ve *n* tam sayıları ve $n \neq 0$ şartı için, eğer *a* ve *b* nin farkı *n* 'in *k* katı kadarsa bu şu şekilde gösterilebilir:

$$a = k \,.\, n \; + r$$

burada; a ve n pozitif tamsayılardır. Bu bağıntıyı sağlayan k ve r değerlerini her zaman bulmak mümkündür. kn'den a ya olan uzaklık r'dir ve kalan(residue) olarak adlandırılır. Veya eğer a ve n pozitif tamsayı iseler, a mod n , a ,n ile bölündüğünde kalan olarak tanımlanır. Böylece herhangi a tamsaysı için,

a= [a/n]x n + a ***mod*** n her zaman yazılabilir. (Örn: 11 mod 7 = 4)

a ve b iki tamsayısı eğer a ***mod*** n =b ***mod*** n iseler benzer modulo n olarak tanımlanır ve $a \equiv b \bmod n$ olarak yazılabilir.

Bölenler: Eğer sıfır olmayan bir b ve m tamsayısı için a=mb şeklinde yazılabiliyorsa b, a'yı böler denir. Böyle bir bölünebilirlik var ise kalan sıfırdır. b|a notasyonu b'nin a'yı kalansız bölebildiğini belirtmek için sıkça kullanılır. Aşağıdaki bağıntılar vardır.

- Eğer a|1 ise a= ±1 dir.
- Eğer a|b ve b|a ise a= ±b dir.
- Herhangibir b ≠ 0 sıfırı böler.
- Eğer, b|g ve b|h ise , b|(mg +nh) herhangi m ve n tamsayıları için vardır.

Teorem a_1, a_2 ve n tam sayıları ve $n \neq 0$ şartı için,

$$(a_1 \ op \ a_2) \bmod n \equiv [(a_1 \bmod n) \ op \ (a_2 \bmod n)] \bmod n$$

denkliği gösterilebilir, burada *op*, " + " veya " * " şeklinde bir operatör olabilir.

- Bir a = b mod n eşitliği, a ve b aynı *n* ile bölündüğünde aynı kalanı verdiklerini ifade eder. Örnek,
  - 100 = 34 mod 11
  - Genellikle 0<=b<=n-1 dir.
  - 2mod7 = 9mod7
  - b 'ye a mod n 'nin kalanı denir.
- Tamsayı modulo n ile yapılan bütün aritmetikte bütün sonuçlar 0 ve n arasında olur.

Modül işleminin özellikleri

Modül işlemi aşağıdaki özelliklere sahiptir.

Eğer, n|(a-b) ise a ≡ b ***mod*** n dir.

a ≡ b ***mod*** n , b ≡ a ***mod*** n anlamına gelir.

a ≡ b ***mod*** n ve b ≡ c ***mod*** n , a ≡ c ***mod*** n anlamına gelir.

Modüler Aritmetik işlemleri

Toplama

(a+b) mod n = [(a mod n) + (b mod n)] mod n

Çıkartma

(a-b) mod n = [(a mod n) - (b mod n)] mod n

Çarpma

axb mod n = [(a mod n) x (b mod n)] mod n

- Tekrarlanan toplamdan türetilir
- Ne a ne de b sıfır değil iken a.b=0 olabilir
  - örnek 2.5 mod 10

Bölme

a/b mod n

- b nin tersi ile çarpmak gibidir: $a/b = a.b^{-1} \bmod n$
- eğer n asal ise $b^{-1} \bmod n$ vardır. $b.b^{-1} = 1 \bmod n$
  - örnek 2.3=1 mod 5 bu nedenle 4/2=4.3=2 mod 5 dir.

Özellikler :

n'den küçük olan pozitif tamsayıların kümesi Z_n aşağıdaki gibi tanımlansın.

$$Z_n = \{ 0,1,\ldots\ldots\ldots\ldots,(n-1)\}$$

Z_n kalanlar sınıfı olarak adlandırılır. Daha doğrusu, Z_n de her bir tamsayı bir kalan sınıfını temsil eder. [r] = { a : a bir tamsayı; öyleki ; a = r mod n dir.]
Z_n içersinde yapılacak modüler artimetik işlemleri Tablo 6.4'deki özellikleri Z_n deki tamsayılar ile sağlar. Z_n çarpımsal etkisiz eleman ile birlikte bir değiştirilebilen bir halka oluşturur.

Özellik	Açıklama
Değişme Kuralı (Commutative)	(a + b) mod n = (b + a) mod n (a x b) mod n = (b x a) mod n
Birleşme Kuralı (Associative)	[(a+b) +c] mod n = [a +(b + c)] mod n [(axb) x c] mod n = [a x(b x c)] mod n
Dağılma Kuralı (Distributive)	[ax(b + c)] mod n = [(axb) + (axc)] mod n
Etkisiz eleman (Identity element)	(0 + a) mod n = a mod n (1xa) mod n = a mod n
Toplamsal invers(-a)	$\forall a \in Z_n$ için ; bir b vardır öyleki ; a + b = 0 mod n dir.

Tablo 6.4.

- Aynı zamanda, indirgeme tamsayılar halkasından tamsayı modulo n 'lerin halkasına bir homomorfizm olduğu için, bir işlem ve sonra modulo n i indirgeyip indirgemeyeceği veya indirgedikten sonra yapacağı işlem seçilebilir.
  - a+/-b mod n = [a mod n +/- b mod n] mod n
  - (a.b) mod n =((a mod n).(b mod n)) mod n
- eğer n, p doğal sayısı olmaya zorlanırsa bu form bir **Galois Field modulo p** ve **GF(p)** ile gösterilir ve bütün tamsayı aritmetiğindeki normal kurallar geçerlidir.

GF(p) (Galois Field) şeklindeki sonlu alanlar.
Birçok kriptografik algoritmada sonlu alanlar önemli bir rol oynarlar. Bir sonlu alanın düzen(order) ı bir p asal sayısının n. kuvveti(p^n) olarak gösterilmelidir. Burada n pozitif bir tamsayıdır. Düzeni p^nolan bir sonlu alan, genellikle GF(p^n) olarak yazılılr. GF sonlu alanı ilk defa çalışan matematikçi olan Galoi'den gelmektedir. Özel durum olan n=1 için, sonlu alan GF(p) olarak yazılır.
Özel durum olarak GF(2^n) ve GF(3^n) verilebilir.
Düzeni p olan bir sonlu alan GF(p), {0,1,.....,p-1} Z_p tamsayılar kümesinin modulo p aritmetik işlemleri ile birlikte tanımlanmasıdır.
Burada herbir elemanın bir çarpımsal tersi vardır ve çarpımsal invers olarak (w^{-1}) Çarpımsal invers . $\forall w \in Z_p$ için (sıfır hariç) Z_p'de bir z vardır ve w*x*z= 1mod p 'dir.
Çünkü , w, p ye göre asaldır. Eğer, Z_p nin elemanlarını w ile çarparsak, sonuçtaki kalanlar Z_p nin elemanlarının tamamının tekrarıdır. Böylece en az bir kalanın değeri 1'dir.Bu yüzden Z_p 'de en az bir eleman vardır öyleki, w ile çarpıldığında kalan 1'dir. Bu tamsayı w'nın çarpımsal tersi(w^{-1}) dir.
Tablo 6.5'de GF(7) sonlu alanında Modulo 7 nin toplamsal ve çarpımsal tersleri gösterilmiştir.

w	-w	w^{-1}
0	0	-
1	6	1
2	5	4
3	4	5
4	3	2
5	2	3
6	1	6

Tablo 6.5 Modulo 7 için toplamsal ve çarpımsal tersler

Asal Sayılar

Bir p >1 sayısı ancak ve ancak bölenleri ±1 ve ±p ise asal sayıdır. Asal sayılar, Açık-anahtarlı kripto sistemlerinde büyük rol oynarlar. Asal sayılarda karşımıza çıkan önemli problemler, asal bir sayının oluşturulması ve bir sayının asal olup olmadığının test edilmesidir. Asal sayı oluşturma, verilmiş bir [r_1, r_2] tam sayılar aralığında asal sayı bulma işlemidir.

Herhangi bir a>1 tamsayısı tek bir şekilde aşağıdaki gibi ifade edilebilir.

$$a = p_1^{a_1} p_2^{a_2} \ldots\ldots\ldots p_t^{a_t}$$

burada $p_1,p_2,\ldots\ldots,p_t$ asal sayılardır ve a_i tamsayıdır. (örn: $3600 = 2^4 \times 3^2 \times 5^2$)

Tanım: $a^{s-1} \equiv 1 \bmod s$ şartını ve $1<a<s$ şartını sağlayan s tam sayısına a tabanına göre **sanki asal** (pseudoprime) sayı denir**.**

Teorem (Fermat teoremi) p bir asal sayı olsun. Her p ile bölünemeyen a pozitif tam sayısı için,

$$a^p \equiv a \bmod p \qquad \text{denkliği;}$$

ve p ile bölünmeyen her a tam sayısı için ise $a^{p-1} \equiv 1 \bmod p$. denkliği her zaman doğrudur:

İsp: Önceki bölümlerde açıklandığı üzere, eğer,Z_p nin elemanlarını{0,1,....,(p-1)} a , modulo p ile çarparsak, sonuçtaki kalanlar Z_p nin elemanlarının tamamının sekansıdır. Bundan başka, a x 0 = 0mod p dir. Bu yüzden (p-1) sayı, { $a$mod p, 2$a$modp, ...,(p-1)$a$mod p } ,dizisi {0,1,....,(p-1)} sayısı ile aynı düzendedir. Her iki kümenin sayılarını çarpıp mod p'sini alarak aşağıdaki bağıntı yazılabilir.

ax2ax ..... x ((p-1)a) = [(a modp) x (2$a$modp) x .....x((p-1)a modp]modp
= [1 x 2 x ..... x (p-1)] modp
= (p-1)! modp

Fakat, a x 2a x .....x((p-1)a) = (p-1)!a^{p-1} dir

Bu yüzden, (p-1)!a^{p-1} = (p-1)! modp . dir. Burada (p-1)! 'i atabiliriz. Sonuçta:

$a^{p-1} = 1 \bmod p$ olduğu gösterilmişolur.

Örn: a=7, p = 19 verilsin.

$7^2 = 49 = 11 \bmod 19$

$7^4 = 121 = 7 \bmod 19$

$7^8 = 49 = 11 \bmod 19$

$7^{16} = 121 = 7 \bmod 19$

$a^{p-1} = 7^{18} = 7^{16} \times 7^2 = 7 \times 11 = 1 \bmod 19$

alternatif olarak $a^p \equiv a \bmod p$ olarak da yazılabilir.

Euler Totient fonksiyonu n tam sayısı için Euler Totient fonksiyonu $\phi(n)$, n den daha küçük olan ve n ile aralarında asal olan bütün pozitif tam sayıların sayısını verir.

p **asal ise** $\phi(p) = p-1$ **dir.**

$n=p.q$ ve p, q asal sayılar ise $\phi(n) = \phi(.pq). = \phi(p).\phi(q) = (p-1).(q-1)$ dir.

$\phi(n) = \phi(.pq)$.olduğunu görmek için, Z_n 'deki kalanlar kümesinin [0, 1, ..., (pq-1)]. Olduğunu düşünelim. Kalanlar kümesindeki {p, 2p,.....,(q-1)p}, {q, 2q, ..., (p-1)q} ve 0 , n'e göre asal değildirler. Buna uygun olarak,

$\phi(n) = pq - [(q-1) + (p-1) + 1]$
$= pq - (p+q) + 1$
$= (p-1) \times (q-1)$
$= \phi(p).\phi(q)$

elde edilir. Tablo 6.6'da n = 30 'a kadar olan sayıların $\phi(n)$ değerleri gösterilmiştir

n	$\phi(n)$	**n**	$\phi(n)$	**n**	$\phi(n)$
1	1	11	10	21	12
2	1	12	4	22	10
3	2	13	12	23	22
4	2	14	6	24	8
5	4	15	8	25	20
6	2	16	8	26	12
7	6	17	16	27	18
8	4	18	6	28	12
9	6	19	18	29	28
10	4	20	8	30	8

Tablo 6.6. 1-30 arası sayılar için $\phi(n)$ değerleri

Teorem (Fermat teoremi) Eğer ***s*** bir asal sayı ve ***OBEB*(*a,s*)=**1 ise ***s***, ***a*** tabanına göre bir sanki asal (pseudo prime) sayıdır.

Tek Yönlü Fonksiyon

F: X $\longrightarrow$ Y

f : $x \longrightarrow f(x)=y$ yalnız ve yalnız aşağıdaki şartları taşıdığı takdirde tek yönlü bir fonksiyondur:

- $f(x)$ bütün x değerleri için polinomsal zamanda çözümlenebilir olmalıdır.
- Verilen bir y değeri için x değeri polinomsal zamanda bulunamamalıdır.

Örnek olarak verilirse $a^m \bmod n \equiv x$ bir modüler üs alma işlemidir ve kolaylıkla yapılabilir, fakat var olan x değerinden m değerini bulmak ayrık logaritma problemine girer ve bunun da hesaplanma süresi polinomsal çözümleme süresinden çok daha uzundur.

Kapaklı Tek Yönlü Fonksiyonlar (Trapdoor One-Way Functions)

Kapaklı tek yönlü fonksiyonlarda ise tek yönlü fonksiyonlara ek olarak analizciye başka bilgiler verilirse fonksiyon daha kolay tersinir hale getirilebilir.
Örneğin yalnız $a^m \bmod n$ değerini bilmekten öte buradaki n değerinin iki asal sayının çarpımı olduğunu ve anahtarların bu sayılara bağlı olduğunu bilmek buradan m değerini bulma aşamasında analizciye ipucu vermiş olur.

6.8.1 GF(p) 'de üstel işlem

- Birçok kriptolama algoritması üstelleştirmeyi kullanır, b üssü ne göre büyüyen bir a sayısı(taban) mod p
  - $b = a^e \bmod p$
- üstelleştirme basit olarak bir n sayısı için O(n) çarpma olan tekrarlanan çarpmalardır.
- Daha iyi bir yöntem kare ve çarpma algoritmasıdır.

```
let base = a, result =1
    for each bit ei (LSB to MSB) of exponent
        if ei=0 then
        square base mod p
        if ei=1 then
        multiply result by base mod p
    square base mod p (except for MSB)
required ae is result
```

- Bir n sayısı için sadece $O(\log_2 n)$ çarpma yapılır.

6.8.2 GF(p) 'de ayrık Logaritma Problemi

Ayrık logaritma problemi, grup olarak tanımlanan matematiksel yapılara uygulanır. Daha önce de açıklandığı gibi, bir grup çarpımı dediğimiz bir ikili işlem ile elemanların birlikte toplanmasıdır. Bir grup elemanı α ve bir n sayısısı için; α^n , α nin n kere kendisi ile çarpımından elde edilisin; $\alpha^2 = \alpha * \alpha$, $\alpha^3 = \alpha * \alpha * \alpha$, ….

Ayrık logaritma problemi, aşağıdaki gibidir. Bir sonlu grup G'de verilen bir α elemanı ve diğer eleman $b \in G$ için ; Öyle bir x tamsayısı bulunsun ki $\alpha^x = b$ eşitliğini sağlasın. Örneğin, $3^x \equiv 13 \pmod{17}$ probleminin çözümü 4 'tür. Çünkü $3^4 = 81 \equiv 13 \pmod{17}$ dir.

Çarpanlara ayırma problemi gibi, ayrık logaritma probleminin de zor olduğu kabul edilir ve bir tek yönlü fonksiyonun sert yönü gibidir. Her nekadar ayrık logareitma problemi herhangi bir grup üzerinde isede kriptografik amaçla genellikle $\mathbf{Z}_n$ grubu kullanılır.

Bir başka ifade ile ayrık logaritma :

- Üstelleştirmede ters problem, bir modulo p sayısının ayrık logaritmasının bulunmasıdır.
  - $\alpha^x = b \bmod p$'de *x'*i bul
- üstelleştirme nispeten kolay iken, ayrık logaritmanın bulunması genellikle kolay yolu olmayan zor bir problemdir.
- Bu problemde, eğer p asal ise , herhangi bir b! = 0 için her zaman bir ayrık logaritması olan bir α olduğu gösterilebilir.
  - α'nın ardışıl kuvvetleri mod p ile **grup** oluşturur

  α mod p, α^2 mod p,....., α^{p-1} mod p 1 farklıdır ve 1 ila p-1 arasında değer alır.
- Öyle ki α ya **primitif kök** denir ve aynı zamanda bulmak nispeten zordur.

α'nın ardışıl kuvvetlerinin mod p ile oluşturduğu **grup'**ta, herhangi bir *b* tamsayısı ve p'nin primitif kökü olan α için bir *x* üssü bulunabilir ki;

$$b = \alpha^x \bmod p \quad 0 \le x \le (p-1) \text{ dir.}$$

Üs *x* ayrık logaritma veya indis olarak gösterilir.

6.8.3 En Büyük ortak Bölen(Greatest Common Divisor)

Teorem *a* ve *n* tam sayıları için, ($a \in \{0,1,...n-1\}$); eğer *a* ve *n* aralarında asal iki sayıysa *a* nın modül *n'* e göre yalnız bir tane tersi vardır ve a^{-1} sembolüyle gösterilir.

$OBEB(a,n) = 1 \Leftrightarrow \exists\ b \in [a,n-1],\ 1 = a.b \bmod n$, yani $b = a^{-1}$ dır.

- A ve b'nin en büyük ortak böleni(a,b) a ve b'nin her ikisini de bölen en büyük sayıdır.
- **Euclid's Algoritması** iki a ve n(a<n) sayısının en büyük ortak bölenini bulmak için kullanılır,
  - Eğer a ve b nin böleni d ise, a-b ve a-2b yi bulur

GCD (a,n) is given by:

let g0=n
g1=a
gi+1 = gi-1 mod gi
when gi=0 then (a,n) = gi-1

örn. (56,98) 'i bulalım.

g0=98
g1=56
g2 = 98 mod 56 = 42
g3 = 56 mod 42 = 14
g4 = 42 mod 14 = 0

sonuçta EBOB (56,98)=14

Teorem (Chinese Remainder Teoremi)

Modüler karekök bulunması problemlerini göz önüne alırsak, asal üs modülo için indirgenebilen genel bir mod m problemi buluruz. Bir sonraki problem, orijinal benzerliği çözmek için, asal üslerin çözümün nasıl parçalanabileceği olacaktır. Bu Chinese kalan teoremi ile yapılabilecektir.

Tipik bir problem eşzamanlı olarak çözülen tamsayı x 'leri bulmaktır.

x **≡ 13 (mod 27)**

x **≡ 7 (mod 16)**

Bu uygulamada iki modülo birbine göre asal olması önemlidir. Diğer durumda iki benzerliğin uygunluğu test edilmelidir. Chinese kalan teoreminin çok basit bir cevabı vardır.

Chinese Kalan teoremi: Birbirine göre asal olan modul *m* ve *n*,için benzerlik ;

x **≡ a (mod m)**

x **≡ b (mod n)**

x için modulo *mn* şeklinde tekbir çözümü vardır.Örnek problemde mod 16.27 = 432 tek bir çözümü olacaktır.

Problemi çözmek için daha basit bir yöntem vardır. Daha basit bir örnek üzerinde düşünelim. Bütün *x* lerin sağladığı

x **≡ 2 (mod 3)**

x **≡ 3 (mod 5)**

İlk benzerliği sağlayan sekans 2,5,8,11,14,17 ,…… dir. Bu sekans tarandığında 5' 2 bölündüğü zaman 3 kalan terim 8 olduğu için cevap 8'dir. Bunun daha kolay bulnması için Öklid'in enbüyük ortak bölen algoritmasından faydalanılır.

Bütün işlemi genelleştirirsek ;

x **≡ a (mod m)**

x **≡ b (mod n)**

Önce *mu+nv*=1 denklemini sağlayan, u ve v tamsayıları bulunmalıdır. Sonra bütün çözümler x= (mu)b + (nv) a (mod mn) nı sağlamalıdır.

Bir diğer örnek $x \equiv 23 \pmod{100}$ $x \equiv 31 \pmod{49}$ verilsin.

Önce; 100u + 49 v = 1 çözülmelidir.

Euclid's algoritması aşağıdaki şekilde kullanılır.

Bölünen	=	Bölüm	.	Bölen	+	Kalan	0 1	1 0
100	=	2	.	49	+	2	2	1
49	=	24	.	2	+	1	49	24
2	=	2	.	1	+	0	100	49

Buradan 49.49 -24.100 = 1 dir. Çözüm 49.49..23- 24.200.31 = -19177 ≡ 423 (mod 4900) dir.

Genel hali;

$x \equiv a_1 \mod m_1$

$x \equiv a_2 \mod m_2$ .....

$x \equiv a_r \mod m_r$ ve $OBEB(m_i, m_j) = 1,\ i \neq j$

benzerlik sistemleri için, *x* ' in en az bir çözümü vardır:

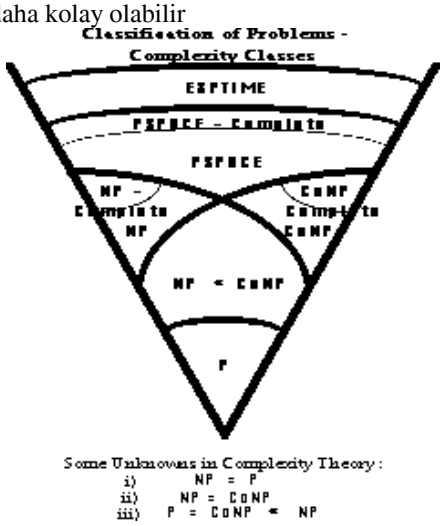
$$x = \sum a_i \,.\, M_i \,.\, N_i$$

$M = m_1 . m_2 . m_3 .. .. m_r$ *ve* $M_i = M / m_i$, $N_i = M_i^{-1} \mod m_i$.

En önemli uygulama RSA algoritmasındaki çok büyük olan p ve q asal sayılarının çarpımında çok zaman alan işlemleri azaltmak için kullanılır. Hesaplamalar Z_n 'den Z_p x Z_q 'ya taşınarak daha küçük bit uzunluklu verilerle işlemler basitleştirilir.

6.9 Karmaşıklık Teorisi (saksı benzeri bakış)

- Karmaşıklık teorisi, bir problemin çözümünün genelde ne kadar zor olduğu ile ilgilenir.
- Problem çeşitlerinin sınıflandırılmasını sağlar
- Bazı problemler esastan diğerlerinden daha zordur.,örneğin
  - Sayıların çarpımı $O(n^2)$
  - Matrislerin çarpımı $O(n^{(2)(2n-1)})$
  - Çapraz kelime çözümleri $O(26^n)$
  - Asal sayıların tanınması $O(n^{\log \log n})$
- En kötü durum karmaşıklığına değinir.
  - Ortalamada daha kolay olabilir



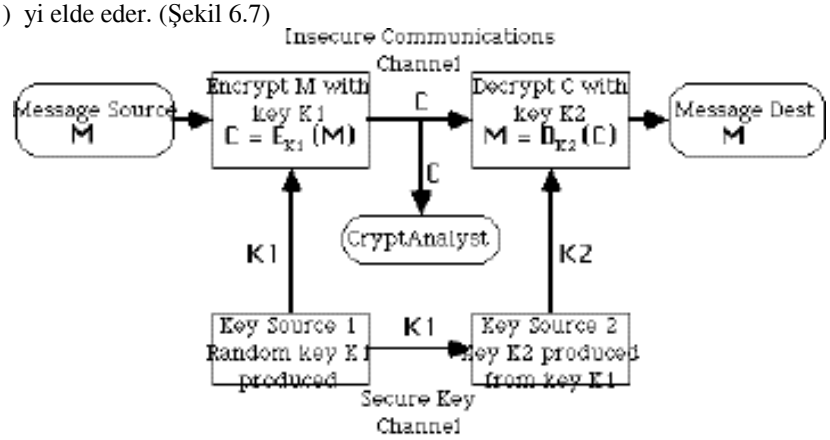
6.9.1 Karmaşıklık Teorisi- Bazı Terminoloji

- Bir problemin anlık durumu genel bir problemin kısmi örneğidir
- Bir problemin giriş uzunluğu, onun kısmi örneğini karakterize etmek için kullanılan n sembol sayısıdır.
- Bir fonksiyonun derecesi, **f(n)** bazı **g(n)** in **O(g(n))** idir.
  - $f(n) <= c.|g(n)|$, bütün, $n >= 0$, bazı c için
- (**P**) polinomsal zaman algoritması O(p(n)) zaman karmaşıklı kısmi bir problemin herhangi bir anını çözer,burada p giriş uzunluğu üzerine bazı polinomlardır
- çözüm zamanı olan (**E**) üstel zaman algoritması sınırlanmamıştır.

- Problemin ani çözümünün bir tahmini için polinomsal zamanda doğruluk testi yapılabilen (**NP**) **non-deterministic polinomsal zaman** algoritmasıdır.
- **NP-complete** problemleri polinomsal çözüme sahip olan bir problem olarak bilinen NP problemlerin alt sınırıdır. Burada bütün NP problemleri polinomsal çözüme sahiptir. Bunlar en zor NP problemleridir
- **Co-NP** problemleri NP problemlerinin eşleniğidir, Co-NP problemlerinin bir çözümünü tahmin etmek çözüm uzayınının detaylı araştırılmasını gerektirir

6.10 Gizli anahtarlı (simetrik) kriptosistemler :

Gizli anahtarlı kriptografik sistemler tarihin ilk devirlerinden beri dünyada kullanımı süregelen kriptografik sistemlerdir. Bu sistemlerde şifreleme algoritması ve deşifreleme algoritması birbirinin tersi şeklindedir. Öncelikle haberleşecek iki grup aralarında gizli bir anahtar tespit ederler. Eğer bu iki grup birbirlerine yakın yerlerde yer almıyorlarsa güvenli bir haberleşme kanalı veya güvenilir bir kurye yoluyla anahtarları birbirlerine ulaştırabilirler. Bir taraf şifreleme algoritmasında girdi olarak açık metin (P) ve anahtarı (K) uygular, ardından şifreli metin (C) yi elde eder ve mesajın alıcısına gönderir. Mesaj alıcısı ise deşifreleme algoritmasının girdileri olarak şifreli metin (C) yi ve aynı (K) anahtarını kullanır ve ardından çıktı olarak açık metin (P) yi elde eder. (Şekil 6.7)

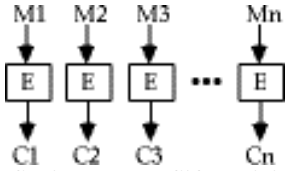


Symmetric (Private-Key) Encryption System

Şekil 6.7 Gizli-anahtarlı kriptosistem ile haberleşme

Gizli-anahtarlı kripto sistemleri uygulama sahalarında ikiye ayrılır;

i. Blok Şifreleme: Şifreleme ve deşifreleme işleminde metinler sabit uzunluklu dizilere bölünüp blok blok işleme tabi tutulur (örneğin 8, 16, 32 bit veya bayt). Anahtar uzunluğu ise yine sabittir. Blok şifrelemeye örnek olarak IBM tarafından 1976 yılında tasarlanan ve A.B.D Teknoloji Standartları Enstitüsü NIST tarafından her dört yılda bir güvenliği onaylanan DES (Data Encryption Standard) algoritması verilebilir. DES algoritması şifrelenecek metni 64 bitlik bloklar halinde şifreler, kullandığı anahtar boyu ise yine 64 bittir. Yalnız burada anahtarın işaret bitlerinin ayıklanmaları durumunda anahtar boyunun 56 bite indiğini hatırlatmak gerekir. Diğer bilinen blok şifrelemeli algoritmalara ise FEAL, IDEA ve RC5 örnek olarak gösterilebilir. Çalışacağımız çoğu modern şifreleyici bu formdadır. (Şek. 6.8)

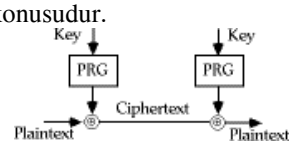


Şekil 6.8.Blok Şifreleyici

ii. Dizi Şifreleme: Bu çeşit şifrelemede algoritmanın girdisi yalnızca anahtardır. Algoritma anahtardan rastgele bir diziye çok benzeyen kayan anahtar dizisi üretir. Daha sonra kayan anahtar dizisinin elemanları ile açık metin veya kapalı metin dizisinin elemanları ikili tabanda toplanarak şifreleme veya deşifreleme işlemi tamamlanır. Dizi şifreleme algoritmalarına örnek olarak **RC4** algoritması gösterilebilir.

- Mesajı bit bit işler. (dizi olarak)
- En meşhur olanı **Vernam cipher** şifreleyicisidir(aynı zamanda **one-time pad denir**)
- 1917'de AT&T de çalışan Vernam tarafından geliştirildi
- basit olarak mesaj bitlerini rastgele anahtar bitlerine ekler.(şek. 6.9(a))
- mesaj biti kadar anahtar biti gerekir. Prtatikte zordur.(örn. Pratikte mag teyp veya CDROM da dağıtılır)
- anahtar tamamen rastgele olduğu için koşulsuz güvenlik sağlanır.
- böyle büyük bir anahtar dağıtımı güç olduğu için anahtar dizisi daha küçük(taban) bir anahtardan üretilebilir. Bunun için rasgele sembol fonksiyonları kullanılır.(şek 6.9(b))
- Her ne kadar bu çok çekici gözükse de pratikte iyi bir kriptografik güçlü rasgele fonksiyon bulmak çok güçtür. Bu hala birçok araştırmacının konusudur.

Şekil 6.9(a)



Şekil 6.9(b)

6.11 Simetrik Şifreleme Algoritmaları

Geleneksel simetrik blok şifreleme algoritmaları(örn. DES) 1973'de IBM'de çalışan Hort Feistel Tarafından geliştirilen Feistel networküne dayanır. Bu nedenle Feistel blok şifreleyicinin anlaşılması önemlidir.

Bir dizi şifreleyici sayısal bir veriyi bit bit veya bayt bayt şifreleme yapar.(Örnek vernem şifreleyici) Blok şifreleyici ise veryi sabit uzunluklu bloklara ayırıp bu blokları şifrelereyerek aynı uzunluklu şifreli bloklar elde eder. Tipik blok uzunlukları 64 veya 128 bit olabilir.

Feistel Şifreleyicinin yapısı

Feistel, pratikte yerine koyma ve yer değiştirme işlemlerine alternatif olan ve shanon tarafından önerilen confusion ve diffusion fonksiyonlarını şifreleme algoritmasında önerdi.

Diffusion da, şifresiz metnin istatistiksel yapısı, şifreli metnin istatistiğine dağıtılır. Bu, şifresiz metnin herbir dijitinin, şifreli metnin etkilediği dijitlerinin bulunmasıyla sağlanır., başka bir ifade ile,her bir şifreli metin dijit'i birçok şifresiz metin dijiti tarafından etkilenir. Örnek olarak; Bir M = m_1,m_2, m_3,…….. karakterlerinden oluşan bir şifresiz metni ortalama işlemi ile k ardışıl karakteri ekleyerek şifrelemek;

$y_n = \sum_{i=1}^{k} m_{n+i} \pmod{26}$ ile yapılmış olsun. Şifresiz metnin istatistiksel yapısının dağılmış olduğu gösterilebilir. Böylece şifreli metindeki karakter dağılımı şifresiz metindeki karakter dağılımının yakınında olacaktır.

Confusion'da ise, anahtarın keşfedilmesi saldırılarına karşı, şifreli metnin istatistiği ile şifreleme anahtarının olabildiğince karmaşık olmasını araştırır. Böylece bir saldırgan şifreli metnin istatisiğini hesaplasa bile hangi anahtar ile şifrelendiğini anlaması çok zorlaşır.

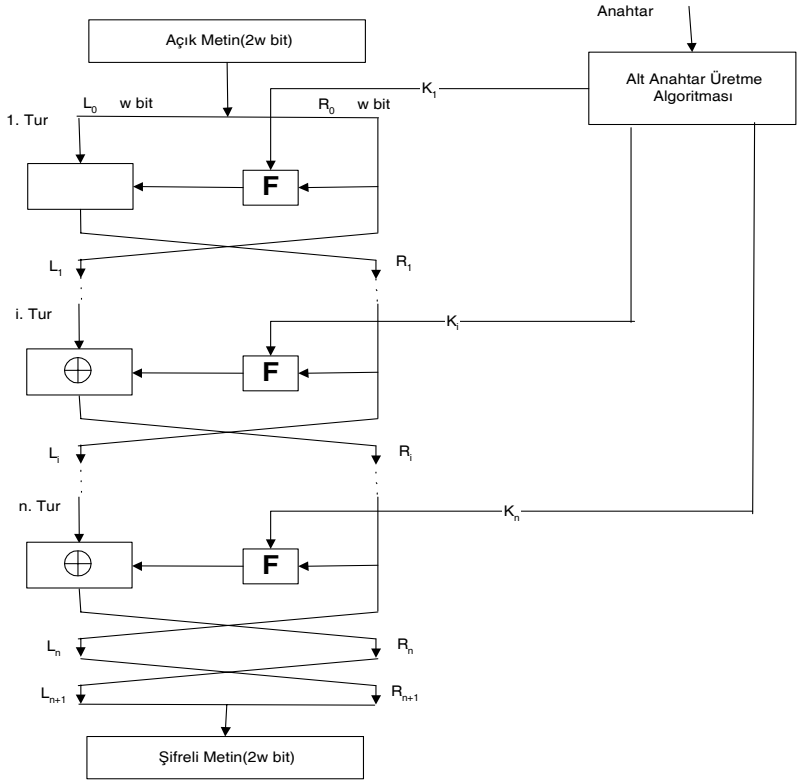
Şekil 6.10'da gösterilen bu algoritmada 2w bit uzunluğun da olan şifresiz metin iki eşit sol ve sağ parçaya ayrılır. Her bir turda ana şifreden üretilen alt şifre ile sağ tarafa F fonksiyonu uygulanır. Bunun sonucu ise sol taraf ile EXOR mantıksal işlemine tabi tutulur. Daha sonrada elde edilen sonuçlar çaprazlanır. Yani sağ taraf sola sol taraf sağa geçer. Böylece turlar devam eder. Asıl anahtardan alt anahtarlar her turda üretilerek F fonksiyonuna girdi olarak kullanılır.
Feistel algoritmasının önemli parametreleri aşağıda açıklanmıştır.

Blok uzunluğu: Büyük blok uzunluğu daha fazla güvenlik anlamındadır. Fakat şifreleme/deşifreleme hızını azaltır. Genel olarak 64 bitlik blok genişliği kullanılır.
Anahtar Uzunluğu: Büyük anahtar genişliği daha fazla güvenlik anlamındadır. Fakat şifreleme/deşifreleme hızını azaltır. Çok kullanılan anahtar uzunluğu 128 bittir.
Tur Sayısı: Fazla tur sayısı şifreleme güvenliğini artırır .Genel olarak 16 Tur kullanılır.
Alt Anahtar Üretme Algoritması : Karmaşıklığı fazla olan bir alt anahtar üretimi kirptoanalizi zorlaştırır.
Tur Fonksiyonu : Fazla karmaşık olan tur fonksiyonu kriptoanalizi zorlaştırır.

Feistel şifreleyici için diğer özellikler ,
Hızlı yazılım şifreleme/deşifreleme: Çoğu uygulamada, şifreleme uygulamaları veya donanım gerçeklemesi şeklinde kullanım fonksiyonlarının içine koyulur. Dolayısı ile algoritmanın icra hızının düşünülmesi gerekir.
Analiz Kolaylığı : Her ne kadar algoritmanın olası kriptoanaliz saldırılarına karşı olabildiğince karmaşık olması istenirse, bu özellik algoritmanın anlaşılabilirliğini de azaltır. Örneğin DES kolay analiz edilen bir algoritma değildir.

Feistel şifreleyicinin deşifreleme algoritması da aynıdır. Şifreli metin giriş olarak kullanılırken alt anahtar tersinden kullanılır. Yani önce K_n , en son olarak da K_1 kullanılır. Bu özellik nedeniyle Şifreleme ve deşifrelemede farklı algoritma kullanılması gerekmez.
Algoritmanın genel matematiksel hesaplanması; LE_i : Sol şifrelenmiş blok, RE_i : Sağ şifrelenmiş blok, olmak üzere,

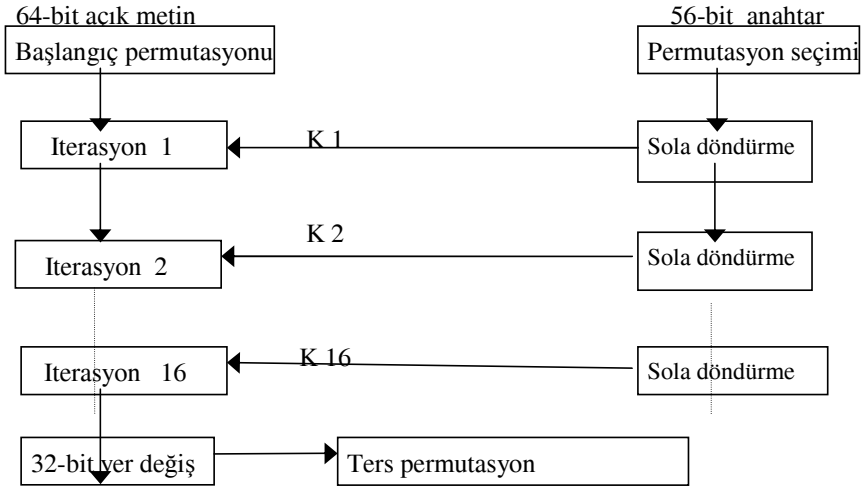
$$LE_i = RE_{i-1}$$
$$RE_i = LE_{i-1} \oplus F(RE_{i-1} , K_i)$$



Şekil 6.10. Klasik Feistel Network

6.11.1 DES

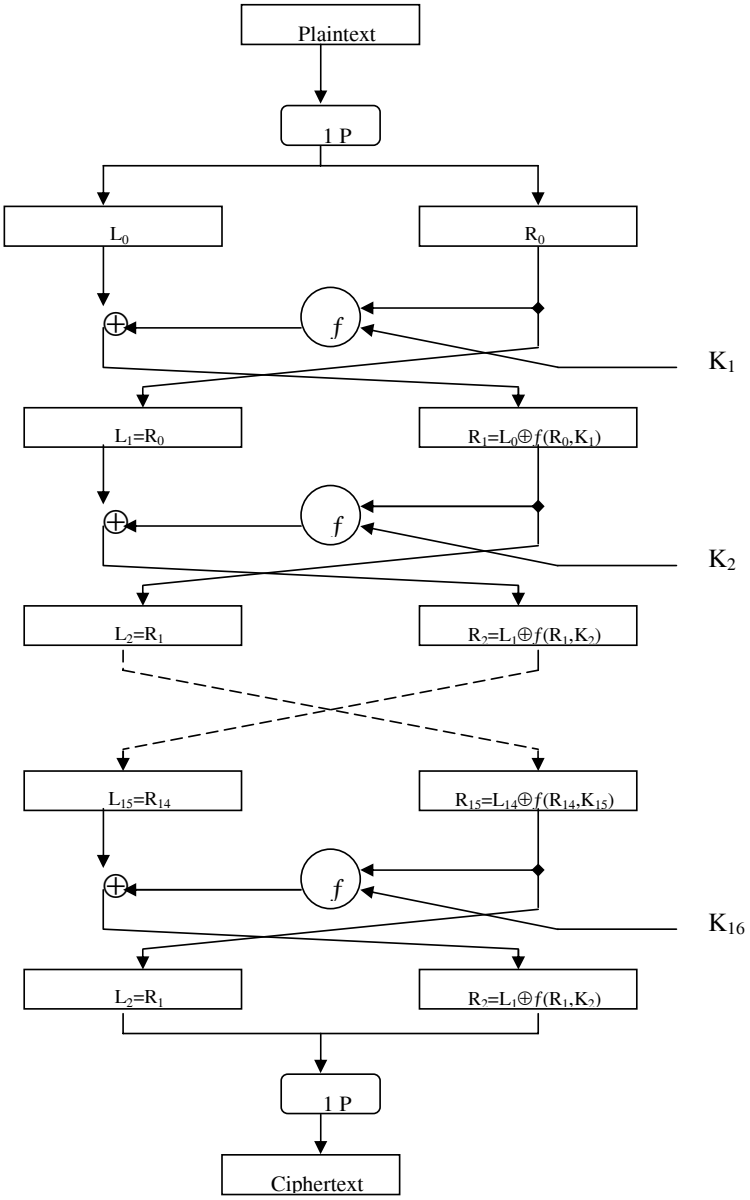
Data Encryption Standart (DES) 1974 yılında IBM tarafından geliştirilmiş ve 1977 yılında yasal olarak atanmıştır. Basit blok şema Şekil 6.11'de gösterilmiştir. Temeli Feistel networküne dayanır.



Şekil 6.11. DES Algoritmasının genel yapısı

DES bir blok şifrelemedir, 64 bit bloklardaki veriyi şifreler. Plain textin 64 bitlik bloğu bir algoritmaya sokulur ve 64 bitlik şifrelenmiş bir ifade elde edilir. Şifrelemede ve şifreyi çözerken her ikisinde de aynı algoritma ve anahtarlar(key) kullanılır.

Anahtar uzunluğu 56 bittir. (Anahtar genellikle 64 bit olarak ifade edilir, fakat her sekizinci bit parity biti olarak kullanılır ve ihmal edilir.) Anahtar herhangi bir 56 bit sayı olabilir ve her zaman değiştirilebilir.



Şekil 6.12 DES Algoritması

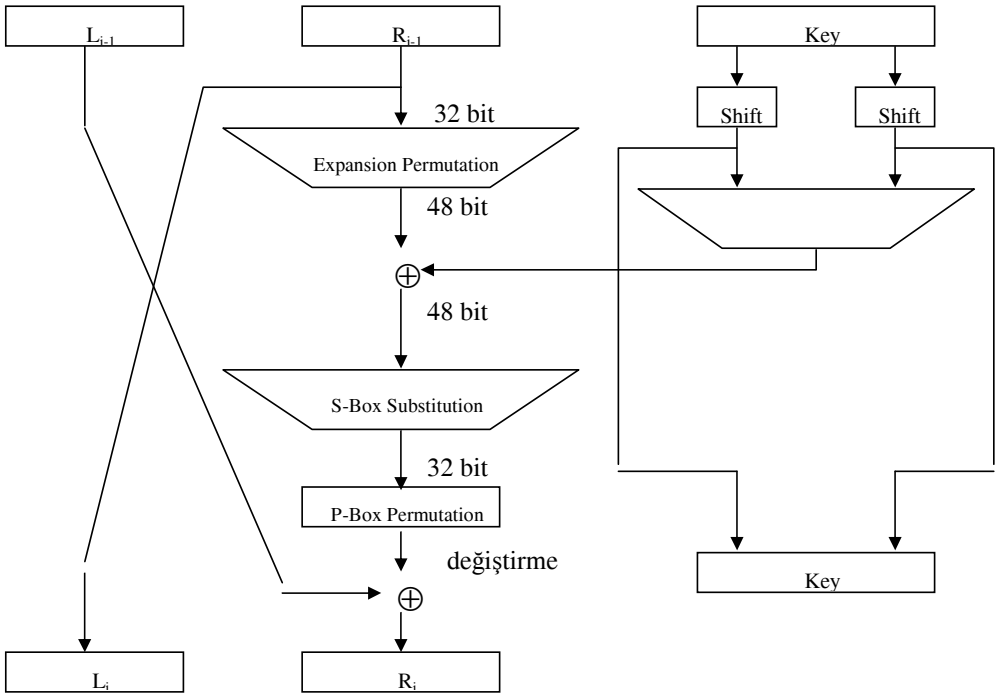
Algoritmanın Özeti :

DES 64 bit blok plaintext de işlem görür. Plaintext, ilk permutasyondan sonra yarısı sağda yarısı solda her biri 32 bit uzunluğunda iki parçaya bölünür. Daha sonra *f* fonksiyonu ve anahtar ile birleştirilerek sonraki adıma geçilir. Aynı işlem 16 kez tekrarlanır ve 16. turun sonunda, sağ ve sol parçalar birleştirilir. Son permutasyondan sonra (başlangıçtaki permutasyonun tersi) algoritma tamamlanarak biter.

Her bir turda anahtar bitleri değiştirilir ve anahtarın 56 bitinden 48 biti seçilir. Verinin sağ yarımı genişleme permutasyonu (expansion permutation) yoluyla 32 bitten 48 bite genişletilir. Genişletilen kısım seçilen 48 bit anahtarla XOR işlemine sokulur. Daha sonra 32 yeni bit üreten 8 S-box içerisine gönderilir ve tekrar değiştirilir. Bu dört işlem *f* fonksiyonunu oluşturur. *f* fonksiyonunun çıktısı verinin sol yarımı ile XOR işlemine tabi tutulur. Sonuçta elde edilen değer yeni sağ yarım olmakta ve sol yarım ise sağ yarımın eski hali olmaktadır. (6.1) de gösterilen bu işlem 16 kez tekrar eder.

$L_i=R_{i-1}$ $\qquad R_i=L_{i-1}\oplus f(R_{i-1},K_i)$ (6.1)

Genel $m_{i+1} = m_{i-1} \oplus f(m_i,K_i)$ (6.2)



Şekil 6.13 DES' in bir turu

Başlangıç Permutasyonu :

Başlangıç permutasyonu tur 1' den önce meydana gelir. Şifrelemeden önce 64 bitlik plain text 32 bitlik iki parçaya bölünür. Tüm çift bitler sol tarafta ve tek pozisyondaki bitler de sağ tarafta yer alır. Tablo 9.3' de tanımlandığı gibi giriş bloklarının yerleri değiştirilir. Tabloda görüldüğü gibi örneğin; başlangıç değişiminde plaintext in 1. pozisyonundaki bite 58 nolu bit taşınmış, 2. pozisyonuna 50 nolu bit atanmış vb...

58 50 42 34 26 18 10 2	57 49 41 33 25 17 9 1
60 52 44 36 28 20 12 4	59 51 43 35 27 19 11 3
62 54 46 38 30 22 14 6	61 53 45 37 29 21 13 5
64 56 48 40 32 24 16 8	63 55 47 39 31 23 15 7

Tablo 6.7 Başlangıç Permutasyonu

Başlangıç permutasyonu ve benzer şekilde sonuç permutasyonu DES' in güvenliğine etki etmez.

Anahtar Dönüşümü :

Başlangıçta, 64 bitlik DES anahtarı her sekiz bit ihmal edildiği için 56 bite düşürülür. Bu tablo 6.8' de tanımlanmıştır. İhmal edilen bu bitler anahtarı kontrol etmek için parity kontrolünde kullanılır. 56 bitlik anahtar elde edildikten sonra DES' in 16 turunun her biri için farklı 48 bit alt-anahtar üretilir. Bu alt-anahtar ler(K_i) şu şekilde belirlenir.

57 49 41 33 25 17 9 1 58 50 42 34 26 18 10 2 59 51 43 35 27 19 11 3 60 52 44 36	63 55 47 39 31 23 15 7 62 54 46 38 30 22 14 6 61 53 45 37 29 21 13 5 28 20 12 4

Tablo 6.8 Anahtar Permutasyonu

İlk olarak 56 bitlik anahtar 28 bitlik iki parçaya bölünür. Turun ihtiyacına göre parçaların bir veya iki biti değiştirilir. Değiştirilecek bit sayıları tablo 6.9' de belirtilmiştir.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
0	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

Tablo 6.9 Turların her biri için değiştirilen anahtar bitlerinin sayısı

Değiştirmeden sonra, 56 bitten 48 biti seçilir. Bu işlemde bitlerin altkümesi seçildiği için, bitlerin düzeni değişir. Bu işlem *compression permutation* olarak adlandırılır. Tablo 6.10' da compression permutation tanımlanmıştır.

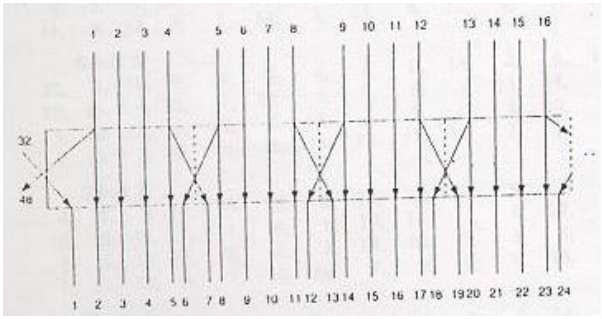
14 17 11 24 1 5 23 19 12 4 26 8 41 52 31 37 47 55 44 49 39 56 34 53	3 28 15 6 21 10 16 7 27 20 13 2 30 40 51 45 33 48 46 42 50 36 29 32

Tablo 6.10 Sıkıştırma Permutasyonu

Genişleme permutasyonu :

Bu işlemde verinin sağ yarısı (R_i) 32 bitten 48 bite genişletilir. Çünkü bu işlem tekrar eden belirli bitleri en uygun şekilde değiştirir. Bu işlem iki amaç için yapılır. XOR işlemi için sağ yarımı anahtar ile aynı uzunlukta yapmak ve yerine koyma (substitution) işlemi sırasında sıkıştırılabilen daha uzun sonuç sağlamak.

Şekil 9.14' de genişleme permutasyonu tanımlanmıştır. Her 4 bit giriş bloğu için, birinci ve dördüncü bitlerin her biri çıkış bloğundan iki biti gösterir, ikinci ve üçüncü bitler ise çıkış bloğundan birer bit gösterir.



Şekil 6.14 Genişleme Permutasyonu

Tablo 6.11'de çıktı pozisyonlarının hangi girdi pozisyonlarına göre nasıl yerleştirildiği görülmektedir. Örneğin; girdi bloğunun 3. pozisyonu çıktı bloğunun 4. pozisyonuna karşılık gelmektedir ve girdi bloğunun 21. pozisyonu çıktı bloğunun 32. pozisyonuna karşılık gelmektedir.

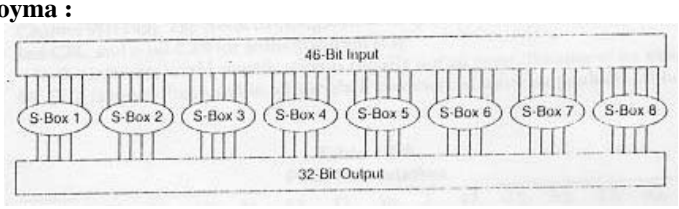
1	2	3	4		5	6	7	8		9	10	11	12		13	14	15	16	
32	1	2	3	4	5	4	5	6	7	8	9	8	9	10	11	12	13	12	13

17	18	19	20		21	22	23	24		25	26	27	28		29	30	31	32	
14	15	16	17	16	17	18	19	20	21	20	21	22	23	24	25	24	25	26	27

28	29	28	29	30	31	32	1												
28	29	30	31	32	1														

Tablo 6.11 Genişleme Permutasyonu

S-Box Yerine Koyma :



Şekil 6.15 S-Box Yerine Koyma

Sıkıştırılmış anahtar genişletilmiş blok ile XOR edildikten sonra, 48 bit yerine koyma işlemine taşınır. Yerine koymalar sekiz tane substitution boxes veya S-boxes tarafından icra edilir. Her bir S-box da 6 bit giriş ve 4 bit çıkış vardır ve sekiz farklı S-box mevcuttur. 48 bit sekiz tane 6 bitlik alt bloğa bölünür. Her bir ayrılan blok, ayrılmış S-box tarafından işletilir. Birinci blok S-box 1, ikinci blok S-box 2 tarafından işleme sokulur.

Her bir S-box 4 satır ve 16 sütundan oluşan bir tablodur. Boxlardaki her bir giriş 6 bit, çıktı 4 bitlik sayıdır. Girişin ilk ve son biti hangi satırın seçileceğini, ortadaki 4 bit ise 16 kolondan hangisinin seçileceğini belirler. Sonuçta tablonun o satır ve sütunundaki elemen çıktı değeri olarak belirlenir. Tablo 6.12'de sekiz S-box un tümü gösterilmiştir.

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
S1 0:	E	4	D	1	2	F	B	8	3	A	6	C	5	9	0	7
1:	0	F	7	4	E	2	D	1	A	6	C	B	9	5	3	8
2:	4	1	E	8	D	6	2	B	F	C	9	7	3	A	5	0
3:	F	C	8	2	4	9	1	7	5	B	3	E	A	0	6	D
S2 0:	F	1	8	E	6	B	3	4	9	7	2	D	C	0	5	A
1:	3	D	4	7	F	2	8	E	C	0	1	A	6	9	B	5
2:	0	E	7	B	A	4	D	1	5	8	C	6	9	3	2	F
3:	D	8	A	1	3	F	4	2	B	6	7	C	0	5	E	9
S3 0:	A	0	9	E	6	3	F	5	1	D	C	7	B	4	2	8
1:	D	7	0	9	3	4	6	A	2	8	5	E	C	B	F	1
2:	D	6	4	9	8	F	3	0	B	1	2	C	5	A	E	7
3:	1	A	D	0	6	9	8	7	4	F	E	3	B	5	2	C
S4 0:	7	D	E	3	0	6	9	A	1	2	8	5	B	C	4	F
1:	D	8	B	5	6	F	0	3	4	7	2	C	1	A	E	9
2:	A	6	9	0	C	B	7	D	F	1	3	E	5	2	8	4
3:	3	F	0	6	A	1	D	8	9	4	5	B	C	7	2	E
S5 0:	2	C	4	1	7	A	B	6	8	5	3	F	D	0	E	9
1:	E	B	2	C	4	7	D	1	5	0	F	A	3	9	8	6
2:	4	2	1	B	A	D	7	8	F	9	C	5	6	3	0	E
3:	B	8	C	7	1	E	2	D	6	F	0	9	A	4	5	3
S6 0:	C	1	A	F	9	2	6	8	0	D	3	4	E	7	5	B
1:	A	F	4	2	7	C	9	5	6	1	D	E	0	B	3	8
2:	9	E	F	5	2	8	C	3	7	0	4	A	1	D	B	6
3:	4	3	2	C	9	5	F	A	B	E	1	7	6	0	8	D
S7 0:	4	B	2	E	F	0	8	D	3	C	9	7	5	A	6	1
1:	D	0	B	7	4	9	1	A	E	3	5	C	2	F	8	6
2:	1	4	B	D	C	3	7	E	A	F	6	8	0	5	9	2
3:	6	B	D	8	1	4	A	7	9	5	0	F	E	2	3	C
S8 0:	D	2	8	4	6	F	B	1	A	9	3	E	5	0	C	7
1:	1	F	D	8	A	3	7	4	C	5	6	B	0	E	9	2
2:	7	B	4	1	9	C	E	2	0	6	A	D	F	3	5	8
3:	2	1	E	7	4	A	8	D	F	C	9	0	3	5	6	B

Tablo 6.12 S-Box lar

P-Box Permutasyonu :

S-box yerine koyma işleminden sonra elde edilen 32 bitlik çıktı P-box da uygun bir şekilde değiştirilir. Bu değişiklikte girdi pozisyonuna göre çıktı pozisyonu tasarlanır. Hiçbir bit iki kez kullanılmaz ve hiçbir bit ihmal edilmez. Bu işlem *straight permutation* olarak çağrılır. Tablo 6.13'de her bir bitin taşındığı pozisyon gösterilmektedir. Örneğin, 21. bit 4. bite taşınmış ve 4. bit 31. bite taşınmıştır.

16 7 20 21 29 12 28 17
1 15 23 26 5 18 31 10
2 8 24 14 32 27 3 9
19 13 30 6 22 11 4 25

Tablo 6.13 P-Box Permutasyonu

En sonunda başlangıçtaki 64 bitlik verinin sol yarımı ile P-box permutasyonu sonucunda elde edilen 32 bitlik veri XOR işlemine sokulmaktadır. Sol ve sağ yarımlar değiştirilerek bir sonraki tur başlamaktadır.

Sonuç Permutasyonu :

Sonuç permutasyonu başlangıç permutasyonunun tersi şekilde çalışır ve tablo 9.10' da tanımlanmıştır. DES' in son turundan sonra elde edilen sağ ve sol yarımlar birleştirilerek ($R_{16}L_{16}$) sonuç permutasyonuna girdi olur. Bu algoritma şifrelemede ve şifreyi çözmede her ikisinde de kullanılır.

40 8 48 16 56 24 64 32 39 7 47 15 55 23 63 31
38 6 46 14 54 22 62 30 37 5 45 13 53 21 61 29
36 4 44 12 52 20 60 28 35 3 43 11 51 19 59 27
34 2 42 10 50 18 58 26 33 1 41 9 49 17 57 25

Tablo 6.14 Sonuç Permutasyonu

Çığ Etkisi :

Bir şifreleme algoritmasında anahtar veya şifresiz metindeki küçük değişikliklerin şifreli metrin üzerinde büyük değişikliğe neden olmasına çığ(avalance) etkisi denir.

DES' in Güvenliği :

Anahtar Uzunluğu ;

Bilindiği gibi DES'in anahtar uzunluğ 56 bittir. Bu ise brute-force atakları için $2^{56} = 7.2 \times 10^{16}$ anahtar sayısı demektir. Tablo 6.2 gözönüne alnırsa, mikrosaniye başına bir çözümleme yapan bir makinenın bin yıl gibi bir sürede DES'i kırabileceğini söylemek mümkündür.

Ancak,1998 yılına özel amaçlı olarak tasarlanan bir "DES kırıcı" bilgisayar($250.000) ile üç günden daha kısa sürede kırılabilmiştir. Bu nedenle anahtar sayısının ortalama yarısı kadar deneme yapılacağı varsayımı ile DES'in brute-force saldırılarına karşı zayıf olduğu söylenebilir.

DES'in alternatifleri olab 3DES ve AES geliştirilmiştir.

DES zamanlama saldırılarına karşı oldukça güçlüdür.

Diferansiyel ve Doğrusal(Lineer) Kiriptoanaliz.

DES'in anahtar uzunluğunun her ne kadar kısa olmasıyla kırılabilirliği fazla ise de daha kısa sürede kırılabilmesi için diferansiyel ve doğrusal kriptoanaliz yöntemleri önerilmiştir.

Difreansiyel Kriptoanaliz

Diferansiyel kriptoanaliz, şifreli metin çiftleri ile onlara ait şifresiz metin çiftleri arasındaki kısmi farkları araştırır. Bu yöntem, aynı anahtar ile şifrelenen şifresiz metin, DES'in turlarında ilerlerken farkının değişimini analiz eder. Diferansiyel kriptoanalizde en yi saldırı 2^{47} adet seçilen şifresiz metin, veya 2^{55} bilinen şifreli metin ve 2^{37} DES işlemi gerektirir.

DES'te şifrelenecek metin bloğu iki eşit parçaya ayrılır ($m = m_0 + m_1$) Her bir çevrimde $2 \le i \le 17$ olmak üzere m_i yeni blok blok elde edilir.

$m_{i+1} = m_{i-1} \oplus f(m_i,K_i)$ (i= 1,2, …….,16)

Diff. Kriptoanaliz

$\Delta m = m \oplus m'$ (Mesaj yarıları)

$\Delta m_i = m_i \oplus m_i'$

$\Delta m_{i+1} = m_{i+1} \oplus m'_{i+1}$

$= m_{i-1} \oplus f(m_i,K_i) \oplus m'_{i-1} \oplus f(m'_i,K'_i)$

$= \Delta m_{i-1} \oplus [f(m_i,K_i) \oplus f(m'_i,K'_i)]$

Eğer biz, Δm_{i-1} ve Δm_i 'yi yüksek bir olasılık ile bilirsek Δm_{i+1} 'i de yüksek olasılık ile bilebiliriz. Eğer bu farklar belirlenebilirse f 'teki alt anahtarların da tahmin edilebilmesi mümkün olabilir.

m ve m' nün her bir çevrimdeki farkları şifreli metin için bulunur.

Diferansiyel Kriptoanalizin işlemi;

İki m ve m' düz metin mesajı için verilen bir fark ile başlanır ve her bir çevrimdeki şifreli metindeki farklar izlenir. Gerçekte 32 bit yarımlık için muhtemel fark ($\Delta m_{17} \parallel \Delta m_{16}$) Sonra bilinmeyen anahtar altındaki şifreli metin arasındaki farkları belirlemek için m ve m' şifrelenir ve muhtemel fark için sonuçlar karşılaştırılır.

$E_K(m) \oplus E_K(m') = (\Delta m_{17} \parallel \Delta m_{16})$

Bütün ara turlardaki muhtemel farklar bulunarak alt anahtarların bitleri tahmin edilir.

Doğrusal(lineer) Kriptoanaliz

Diğer bir yöntem ise doğrusal kriptoanalizdir. Doğrusal kriptoanalizde DES için 2^{47} bilinen şifresiz metin ile ile 2^{47} seçilen şifresiz metin karşılaştırılarak anahtar bulunabilir. Her ne kadar bu küçük bir iyileştirme olsada doğrusal kriptoanaliz kullanılabilir.

Bu yöntemin esası, eğer şifresiz metin bloğunun bitlerine birbiri ile XOR işlemi uygular, şifreli metin bitlerini de birbiri ile XOR'lar ve sonra sonuçlara da XOR işlemi uygulanırsa anahtar bitlerinin bazılarının XOR'lanarak elde edildiği tekbir bir bitlik sonuç elde edilir. Bu doğrusal bir yaklaşımdır ve bir p olaslılığı ile sağlanır. Eğer bu olasılık $p \neq 0,5$ ise, bu işlem anahtarın bulunması için kullanılabilir. Toplanan şifresiz metinler ve karşılığında atanan şifreli metinler anahtar bitlerinin tahmin edilmesi için kullanılabilir. İşlemler aşağıda matematiksel olarak açıklanmıştır.

n bit şifresiz metin ,şifreli metin ve m bit anahtar alalım.

P[1], P[2], ……., P[n] , ve C[1], C[2], ……., C[n]

K[1], K[2], …….., K[m] olsun ve;

$A[i,j,\ldots..,k] = A[i] \oplus A[j] \oplus \ldots\ldots\ldots\oplus A[k]$ tanımlansın.(bitler bir biri ile XOR'lanır)

Doğrusal kriptoanalizin amacı, aşağıdaki şekilde etkin bir lineer denklem bulmaktır.Bu denklemin sonucunun 1 olma olasalığı p'dir. Öyleki; $p \neq 0,5$ ihtimali 0,5 ten farklı olsun.

$P(\alpha_1, \alpha_2,\ldots\ldots\ldots\ldots., \alpha_a,) \oplus C[\beta_1, \beta_2,\ldots\ldots\ldots., \beta_b] = K[\gamma_1, \gamma_2,\ldots\ldots\ldots\ldots\ldots\ldots, \gamma_c]$

Burada x=0,1; $1 \le a$; $b \le n$, $1 \le c \le m$ ve α,β ve γ terimleri sabit bit konumlarını belirtir.

Önce önerilen bağıntı tanımlanır(büyük miktardaki açık ve şifreli metin için) Eğer sonuç çoğunda 0 ise $K[\gamma_1, \gamma_2,\ldots\ldots\ldots\ldots\ldots\ldots, \gamma_c] = 0$ dır. Eğer çoğunda 1 ise $K[\gamma_1, \gamma_2,\ldots\ldots\ldots\ldots\ldots\ldots, \gamma_c] = 1$. Bu bize anahtar bitleri üzerinde doğrusal bir denklem verir. Daha fazla bağıntı bulmayı deneyerek anahtar bitleri tahmin edilebilir.

Zayıf Anahtarlar (Weak Keys):

Algoritmanın her bir turu için başlangıçtaki anahtar değiştirilerek bir alt-anahtar elde edilir. Başlangıçtaki anahtarlar zayıf anahtarlardır. Hatırlanacağı gibi başlangıç değeri iki yarım parçaya bölünmekte ve her bir yarım bağımsız olarak değiştirilmekteydi. Her bir yarımdaki tüm bitler 0 veya 1' den oluşuyorsa, o zaman algoritmanın herhangi bir dönüşümü için kullanılan anahtar, algoritmanın bütün dönüşümleri için de aynı olacaktır. Bu olay, anahtar tamamen 1' lerden, tamamen 0' lardan veya bir yarısı 1' lerden diğer yarısı 0' lardan oluşuyorsa meydana gelir.

Tablo 9.11' de hexadecimal olarak 4 zayıf anahtar örneği gösterilmiştir. (Sekizinci bitler parity biti olarak kullanılmaktadır.)

Zayıf Anahtar Değeri				Gerçek Anahtar	
0101	0101	0101	0101	0000000	0000000
1F1F	1F1F	0E0E	0E0E	0000000	FFFFFFF
E0E0	E0E0	F1F1	F1F1	FFFFFFF	0000000
FEFE	FEFE	FEFE	FEFE	FFFFFFF	FFFFFFF

Tablo 6.15 DES Zayıf Anahtarlar

Tur Sayısı :

Niçin 16 tur? Niçin 32 değil? Beş turdan sonra her şifrelenmiş text biti, her plaintext bitinin ve her anahtar bitinin bir fonksiyonudur. Sekiz turdan sonra şifrelenmiş text, her plaintext ve her anahtar bitinin tamamen rasgele fonksiyonudur.

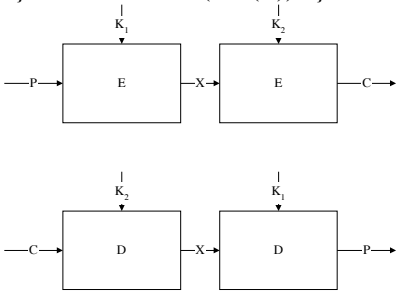
DES 16' dan daha az turda gerçekleştiği zaman, brute force saldırıları olarak bilinen saldırılarla daha kolay ve verimli bir şekilde kırılabilir.

DES'in Farklı Şekilleri :

Double DES :

DES'in iki ayrı anahtar ile arad arda şifrelemede kullanılmasıdır. Bu durumda anahtar uzunluğu 112 bit olacaktır. Brute-Force saldırılarına karşı 2^{112} adet anahtar kombinezonunun denenmesi gerecektir.

Şifreleme $C = E_{K2}(E_{K1}(P))$ Deşifreleme $P = D_{K1}(D_{K2}(C))$ şeklinde olacaktır.



Şekil 6.16. Double DES

Ancak bu şekilde olan şifrelemede anahtar uzunluğu artmasına karşın, Ortada karşılaşma(meet in the middle) saldırılarına zayıflığı vardır.

Ortada Karşılaşma(Meet in the middle attacak) saldırısı

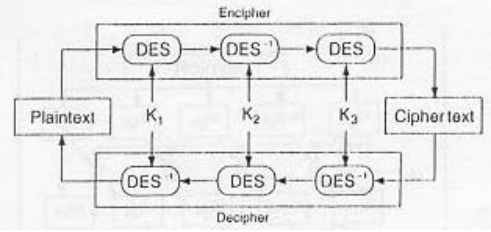
Şekil 6.16.'dan görüldüğü gibi X değerinin hesabı aşağıdaki şekilde yapılabilir.

$X = E_{K1}(P) = D_{K2}(C)$

Verilen bir (P,C çifti ile P, K_1 'in bütün anahtar kombinezonları(2^{56}) ile şifrelenerek X'n değerine göre sıralanır. C yine K_2'nin bütün anahtar kombinezonları(2^{56}) ile deşifrelenerek X'n değerine göre sıralanır. Herikisindede aynı olan X'teki K_1 ve K_2 muhtemel anahtarlardır.

Bunun önüne 3lü DES uygulaması ile geçilebilir. 3DES, bir plaintext'e üç kere DES algoritması uygulayarak şifrelenmiş text elde edilme yöntemidir. (Şekil 6.17) 3DES iki veya üç ayrı anahtar kullanılarak yapılabilir.

$$C = E_{K3}(E_{K2}(E_{K1}(P))) ; \quad P = D_{K1}(D_{K2}(D_{K3}(C)))$$



Şekil 6.17 Triple DES

CRYPT(3) :

UNIX sistemler üzerinde bulunan DES tabanlı algoritmadır. Aslında passwordlar için bir yollu fonksiyon gibi kullanılır, fakat bazen şifreleme için de kullanılır.

Generalized DES :

Generalized DES (GDES), algoritmayı kuvvetlendirmek ve DES'i hızlandırmak amacıyla tasarlanmıştır. Hesap miktarı sabit iken blok boyutu arttırılmıştır.
DES varyanslarına ek olarak DESX, RDES, s^n DES de verilebilir.

6.11.2 IDEA(International Data Encryption Algorithm)

Simetrik blok şifreleme algoritması olan IDEA 1991'de Swiss Federal Institute of Technology 'de geliştirilmiştir. 128 Bit anahtar uzunluğu kullanılır. IDEA alt anahtar üretim ve tur fonksiyonları bakımından DES'ten farklıdır. S-boxes kullanılmaz. XOR , 16 bit tam sayı toplama ve 16 bit tamsayı çarpma matematik işlemlerini kullanır. Kriptoanalizi zor olan bir algoritmadır. Alt anahtar üretim algoritması sadece dairesel kaydırma üzerinedir, fakat her bir sekiz turda altı alt anahtar üreten karmaşık bir yapıya sahiptir. İlk 128 bit anahtar kullanan algoritma olduğu için kriptoanalistlerin üzerinde çok çalıştıkları bir algoritmadır.

6.11.3 BlowFish

Blowfish , bağımsız kriptocu olan Bruce Schneier tarafından 1993'te geliştirildi, kısa zamanda DES'e en popüler alternatif haline geldi. Kolay programlanabilen ve hızlı çalışan bir algoritmadır. Aynı zamanda 5K dan az bellekte çalışan çok karmaşık bir algoritmadır. Anahtar uzunluğu değişkendir ve 448 bit kadar olabilir. Pratikte 128 bit anahtar kullanılır ve 16 tur kullanır.
Blowfish DES gibi S-box ve XOR fonksiyonu kullanır fakat aynı zamanda ikili toplama da kullanır. Sabit S-boxes kullanan DES'in tersine, Blowfish anahtarın bir fonksiyonu olarak üretilen dinamik S-box kullanır.Blowfish'te alt anahtar ve S-box'lar, blowfish algoritmasının anahtar üzerinde tekrarlanarak uygulanmasıyla elde edilirler. Alt anahtar ve S-box'ların üretilmesi için Blowfish şifreleme algoritmasının toplam 512 kere icra edilmesi gerekir. Dolayısı ile çok sık gizli anahtar değişimi gerektiren uygulamalarda blowfish kullanılması uygun değildir.

6.11.4 RC5

RC5, 1994'te RSA asimetrik şifreleme algoritmasını geliştirenlerden birsi olan Ron Rivest tarafından geliştirildi. RC5 Aşağıdaki özelliklere sahiptir.

Donanım veya yazılım ile gerçeklenmeye uygundur.: Mikro işlemcilerde bulunan primitif hesaplama operatörlerine sahiptir.
Hızlılık : Basit ve kelime yönelimlidir. Temel işlemler bir anda verinin bütün kelimesi üzerinde yapılır.
Değişik kelime uzunluklu işlemcilere adapte edilebilirlik: bir kelimdeki bit sayısı RC5'te parametredir. Farklı kelime uzunluklu farklı algoritmalar oluşturur.
Değişken sayıda Tur : Değişken tur sayısı RC5'in diğer parametresidir. Bu parametre daha fazla hız ile daha fazla güvenlik arasında değişim yapar.
Değişken anahtar Uzunluğu : Anahtar uzunluğu RC5'in üçüncü parametresidir. Bu parametre de daha fazla hız ile daha fazla güvenlik arasında değişim yapar.
Basitlik : RC5 kolay programlama için basit bir yapıya sahiptir.
Düşük bellek Gereksinimi: Düşük bellek gereksinimi RC5'i smart kartlar ve sınırlı belleğe sahip diğer benzer cihazlarda kullanımını sağlar.
Yüksek Güvenlik : RC5 uygun parametreler ile yüksek güvenlik sağlar.
Veri bağımlı Döndürmeler: Verinin miktarına bağlı olarak döndürme gerçekleştirir. Bu algoritmanın kripto analistlere karşı gücünü artırır.

6.11.5 CAST-128

CAST 1997'de Entrust Teknolojiler'den Carlise Adams ve Stafford Tavares Tarafından geliştirilen bir tasarım prosedürüdür. Bir özel algoritma 8 bit artımlar ile 40 bitten 128 bit'e kadar değişen anahtar uzunlukları kullanır. CAST, DES'te kullanılanlardan daha uzun olan sabit S-boxlar kullanır. Bu S-boxların tasarımı Kriptoanaliste karşı önemlidir. CAST'taki alt anahtar üretimi diğer blok şifreleyicilerden farklıdır. Doğrusal olmayan S-boxlar kullanılarak alt anahtar üretimi yapılır. CAST-128'in diğer enteresan özelliği tur'dan tur'a değişen F tur fonksiyonudur.

Algoritma	Anahtar Uzunluğu	Tur Sayısı	Matematiksel İşlemler	Uygulamalar
DES	56 Bit	16	XOR, Sabit S-boxes	SET,Kerberos
Triple DES	112 veya 168 bit	48	XOR, Sabit S-boxes	Mali anahtar yönetimi, PGP, S/MIME
IDEA	128 Bit	8	XOR, Toplama, Çarpma	PGP
Blowfish	Değişken, 448 bit	16	XOR, Değişken S-Boxes, Toplama	
RC5	Değişken 2048 Bit	Değişken 255	Toplama, Çıkartma, XOR, Döndürme	
CAST-128	40-128 bit	16	Toplama, Çıkartma, XOR, Döndürme, Sabit S-boxes	PGP

Tablo 6.16. Değişik Simetrik Kriptolama algoritmalarının özellikleri

Gelişmiş Blok şifreleme algoritmalarının Özellikleri

- Değişken anahtar uzunluğu
- Karmaşık aritmetik işlemler
- Veriye bağlı döndürme
- Anahtar bağımlı S-box
- Çok uzunluklu anahtar düzenleme algoritmaları
- Değişken şifresiz/şifreli metin blok uzunluğu
- Değişken tur sayısı
- Her bir turda her iki yarımlık veriye işlem
- Değişken F fonksiyonu
- Anahtar bağımlı döndürme

6.12 Blok Şifreleme Çalışma modları

Simetrik blok şifreleme bir zaman diliminde bir bitlik blok veriyi işler. Veri şifreleme ve üçlü veri şifreleme algoritmalarında blok uzunluğu 64 bittir. Daha uzun veriler 64 bitlik bloklara bölünürler.

ECB(Electronic codebook) modunda şifresiz metin 64 bitlik bloklar halinde işleme aynı anahtar ile girer. Codebook terimi, verilen bir anahtar için her bir 64 bitlik bloğa karşılık sadece bir şifreli metin olduğu için kullanılır.

Bu modda eğer 64 bitlik bloklar metin içerisinde tekrarlanırsa bunlar için aynı şifreli metin üretilecektir. BU ise ECB modu kriptoanaliz açısından güvensiz yapar. Eğer metin her zaman önceden tanımlı alanlar ile başlarsa kriptoanalist açık ve şifreli metin çiftini elde edebilir. Eğer mesaj tekrarlanan elemanları içerirse bu tekrarlama periyodu da kripto analist tarafından tanınabilir.Bunun üstesinden iki alternatif olan CBC ve CFB modlar ile gelinebilir.

6.12.1.1 CBC(Cipher Block Chaining Mode)

Bu modda (CBC) o andaki şifresiz metin bloğu ile bir önceki şifreli metin bloğu, XOR mantıksal işlemine tabi tutulur. Her bir blok için aynı anahtar kullanılır. Böylece şifreli metinde tekrarlanan 64 bitler olmaz.

Deşifreleme için her bir şifreli blok deşifreleme algoritmasından geçer. Sonuç açık metin bloğunu elde etmek için önceki şifreli metin ile XOR'lanır. Bunu görmek için aşağıdaki ifadeyi yazabiliriz:

$$C_i = E_K[C_{i-1} \oplus P_i]$$

Burada $E_K[X]$, X'in K anahtarı kullanılarak şifrelenmiş şekli ve $\oplus$ ise XOR işlemidir. Sonra,

$$D_K[Ci] = D_K[E_K(C_{i-1} \oplus P_i)]$$

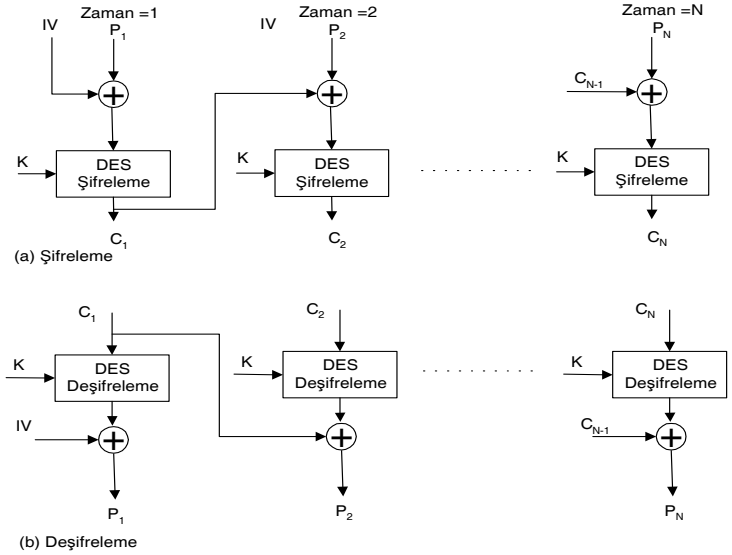
$$D_K[Ci] = (C_{i-1} \oplus P_i)$$

$$C_{i-1} \oplus D_K[Ci] = C_{i-1} \oplus C_{i-1} \oplus P_i = P_i$$

Şekil 6.18 'de görüldüğü gibi, ilk şifreli bloğu elde etmek için başlatma vektörü(IV) ilk açık metin bloğu ile XOR işlemine tabi tutulur. Deşifrelemede ise, ilk şifresiz bloğu elde etmek için IV deşifreleme algoritmasının çıkışı ile XOR'lanır. Burada başlatma vektörü (IV) güvenlik için önemlidir. Bu nedenle şifre gibi korunması gerekir. İlk bloğun şifrelenmesi aşağıdaki ifadede gösterilmiştir.

$$C_1 = E_K(IV \oplus P_i)$$

$$P_1 = IV \oplus D_K(C_1)$$



Şekil 6.18. CBC (Cipher Block Chaining Mode)

6.12.1.2 CFB(Cipher Feedback Mode)

DES tasarımı 64 bitlik blok şifrelemeyi kullanır. Bununla birlikte CFB modu ile DES'i dizi şifreleyici haline dönüştürmek mümkün olmaktadır. Bu yapıda herbir karakterin 8 bit olduğu

varsayımı ile 8 bitlik alt bloklar ile yapılan şifrelemede karakter bazında dizi şifrelemesi gerçekleştirilmiş olmaktadır.
Yine ilk blok için başlangıç vektörü IV kullanılır. IV'ninde ötelenmesiyle 8 bitlik alt vektör ile ilk blok şifrelemesi gerçekleştirilir.
Deşifreleme için düz metin birimini elde etmek için alınan şifreli metin biriminin şifreleme fonksiyonunun çıkışı ile XOR'lanması dışında aynı tasarım kullanılır. Yani deşifrelemede de şifreleme fonksiyonu kullanılır. $S_j(X)$, X'in en yüksek anlamlı bitleri olarak tanımlayalım.Buradan,

$$C_1 = P_1 \oplus S_j(E(IV))$$

Bu nedenle,

$$P_1 = C_1 \oplus S_j(E(IV))$$

Elde edilir. Aynı şekilde sürecin alt adımlarında işlem devam eder.

6.12.2 AES (Advanced Encryption Standard)

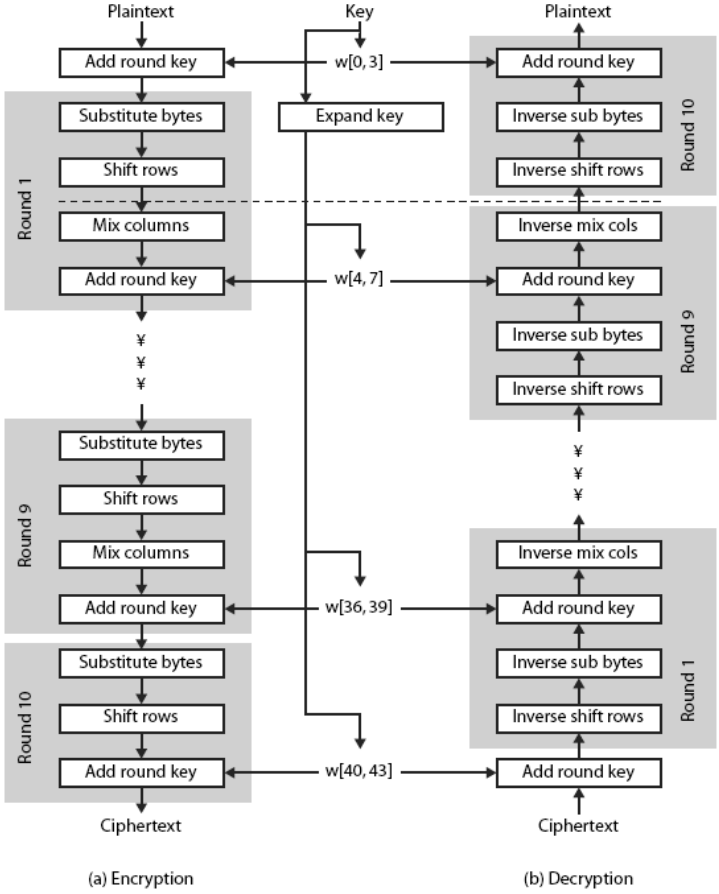
3DES algoritması her nekadar 168 bitlik anahtar kullanıyor ve brute-force saldırılarına karşı yeterli güvenlik sağlıyor ise de üç adet DES'in ard arda çalışması nedeniyle yavaş bir algoritmadır. Bu nedenle NIST 1997'de 3DES'in yerini alacak daha hızlı ve güvenli bir simetrik şifreleme algoritması geliştirilmesini önerdi. Bu çağrı sonunda Belçikadan Dr. Joan Daemen ve Dr.Vincent Rijmen geliştirdiği Rijndael algoritması AES olarak kabul edildi. AES'in önemli özellikleri aşağıda verilmişitir.

1 128 bit veri, 128/192/256 bitlik anahtar uzunluğuna sahiptir.
2 Feistel networkü yerine iteratif olarak çalışır
3 Veriyi dört bayt lık dört sütunluk bloklar halinde işler.
4 Herbir tur'da veri bloğunun tamamı üzerinde işlem yapar.
5 Basit, bilinen saldırılara karşı dirençli, birçok işlemcide hızlı ve kod basitliği sağlayacak şekilde tasarlanmıştır.

Şekil 6.19 'da blok diyagramı gösterilen AES'in çalışması aşağıda özetlenmiştir.

1 DES(Feistel) mimarisinde veri bloğunun yarısı diğer yarısını modifiye etmekte kullanılır, sonra yer değiştirilir. AES(Rijndael) mimarisinde her iki yarı da paralel şekilde işlenir.
2 Sağlanan giriş anahtarı 40 adet dörtlük 32 bitli wordler şeklinde genişletilir w[i]. Dört farklı 128 bitlik kelime herbir turda tur anahtarı olarak kullanılır.
   Herbir turdaki dört farklı everede, bir permutasyon ve üç yer değiştirme kullanılır.
   - Substitute baytları: bloğun bayt bayt yer değiştirmesi için S-box'lar kullanılır(her bayt için bir S-box).
   - Shift-Rows: Basit bir permutasyon(bayt'ları grup ve sütunlar arasında değiştirme)
   - Mix columns: $GF(2^8)$ üzerinde yapılan aritmetiği kullanarak yer değiştirme
   - Add-Round key: Basit bit bit XOR işlemi(mevcut blok ve genişletilen anahtarın turdaki hali ile)
3 Yapı çok basit: Şifreleme ve deşifreleme için şifreleyici add round key evresi ile başlar. Herbiri 4 evre olan 9 tur ile devam eder.
4 Sadece add round key evresi anahtar kullanır. Bu nedenle şifreleyici add round key evresi ile başlar ve biter.
5 Etki olarak add round key evresi bir Vernam şifreleyici gibidir ve çok zor değildir.Diğer üç evre birlikte confusion, diffusion ve doğrusal olmamayı sağlar. Fakat anahtar kullanmadıkları için güvenlik sağlamazlar.
6 Herbir evre kolaylıkla evrilebilir. $A \oplus A \oplus B = B$ gibi
7 Çoğu blok şifreleyicide olduğu gibi deişfreleme algoritması anahtarı ters yönde genişletir. Bununla birlikte deşifreleme algoritması, şifrelemeye benzemez. Bu AES'in parçalı yapısının sonucudur.

8 Dört evre ters çevrilebilir şekilde kurulduğunda deşifrelemenin plaintext'i bulması sağlanır.
9 Son turda , şifreleme ve deşifrelemenin her ikisi de sadece üç evre içerir. Bunlar Substitute bayt, Shift columns ve add round key 'dir. Bu AES'in parçalı yapısının sonucudur ve şifreleyiciyi evrilebilir yapmayı gerektirir.
10 Deşifreleme evreleri:
- Inverse-Shift-Rows:
- Inverse Sub bayts:
- Inverse Mix columns:



Şekil 6.19 : AES Şifreleme ve Deşifreleme adımları

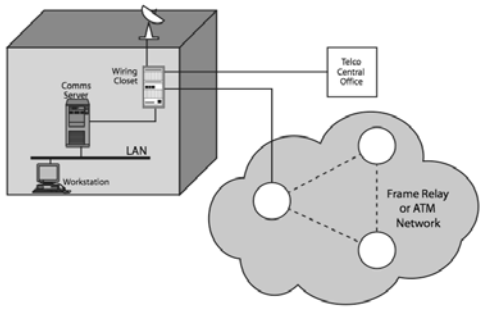
Gizli anahtarlı (simetrik) kriptosistemlerin Güvenliği :

Geleneksel olarak simetrik şifreleme mesaj gizlilğini sağlamak için kullanılır.
İki farklı şifreleme alternatifi vardır.

a. Link Şifreleme : Şifreleme her bir iletişim bağlantısı üzerinde bağımsız olarak yapılır. Bağlantılar arasındaki trafiğin deşifrelenmesi gerekir. Birçok cihaz ve birçift anahtar gerektirir
b. Uçtan uca şifreleme : Şifreleme orijinal kaynak ve son varış noktası arasında yapılır. Her iki uçta paylaşılmış anahtarlar ve cihazlar gerekir.

Şekil 6.20'de gösterilen haberleşme ağı'nda açıklık noktaları belirtilmiştir. YAŞ'ne bağlı olan bir iş istasyonunun gönderdiği mesajlar YAŞ'ın özelliği itibarı ile dinlenmeye müsaittir. Haberleşme sunumcusuna erişim hakkı elde eden bir saldırgan ağ trafiğini dinleyip analiz edebilir. YAŞ 'nin

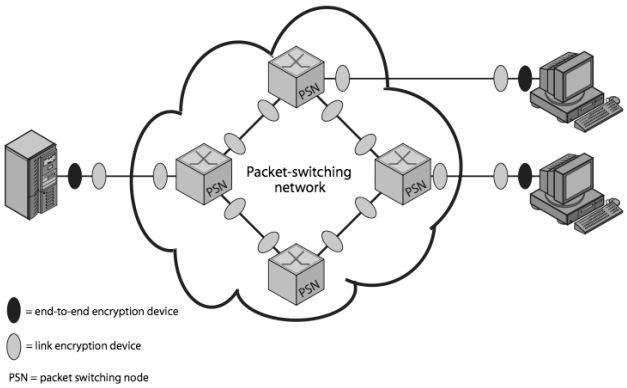
dışında bir yönlendirici veya çevirmeli modem ile dış ağa bağlantı olabilecektir. Bunların bağlantı noktaları zayıf noktalardır. Dış ağdaki herhangi bir haberleşme bağlantısı saldırıya açık yerlerdir. Böylece saldırıya acık bircok nokta bulunduğu görülmektedir.



Şekil 6.20. Açıklık noktaları

Bağlantılara karşı uçtan uca Şifreleme

İletişimde şifreleme için iki yöntem düşünülebilir. Herbir bağlantı yı ayrı ayrı şifreelmek ve uçtan uca haberleşmeyi şifrelemek Şekil 6.21'de bir paket anahtarlamalı ağ'da bağlantıların ve uçtan uca haberlesmenin sifrelenmesi gösterilmistir



Şekil 6.21. Paket anahtarlamalı ağ'da şifreleme

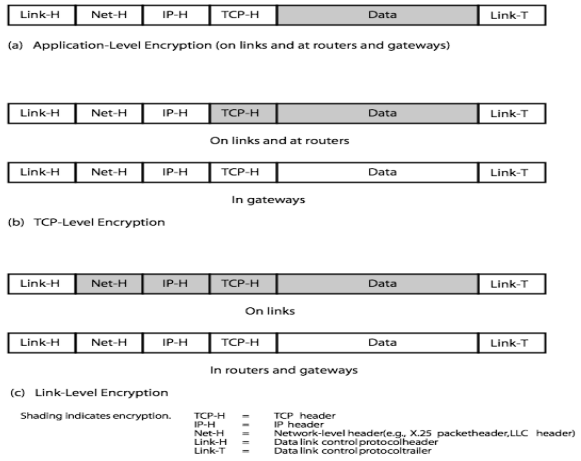
Uçtan uca haberleşme kullanıldıığ zaman başlık şifresiz olarak bırakılmalıdır. Böylece ağ yönlendirme bilgisini doğru olarak sağlayabilir.
Bu nedenle her nekadar, içerik şifrelensede, trafik izi akışını anlamak mümkündür
İdealde heriki şifrelemede

Uçtan uca şifreleme, mevcut veri hattı üzerindeki veri içeriğini şifreler ve kimlik doğrulama sağlar.

Bağlantı ise trafik akışının gözlenmesini engeller
OSI referans modelinin değişik katmanlarında şifreleme fonksiyonu sağlanabilir

Katman 1 ve 2'de bağlantı şifreleme
Katman 3,4,6 ve 7'de uçtan uca şifreleme
Bilgi şifrelenirken anahtar ve içerik ile birlikte daha karmaşık hale gelir.

Şekil 6.22'de gösterilen protokol seviyelerindeki şifrelemelerde üst katmanlarda daha az verinin sifrelendiği. alt katmanlarda ise daha fazla verinin sifrelendiği görülmektedir.



Şekil 6.22: Şifreleme ve protokol seviyeleri arasındaki bağıntı.

Trafik Analizi, iletişim grupları arasındaki haberleşme akışını gözlemektir.
Askeri ve ticari alanda faydalı olabilir
Gizli bir kanal oluştumakta kullanılabilir
Bağlantı şifreleme başlık detaylarını gizler fakat, ağ parçalarında ve uç noktalarda hala gözlenebilir
Trafik padding akışı anlaşılması güç haler getirir fakat, sürekli trafiğin maliyeti artar

Anahtar Dağıtımı

Şimetrik şifreleme yöntemlerinde ortak bir anahtar her iki grup tarafından paylaşılır. Problem, bu anahtarın güvenli olarak dağıtılmasıdır. Güvenli bir sistem sık sık anahtar dağıtım yönteminin kırılmasıyla etkisiz hale gelebilir
Verilen A ve B grupları için değişik anahtar dağıtımı alternatifleri olabilir

A anahtarı seçer ve fiziksel olarak B'ye iletir.
Üçüncü şahıs anahtarı seçer , A ve B'ye dağıtır
Eğer A ve B önceden haberleşiyorsa,önceki anahtarı kullanarak yeni anahtarı şifreler
Eğer A ve B , C ile birlikte güvenli bir iletişim kanalına sahipse, C anahtarı A ve B arasında iletir

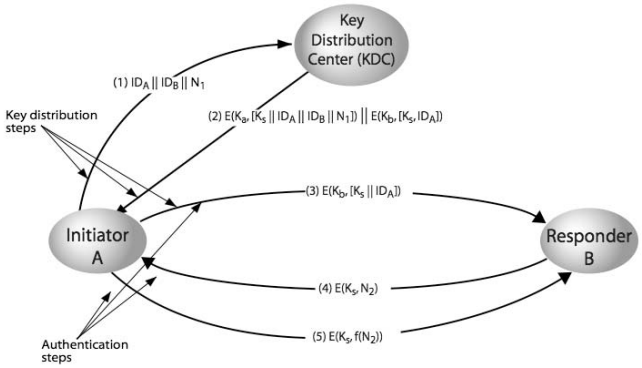
Tipik olarak anahtarların bir hiyerarşisi vardır.
Oturum anahtarı, Herbir oturum için kullanılır. Ağdaki N adet hostun kurabileceği oturum sayısı N(N-1)/2 adettir. Yani N(N-1)/2 adet oturum anahtarı kullanılabilecektir.
Oturum anahtarı;

Geçici anahtardır
Verinin kullanıcılar arasında şifrelenmesi için kullanılır.
Tek bir oturumda kullanılır ve sonra atılır.

Ana Anahtar
Anahtar dağıtım merkezi ile kullanıcılar arasında N adet tir.
Ana anahtar;

Oturum anahtarlarını şifrelemek için kullanılır

Kullanıcı ile anahtar dağıtım merkezi arasında paylaşılır



Şekil 6.23: Anahtar dağıtımı senaryosu

Merkezi olmayan anahtar dağıtımı
Merkezi olmayan anahtar dağıtımında, herbir uç sistem, oturum anahtarı dağıtımı için güvenli bir şekilde haberleşmesi gerekir. Böylece N adet uç sistemin konfigürasyonu için N(N-1)/2 adet ana anahtar gerekebilir.

Oturum anahtarı aşağıdaki adımlar ile sağlanır

- A,B 'den N_1 içeren bir mesaj ile oturum anahtarı ister
- B, ortak olan ana anahtar ile şifrelenmiş şekilde A'ya cevap verir. Mesajda B'nin seçtiği oturum anahtarı ve $f(N_1)$, (N_1+1) , N_2 bulunur
- Yeni oturum anahtarı ile A, $f(N_2)$ 'yi B'ye gönderir.

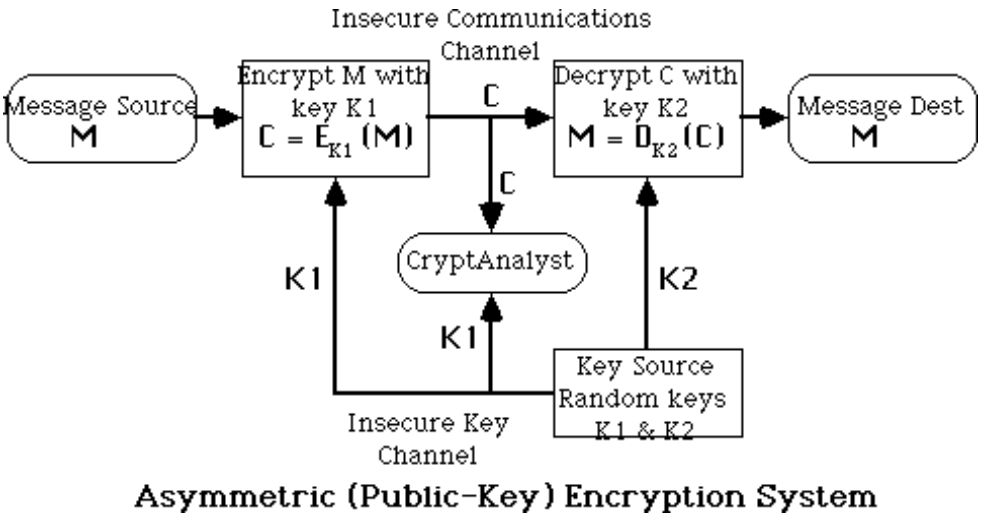
Böylece herbir düğüm ençok (N-1) ana anahtar saklamak zorunda kalır veya gerektiğinde üretilip kullanılır

7 AÇIK ANAHTARLI KRİPTOSİSTEMLER VE SAYISAL İMZALAR (Public Key Cryptosystems and Digital Signatures)

7.1 Açık anahtarlı (asimetrik) kriptosistemler:

Gizli-anahtarlı kripto sistemlerinin aksine Açık-anahtarlı kripto sistemlerinin kullanımı henüz çok yenidir. Açık-anahtarlı kripto sistemleri üzerine ilk öneri, 1976 yılında Diffie ve Hellman tarafından yapılmıştır. Ardından 1977 yılında Rivest, Shamir ve Adleman **RSA** Kriptosistemi adlı yeni bir Açık-anahtarlı kripto sistemini bulmuşlardır. 1978 yılından beri kripto dünyasına değişik teklifler yapılagelmiştir. Bunlardan en önemlileri **El-Gamal** tarafından tasarlanan El-Gamal Açık-anahtarlı kripto algoritması ve eliptik eğri Açık-anahtarlı kripto sistemleridir. Temelde Açık-anahtarlı kripto sistemlerinin gayesi belli bir anahtar üzerinde anlaşmanın ve karşı tarafa bu anahtarı güvenli olarak ulaştırabilmenin zorluğunu ortadan kaldırmaktır. Burada tek yönlü bir mesajlaşma sözkonusudur. Mesaj alıcısı sadece kendisinin bileceği **"Gizli-anahtar"** ve diğer kişilere dağıtabileceği bir **"Açık-anahtar"** dan oluşan anahtar çifti belirler. Kullanılan anahtar üretim algoritmasına göre bu iki anahtar arasında matematiksel bir bağlantı mutlaka olabilecektir fakat asıl amaç, bilinen açık anahtardan gizli anahtarın hesaplanmasının polinomsal zamanda imkansız olabilmesidir.

Mesaj göndericisi alıcıya ait herkesçe bilinen açık anahtarı kullanarak Açık-anahtarlı kripto algoritmasıyla göndereceği mesajı kapatır ve alıcıya gönderir, mesajın alıcısı ise yalnız kendisinin bildiği gizli anahtar ile deşifreleme algoritmasını kullanarak mesajı açabilir. Gizli anahtar yalnız alıcı tarafından bilindiği için başka birinin bu mesajı açması mümkün olamayacaktır. Gizli anahtarın açık anahtardan polinomsal zamanda türetilmesini imkansız kılmak için Diffie ve Hellman' ın "**tek-yönlü fonksiyon**" mantığı üzerine kurulu **Anahtar değişim protokolü** (Key Exchange Method) vardır .



Şekil 7.1 Açık-anahtarlı kripto sistemi

Özellikler

- Geleneksel Gizli anahtarlı kriptografi gönderici ve alıcının birlikte paylaştığı tek bir anahtar kullanır.
- Eğer bu anahtar açıklanırsa haberleşme tehlikeye düşer

- **Açık anahtarlı**(veya çift anahtarlı, asimetrik) kriptografi iki anahtar kullanmayı gerektirir:
  - Mesajları şifrelemekte ve imzaları doğrulamakta kullanılan herkes tarafından bilinebilen bir **açık anahtar**
  - Mesajları deşifrelemekte ve imza oluşturmakta kullanılan sadece alıcı tarafından bilinen bir **gizli anahtar**
- Açık anahtar özel(gizli) anahtardan ve şifreleme hakkındaki diğer bilgilerinden kolaylıkla hesaplanır (Bu bir polinomsal zaman problemidir (P-time))
- Bununla beraber açık anahtarın ve şifrelemenin bilinmesi, gizli anahtarı hesaplamak için hala hesaplama bakımından verimsizdir (NP-time problem)
- Böylece açık anahtar, kendisi ile güvenli haberleşmek isteyen herhangi birisine dağıtılabilir. (her nekadar açık anahtarın güvenli dağıtımı önemsiz olmayan bir anahtar dağıtımı problemidir)
- Açık anahtarlı algoritmaların üç önemli sınıfı vardır.
  - **Açık anahtar Dağıtım Şeması (Public-Key Distribution Schemes** PKDS) burada şema bilginin bir kısmının güvenli olarak değiştirilmesi için kullanılır (değer iki tarafa bağlıdır).
  - Bu değer gizli anahtar şeması için bir oturum anahtarı olarak kullanılır.
  - **İmza Şeması(Signature Schemes)** Sadece sayısal imza üretmek için kullanılır, burada gizli anahtar imzayı üretmekte , açık anahtar ise doğrulamakta kullanılır
  - **Açık anahtar Şeması(Public Key Schemes PKS)** –şifrelemek için kullanılır, burada açık anahtar mesajları şifreler, gizli anahtar mesajları deşifreler
  - Herhangi bir açık anahtar şeması, gerekli olan oturum anahtarlı mesajı seçmek suretiyle PKDS olarak kullanılabilir,.
  - Çoğu açık anahtar şeması aynı zamanda imza şemasıdır(sağlanan şifreleme&deşifreleme her iki sırada yapılabilir.)

7.1.1 Diffie-Hellman Açık anahtar Dağıtım Şeması

- İlk açık anahtar tipi şema PKDS idi ve 1976 da Diffie & Hellman tarafından yayınlandı:
- Bu zamanda mükemmel bir kriptografi üst bakışıdır:
- Açık anahtar dağıtım şemasıdır
  - Herhangi bir keyfi mesajı değiştirmek için kullanılmaz
  - Değeri üyelere bağlı olan bir anahtardır(ve onların açık ve gizli anahtar bilgisi)
- Sonlu bir alanda(Galois) ya bir asal sayının tamsayı modulu veya bir polinomsal alan üzerinde üstelleştirilmesine dayanır.
  - nb üstelleştirme $O((\log n)^3)$ işlem mertebesindedir.
- Güvenliği bu alanlardaki logaritmik hesaplamanın güçlüğüne dayanır
  - nb ayrık logaritma $O(e^{\log n \log\log n})$ işlem mertebesindedir.
- Diffie-Hellman PKDS aşağıdaki şekilde çalışır.
  - Güvensiz bir iletişim kanalı üzerinden bazı anahtarları değiştirmek isteyen iki A& B olsun, Bunlar;:
  - Büyük bir asal sayı seçerler. p (~200 dijit), ve
  - α bir mod p pirimitif elemandır
  - A nın x_A gibi bir gizli sayısı vardır ($x_A < p$)
  - B nin x_B gibi bir gizli sayısı vardır($x_B < p$)
  - A ve B açıklayacakları y_A ve y_B yi sırasıyla hesaplarlar
    - $y_A = \alpha^{xA} \bmod p$ $y_B = \alpha^{xB} \bmod p$
  - Sonra anahtar aşağıdaki şekilde hesaplanır
    - $K_{AB} = \alpha^{xA.xB} \bmod p$ (ortak Gizli Anahtar)
    - $= y_A^{xB} \bmod p$ (**B** hesaplayabilir)
    - $= y_B^{xA} \bmod p$ (**A** hesaplayabilir)

- A ve B arasında güvenli haberleşme için bir gizli anahtarlı şifreleyicide kullanılabilir.
- nb: Eğer iki kişi sonradan haberleşmek isterse kendi açık anahtarlarını değiştirmedikçe aynı gizli anahtara sahip olacaklardır.(genellikle sık olmaz)

7.1.2 RSA Açık anahtarlı Kriptosistem

- En çok bilinen ve en pratik açık anahtarlı tasarım olarak kabul edilen algoritma 1977'de Rivest, Shamir & Adleman tarafından önerildi:
- Mesajları şifrelemek, Anahtar değiştirmek ve sayısal imza oluşturmak için kullanılan bir açık anahtarlı tasarımdır.
- Tamsayı modulo bir sonlu alan(Galois) içinde tamsayı modulo üzerinde üstelleştirmeye dayanır
  - nb üstelleştirme işlemleri $O((\log n)^3)$ mertebesindedir.
- güvenliği,büyük sayıların çarpanlarının hesaplanmasının zorluğuna bağlıdır.
  - nb faktörizasyon işlemleri $O(e^{\log n \log\log n})$ mertebesindedir.
  - (Ayrık logaritma ile benzerdir.)
- Algoritma Kuzey Amerikaya patentlidir. (Bu nedenle dünyanın başka bir yerinde patentlenemez)
  - Bu yöntemin uygulanmasında yasal zorlukların kaynağıdır
- RSA, modüler aritmetiği kullanarak üstelleştirmeye dayanan bir açık anahtarlı şifreleme algoritmasıdır.
- Yöntemin uygulanması için önce anahtarların üretilmesi gerekir.
- Her bir kullanıcı tarafından anahtar üretimi aşağıdakileri içerir:
  - Rasgele çok büyük iki asal sayı seçilir(~100 digit), p, q
  - n = p.q hesaplanır
  - $\phi(n) = (p-1).(q-1)$ hesaplanır.
  - rasgele bir şifreleme anahtarı seçilir öyle ki : ebob($\phi(n)$,e) =1 ; e < $\phi(n)$,
  - deşifreleme anahtarı d hesaplanır: $d = e^{-1} \bmod \phi(n)$, $0 \le d \le n$
  - Açık Anahtar: KA={e,n}
  - Gizli Anahtar :KG={d,n}
- Şifreli metin C'yi elde etmek için M mesajının şifrelenmesi:$C=M^e \bmod n$ $0 \le d \le n$
- M Mesajını elde etmek için C şifreli metnin deşifre edilmesi: $M = C^d$ Mod n dir.
- RSA sistemi aşağıdaki sonuca dayanır:

Eğer n = pq burada p, q farklı büyüklükteki asal sayılardır. Buradan,

$x\ \phi(n) = 1 \bmod n$

Bütün x'ler p veya q tarafından bölünemezler

ve $\phi(n) = (p-1)(q-1)$

7.1.2.1 RSA Örneği

- p=7 ve q= 17 olan iki asal sayı seçilir.
- n = p.q = 119 değeri hesaplanır.
- $\phi(n) = (p-1)(q-1) = 96$ hesaplanır.
- Bir e sayısı seçilir , öyle ki $\phi(n) = 96$ ve ebob($\phi(n)$,e) =1 ; e < $\phi(n)$, buradan e= 5 seçilir,
- Öyle bir d sayısı belirlenir ki, $de = 1 \bmod 96$ ve d < 96 d için doğru değer d= 77 dir.
- Çünkü $77 \times 5 = 385 = 4 \times 96 + 1$
- Sonuçta anahtarlar ; açık anahtar $K_A = \{ 5,119\}$; gizli anahtar ; KG = { 77,119} olacaktır.
- Şifreleme için ise;
  Açık metin olarak M= 19 seçilsin;
  $C=M^e \bmod n$,$19^5 \equiv 66 \bmod 119$ elde edilir. Şifreli metin 66'dır.

- Deşifreleme için;
  $M = C^d \text{ Mod } n$; $66^{77} \equiv 19 \text{mod } 119$ elde edilir ki açık metinin 19 olduğu sonucuna ulaşılır.

7.1.2.2 RSA'nın Güvenliği

- RSA algoritmasının güvenliği, n'nin modülünün çarpanlarına ayrılmasının zorluğuna dayanır,
- En iyi bilinen çarpanlarına ayırma algoritması olan (Brent-Pollard) n sayıs üzerindeki en büyük çarpan p ise

$$O\left(\frac{e^{\sqrt{2 \ln p \ln \ln p}}}{\ln p}\right)$$

işlem mertebesindedir. (Talo 9 .13)

Tablo 7.1

n'deki onlu dijit sayısı	n'nin çarpanlarına ayrılmasındaki işlem(bit) sayısı
20	7200
40	3.11e+06
60	4.63e+08
80	3.72e+10
100	1.97e+12
120	7.69e+13
140	2.35e+15
160	5.92e+16
180	1.26e+18
200	2.36e+19

- Bu 200 dijit uzunluğunda olan n için 1-100 MIPS lik modern bilgisayar için sayı 10^6 ya bölünerek saniye cinsinden zaman hesaplanır.
  - nb: halen 1e+14 işlem hesaplama için elverişililik limiti olarak kabul edilir ve 3e+13 usec/yıl alır.
- Fakat çoğu bilgisayarlar 32/64 bitten daha büyük sayılar üzerinde doğrudan işlem yapamazlar.
- Bu nedenle büyük sayılar üzerinde işlem yapmak için kütüphaneleri kullanılır.

7.1.2.3 Multi-Precision Arithmetic

- Çoklu kelime(multiple precision) sayılar üzerinde çalışan fonksiyon kütüphanelerini kapsar.
- Klasik referanslar "yarı nümerik algoritmalar" olarak bilinir
  - Dijit dijit çarpma yapılır
  - Kare alma ve çarpma ile üs alma işlemi yapılır
- Bilinen kütüphaneler kullanılıp tekerlek yeniden keşfedilmeye uğraşılmamalıdır.
- Modülo aritmetiği özellikle modülo indirgemeler ile özel hünerler kullanabilir.

7.1.2.4 Daha Hızlı modülo İndirgeme

* Chivers (1984), multi-precision aritmetik işlemleri yaparken modülo indirgemeleri yapmanın hızlı bir yolunu gösterdi

Bir b tabanlı n karakterli tamsayı $A(a_0, \ldots, a_{n-1})$ verilsin tamsayı A aşağıdaki gibi gösterilebilir

$$A = \sum_{i=0}^{n-1} a_i b^i$$ buradan

$$A \equiv \left\{ \sum_{i=0}^{n-2} a_i \, b^{i} + a_{n-1} \, b^{n-1} \pmod{jm} \right\} \pmod{m}$$

yukarıdaki ifade, bir sayının En yüksek Anlamlı Dijitinin çıkartılabileceğini ve kalan dijitlere eklenebilen mod m kalanının asıl sayıya mod m uyumlu olan bir sayıda sonuçlanacağını gösterir.

bir sayıyı indirgemek için Chivers algoritması aşağıdaki gibidir:

1. ***R = (b^d, 2.b^d, ... , (b-1).b^d)(mod m)*** *şeklinde Bir dizi düzenle*

2. FOR i = n-1 to d do

WHILE A[i] != 0 do

j = A[i];

A[i] = 0;

A = A + b^{i-d}.R[j];

END WHILE

END FOR

Burada; A[i] A sayısını i" inci karakteridir, R[j] R dizisinden j. tamsayı kalandır.

A daki sembol sayısı n, Modüldeki sembol sayısı d'dir.

7.1.2.5 RSA 'in Hızlandırılması – Değişik Çarpma Teknikleri

- Geleneksel çarpma $O(n^2)$ mertebesinde bit işlemi yapar, daha hızlı teknikler aşağıdakileri içerir:
- Schonhage-Strassen Tamsayı Çarpma Algoritması:
  - Herbir tamsayı bloklara bölünür, ve bir polinomun katsayıları olarak kullanılır.
  - Bu polinomların uygun noktalarda değeri hesaplanır, sonuç değerler çarpılır
  - Çarpım polinomun katsayılarını oluşturmak için bu değerlerin enterpolasyonu alınır.
  - Orijinal tamsayının çarpımını bulmak için katsayılar birleştirilir
  - Enterpolasyon fazını hızlandırmak için Ayrık Fourier dönüşümü ve Katlama (konvolüsyon) dönüşümü kullanılır.
  - O(n log n) bit işleminde çarpma yapılablilir .
- Özel donanım kullanılabilir Çünkü:
  - Elde propagasyon gecikmesi nedeniyle geleneksel aritmetik birimler büyütülemez.
  - Böylece O(n) bit işlemde çarpma yapmak için O(n) kapılı ya paralel elde saklama veya gecikmeli elde-saklama teknikleri kullanılır.
  - Veya, O(log n) bit işlemde çarpma yapmak için $O(n^2)$ kapılı, paralel-paralel teknikler kullanılır

7.1.2.6 RSA ve Chinese Kalan Teoremi

- RSA için deşifreleme hızında anlamlı bir iyileştirme, sırasıyla modulo p ve modulo q çalıştırmak için Chinese kalan teoremini kullanarak yapılır.
  - P ve q yarı büyüklükte olduğu için , n = p.q nin büyüklüğü yarı dır ve böylece aritmetik çok daha hızlıdır.
- Deşifreleme hesabından, iki denklem üretmek suretiyle RSA'de Chinese kalan teoremi kullanılır

$M = C^d \bmod R$

Aşağıdaki gibidir:

$M1 = M \bmod p = (C \bmod p)^d \bmod (p-1)$

$M2 = M \bmod q = (C \bmod q)^d \bmod (q-1)$

Buradan denklem çiftinin

$M = M1 \bmod p \qquad M = M2 \bmod q$

CRT ile aşağıda verilen tek bir çözümü vardır:

$M = [((M2 + q - M1)u \bmod q]^p + M1$

Burada p.u mod q = 1 dir.

7.1.2.7 Pratikte RSA Gerçeklenmesi

- Yazılım ile gerçeklemeler
  - Genellikle 256-512 bit blok uzunluğunda 1-10 bits/saniye de icra edilir
  - Gerçeklemenin iki ana şekli:
    - - Mikrobilgisayarlarda, hibrid bir algoritmada anahtar değiştirme mekanizmasının parçası olarak.
    - - daha büyük makinalarda güvenli bir posta sisteminin elemanları olarak
- Donanım Gerçeklemeleri
  - Genellikle 256-512 bit blok uzunluğunda 100-10000 bits/saniye de icra edilir
  - Bütün bilinen gerçeklemeler büyük bit uzunluklu geleneksel Aritmetik Mantık Birimdir

7.1.3 El Gamal

- Diffie-Hellman anahtar dağıtım şemasının mesajlar güvenli değiştirmeyi
- 1985 de ElGamal tarafından geliştirildi
- Diffie-Hellman ki gibi güvenliği faktör işlemli logaritmaların zorluğuna dayanır.
- **Anahtar Üretimi**
  - Büyük bir asal sayı seçerler. p (~200 dijit), ve
  - α bir mod p pirimitif elemandır
  - A nın x_A gibi bir gizli sayısı vardır ($x_A < p$)
  - B nin x_B gibi bir gizli sayısı vardır($x_B < p$)
  - A ve B açıklayacakları y_A ve y_B yi sırasıyla hesaplarlar
    - $y_A = \alpha^{xA} \bmod p$ $y_B = \alpha^{xB} \bmod p$
- M mesajını C şifreli metni kriptolamak için,
  - Rasgele bir **k** sayısı seçilir, 0 <= k <= p-1
  - **K** mesaj anahtarı aşağıdaki şekilde hesaplanır
    - $K = y_B^k \bmod p$
  - Şifreli metin çifti : C = {c1,c2} aşağıdaki gibi hesaplanır
    - $C_1 = [\alpha]^k \bmod p$ $C_2 = K.M \bmod p$
- Mesajı deşifrelemek için
  - **K** mesaj anahtarı çıkartılır
    - $K = C_1^{xB} \bmod p = [\alpha]^{k.xB} \bmod p$
  - M için aşağıdaki denklem çözülerek **M** elde edilir:
    - $C_2 = K.M \bmod p$

7.2 Açık anahtarlı Şifreleme sistemlerinde Anahtar Yönetimi

Açık anahtarlı şifrelemenin en önemli özelliklerinden birisi anahtar dağıtımı problemine getirdiği çözümdür. Bu çözümler;
Açık anahtarların dağıtımı ve gizli anahtarların dağıtımında açık anahtarlı şifrelemedir.
Açık anahtar dağıtımnda aşağıda gruplandırılan teknikler önerilmiştir.

Açık duyuru yapılması
Açıkça erişilebilen katalog
Açık-anahtar otoritesi
Açık-anahtar sertifikaalrı

Açık duyuru

Açık anahtarlı şifrelemenin önemli noktası, herhangi bir iştirakçinin kendi açık anahtarını diğer bir iştirakçiye gönderebilmesi veya daha geniş bir gruba yayımlayabilmesidir. Bunun ana zayıf

noktası, herhangi birisinin başkasına ait anahtarı üretip yayımlaması, ve bu kişinin tespit edilinceye kadar kendisini gizleyebildiği sahtekarlıktır.

Açık erişilebilir Katalog

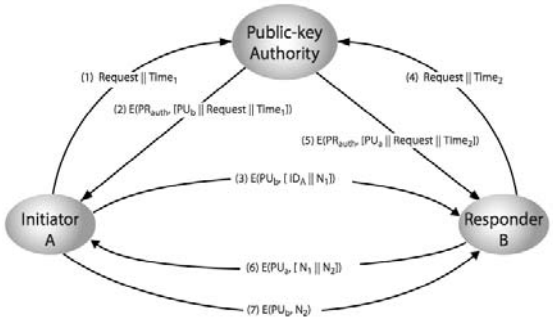
Güvenilği daha yüksek olan diğer bir yöntem ise, açık anahtarların serbestçe erişilebilen bir katalogda duyurulmasıyla sağlanır. Bu katalogların bakım ve dağıtımı, diğer güvenilir bir kuruluşun sorumluluğunda olabilir. Katalog aşağıdaki özelliklerle güvenlidir.

- {Ad,açık-anahtar} girişlerini içerir
- Üyeler, kataloğa güvenli olarak kayıt olurlar
- Üyeler anahtarlarını herhangi bir zamanda geğiştirebilirler
- Katalog periyodik olarak yayımlanır
- Kataloğa elektronik olarak erişilebilir

Bu yöntem, açık duyuruya göre daha güvenilirdir ancak hala karıştırma veya sahtekarlığa karşı zayıflıkları vardır.

Açık Anahtar Otoritesi

Daha güvenli olarak açık anahtar dağıtımının yapılması, açık anahtarların kataloglardan dağıtımının daga sıkı denetimi ile sağlanabilir. Kullanıcının catalog için açık anahtarı bilmesini ve istediği bir açık anahtarı güvenli olarak alabilmesi için catalog ile gerçek zamanda etkileşime girmesi gerekir. Bunun için Şekil 7.2'de gösterilen 7 adet mesajlaşma gereklidir



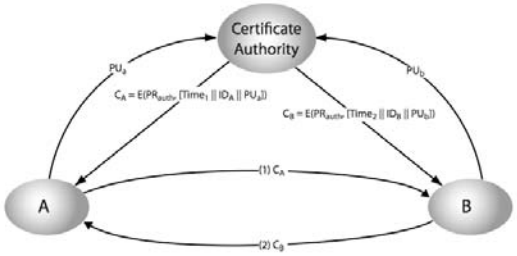
Şekil 7.2. Açık anahtar otoritesi ile anahtar dağıtımı için mesajlaşma

Açık-Anahtar Sertifikaları

Diğer bir geliştirme, anahtarlar bir açık anahtar otoritesinden alınmış olsa dahi, bir açık anahtar otoıritesi ile bağlantı kurmadan anahtar değişimi yapmak için sertifikaların kullanılmasıdır. Bir sertifika, bütün içeriği güvenli açık anahtar veya sertifika otoriteisi tarfından imzalanmış olan açık anahtarın kimlik bilgilerini içeren halidir. Bu, açık anahtar otoritesinin açık anahtarını bilen birisi tarafından doğrulanabilir.

Açık anahtar sertifikaları tarafından onaylanmış olan X.509 standardı uluslararsı kabul görmüş bir yöntem. X.509 sertifikaları,IPSEC, SSL, SET, ve S/MIME gibi güvenlik uygulamalarında sıkça kullanılır.

Bu yöntemle anahtar dağıtımının akışı Şekil 7.3'te gösterilmiştir.



Şekil 7.3 : Sertifikalı anahtar dağıtımı

Gizli Anahtarların açık anahtarlı Dağıtımı

Açık anahtarlar bir kere dağıtıldığı veya erişilebilir hale geldiği zaman, güvenli haberleşme, gizlice dinleme ve/veya karıştırma saldırılarını önlemeyi mümkün kılar. Bununla birlikte birkaç kullanıcı, başarılan nispeten yavaş veri hızları nedeniyle açık-anahtarlı şifreleme sistemlerinin kullanımını haberleşme için pahalı bulabilecektir. Buna bağlı olarak, açık-anahtarlı şifreleme geleneksek şifreleme için gizli anahtar dağıtımı için kullanılabilir. Açık anahtarlı sistemlerin özellikleri aşağdadır.

- Açık anahtarı elde etmek için önceki yöntemler kullanılabilir
- Gizlilik ve kimlik doğrulama için kullanılabilir.
- Fakat açık anahtar algoritmaları yavaştır
- Bu nedenel mesaj içeriğini şifrelemek için genellikle gizli anahtarlı şifreleme kullanılır
- Burada oturum anahtarına ihtiyaç vardır
- Uygun bir oturum sağlamak için birkaç alternatife sahiptir

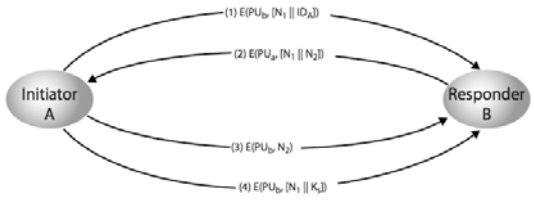
Basit Gizli Anahtar Dağıtımı

Son derece basit bir yöntem 1979 yılında Merkle tarafından önerildi. Fakat bu yöntem, mesajı alıp bir başka mesaj ile değiştirme yapan ortadaki adam saldırlıarına karşı güvensiz idi.

Merkle'nin 1979'daki önersinde;

- Kullanıcı A yeni bir geçici anahtar çifti üretir
- A kullanıcıs, B'ye, açık anahtarı ve kimlik bilgilerini gönderir
- B , bir K oturum anahtarı üretir ve sağlanan açık anahtar ile şifreleyerek A'ya gönderir
- A, oturum anahtarını açar ve her ikisi kullanır

Burada problem, bir başkasının araya girmesi ve protokoloün her iki yarısında rol yapmasıdır. Aktif ve pasif saldırılara karşı güvenli bir anahtar değişim yöntemi Şekil 7.4'de gösterilmiştir. Burada, açık anahtarların güvenli olarak değiştirildiği varsayılmıştır. Mesajlar da heri ki taraf birbirlerinin açık anahtarlarını kullanarak haberlesirler.



Şekil 7.4 Gizli anahtarların açık anahtarlar ile güvenli iletimi

7.3 Eliptik Eğri Kriptografi

Günümüzdeki açık anahtarlı kriptografik uygulamalar başlıca 3 ana matematiksel probleme dayandırılarak geliştirilmektedir. Bu alanlar sırasıyla; bir **tamsayının çarpanlarına ayrılması problemi, ayrık logaritmik problemi ve ve eliptik eğrilerde ayrık logaritma problemi** olarak sınıflandırılmaktadır. Son dönemlerde organizasyonlar , güvenlik gereksinimlerini karşılamak üzere , daha yüksek boyutlu anahtarlara ihtiyaç duymuşlar , bu gereksinim ise gerek hafıza ihtiyacı, gerekse işlem yükü açılarından maliyet ile doğru orantılı olarak organizasyon sistemlerine büyük yük getirmiştir. Eliptik eğri grupları temeline dayanan şifreleme , anahtar boyutları ve transmisyon hızlarında büyük gelişmelere olanak sağlamaktadır

Eliptik Eğri Aritmetiği

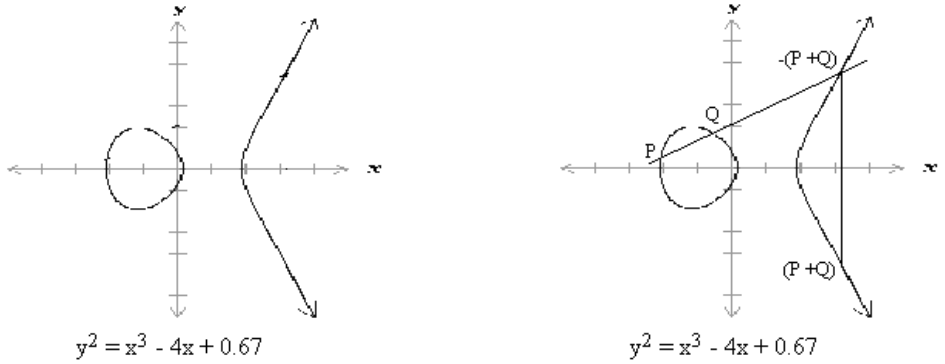
Eliptik Eğri Nedir?

Eliptik eğri çalışmaları matematiğin önemli bir dalıdır. Eliptik eğriler(x,y) düzleminde yavaşça bükülerek çizilebilen basit fonksiyonlardır. Fakat eğrinin (x,y) koordinatlarını kestiği noktaları matematikçiler çalışmaya başlayınca ilginç sonuçlar ortaya çıktı. Eliptik eğri kriptografi eliptik eğri kuramının önemli bir uygulamasıdır

Bir eliptik eğri seçilen belirli a ve b sayıları ile aşağıdaki eşitliği sağlayan (x,y) noktalarının kümesidir.

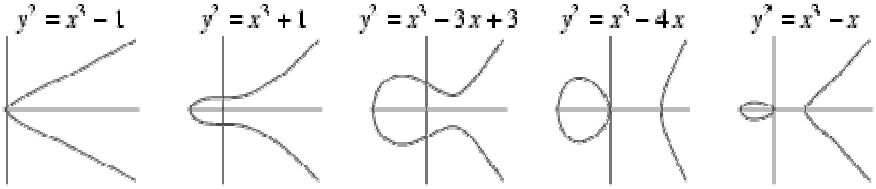
$y^2 = x^3 + ax + b \qquad x,y,a,b \in R$

a ve b tipik olarak tamsayıdır, fakat sistem gerçel sayılar ilede çalışabilir. Eliptik ismine rağmen eğri elips şeklinde değildir. Örneğin a = -4 ve b = 0.67 için eğri denklemi $y^2 = x^3 - 4x + 0.67$. şeklindedir Denklemin sağladığı eğri şekil 7.5'de gösterilebilir.



Şekil 7.5. Eliptik eğri

Değişik a ve b değerleri için elde edilen eliptik eğri şekil 7.6'da gösterilmiştir.



Şekil 7.6. Farklı Eliptik eğiriler

Gerçel sayılar üzerinde bir ECC grubu, sonsuzda özel bir nokta(O) ile birlikte eğri üzerindeki noktaları içerir. Eğer $x^3 + ax + b$ ifadesi tekrarlanan faktor içermiyorsa veya eşdeğer olarak eğer, $4a^3 + 27b^2 \neq 0$ ise eliptik eğri bir grup oluşturmak için kullanılabilir. Bir grup basitçe eğri üzerindeki noktaların kümesidir denilebilir. Grup olması nedeniyle, eğri üzerindeki diğer bir noktayı veren noktalar eklemek mümkündür. Graf üzerinde eğriyi P ve Q

noktalarında kesen bir doğru çizerek iki nokta eklenebilir. Yukarıdaki ifadelerr basitçe eliptik eğriyi tanımlar. Eliptik eğrinin diğer özellikleri olan toplama ve eğri üzerindeki bir noktanın aynılanması sonraki bölümde anlatılacaktır.

Sonlu alan (F_p)üzerinde Eliptik Eğriler

Güvenli verinin önemi nedeniyle şifreleme uygulamaları hızlı hesaplama ve tam çözüm gerektirir. Kriptografide eliptik eğrileri gerçel sayılar üzerinde kullanılması daha fazla yuvarlatma hatası, yavaş hesaplama ve hesaplamada artış getirir. Bu nedenle şifreleme uygulamalarında sonlu alanlar F(p) ve F(2^m) sıkça kullanılır.

Sonlu alan F(p)' nin kısa açıklaması, kendisinin 0 ve p-1 arasında değer alması ile yapılır. Gerçel sayılar kısımındaki kurallar ile aynı şekilde, eğrinin elemanları olan x, y, a, b , F(p) 'nin de elemanları olmalıdır. Eğer $x^3 + ax + b$ nin F_p içinde indirgenemyen polinom olduğu hatırlanırsa, (eğer $4a^3 + 27b^2$ modp$\neq$ 0 ise) eğrimiz bir grup olarak kullanılabilir. Bu tanımlamalar ile F_p üzerindeki bir eliptik eğri grubu eğri üzerindeki noktalara ilaveten sonsuzdaki noktadan meydana geldiği söylenebilir. Kriptografik hesaplalmalarda bazı cebrik kurallar eliptik eğriler için uyarlanabilir.

İki farklı P ve Q noktasının eklenmesi:

$P = (x_p , y_p)$ noktasının negatifi $- P = (x_p , - y_p)$ 'ye eşitti.

İki noktanın toplamı olan P + Q = R hesaplamak için aşağıdaki denklem çifti kullanılarak eğrideki yeni noktanın koordinatları hesaplanır.

$X_r = [\lambda^2 - x_p - x_q]$ modp

$y_r = [- y_p + \lambda(x_p - x_r)]$ modp

burada $\lambda = (y_p - y_q)/ (x_p - x_q)$ iki noktanın eğimidir.

Bir noktanın Aynılanması

$P = (x_p , y_p)$ noktasının aynılanması için aşağıdaki denklem çifti kullanılır.

$X_r = [\lambda^2 - 2x_p]$ modp

$y_r = [- y_p + \lambda(x_p - x_r)]$ modp

burada $\lambda = (x_p^2 - a) / (2y_p)$ eğimdir ve a 'da eğri parametresidir.

Eğri üzerindeki bir noktayı bulmak ve bu noktayı aynılayarak neticede sonsuzdaki (O) noktasının bulmak için, nokta sonsuzdaki noktaya ulaşıncaya kadar kendisine eklenir, eklenme sayısına noktanın derecesi denir.Kriptografik uygulamalarda, şifreleme süreci için global açık parameter olan temel nokta yüksek dereceden bir nokta olarak seçilir.

Eliptik Eğri Kriptografi (ECC)

1985 'de Neal Koblitz ve Victor Miller tarafından bulunan sonlu alanlar üzerinde eliptik eğrilerdeki ayrık logaritma denetlenemez görünümündedir. Eliptik eğri ayrık logaritma problemi(ECDLP) aşağıdaki şekilde açıklanabilir:

- P, büyük asaldır ve büyük dereceli P, E eğrisi üzerindedir.
- x.P , P'nin skaler çarpımı olarak verilsin, x kere (aynı zamanda P'nin x kere kendi üzerinde toplanmasıdır.)
- Q, x.P = Q 'i sağlayan eğri üzerindeki diğer bir noktadır.
    - Eptik eğri ayrık logaritma problemi, verilen P ve Q için x değerinin bulunmasıdır.

Eliptik eğri Anahtar Değişimi:

Eliptik eğri kullanrak anahtar değişimi aşağıdaki şekilde gerçekleşir.

Öncelikle, asal sayı olacak şekilde bir $p \approx 2^m$ (kriptografi pratiği için m>150, m=180) (Sonlu alan F(2^m) için) ve eliptik eğri denklemi için a, b'yi seçmek gerekir. Bu $E_p(a,b)$ noktalarının bir eliptik grubunu tanımlar. Sonra, $E_p(a,b)$ içinde bir üretici nokta olan $G = (x_1, y_1)$ seçilir. G'nin seçiminde önemli nokta, en küçük n değerinde nG=O çok büyük asal sayı olmalıdır. $E_p(a,b)$ ve G parametreleri bütün üyeler tarafından bilinirler. Seçilen bu parametreler ile anahtar değişimi aşağıdaki şekilde yapılır.;

A, n_A < n.olacak şekilde bir tamsayı seçer. Sonra $P_A = n_A \times G$ 'yi hesaplar

n_A = A 'nın gizli anahtarı

P_A = A 'nın açık anahtarı

Aynı yöntem ile, B, n_B < n.olacak şekilde bir tamsayı seçer. Sonra $P_B = n_B \times G$ 'yi hesaplar

n_B = B 'nın gizli anahtarı

P_B = B'nin açık anahtarı

Sonra her kullanıcı için sistemin ana gizli anahtarı üretilir.

$K = n_A \times P_B \quad \Rightarrow$ kullanıcı A için

$K = n_B \times P_A \quad \Rightarrow$ kullanıcı B için

Basitçe gösterilebilir ki;

$K = n_A \times P_B = n_A \times (n_B \times G) = n_B \times (n_A \times G) = n_B \times P_A$ dır

Bu algoritmada ayrık logatirma problemi(kriptoanaliz) verilen G ve K.G ile K değerini çözmektir ki oldukça zordur.

Örnek olarak p=211, $E_p(0,-4)$ ile $y^2 = x^3 - 4$ denklemine eşittir. ve G=(2,2) dir. Birisi $241G = O$ hesaplayabilir. A'nın özel anahtarı n_A = 121, böylece A'nın açık anahtarı P_A =121(2,2) =(115,48) dir. B'nın özel anahtarı n_B = 203, böylece B'nın açık anahtarı P_B =203(2,2) =(130,203) dür. Paylaşılan anahtar ise 121(130,203) = 203(115,48) = (161,169) dur.

Ana gizli anahtarın x,y koordinatlarından ibaret olan iki değere sahip olduğu görülür. Geleneksel kriptorafide tek bir K değeri(ya x yada y değeri) kullanılacaktır.

Eliptik Eğri ile Şifreleme/Deşifreleme:

Literatürde eliptik eğrileri kullanarak değişik mesaj şifreleme/deşifreleme yaklaşımı mevcuttur. Burada en basit olan yaklaşım ele alınacaktır. Yaklaşımlardan diğeri Elliptic Curve ElGamal yöntemidir.

- Anahtar değişim sistemindeki gibi , bir şifreleme/deşifreleme sistemi de parametre olarak bir G noktası ve bir E_q (a, b) eliptik grup gerektirir.
- Her A ve B kullanıcısı birer gizli anahtar n_A ve n_B seçer ve $P_A = n_A \times G$ ve $P_B = n_B \times G$ yi açık anahtarları olarak hesaplarlar.
- Bir P_m mesajının şifrelenmesi için, gönderici (bu örnekte kullanıcı A) rastgele bir k tamsayısı seçer ve C_m şifreli metini iki parça olarak aşağıdaki şekilde üretir;
- $C_m = \{k.G, P_m + k.P_B\}$
- Burada gönderici şifrelemek için alıcının açık anahtarını kullanır.
- Deşifreleme işleminde alıcı k.G'yi kendi gizli anahtarı ile çarpar ve şifreli metinden çıkartır. İşlem aşağıdaki eşitlikte gösterilmiştir;

$$P_m + k.P_B - n_B.(k.G) = P_m + n_B.k.G - n_B.k.G = P_m$$

Anahtar değişimi örneğinde görüldüğü gibi ayrık logaritma problemi buradada k'nın verilen G ve kG den elde edilmesi ile aynıdır.

Örnek olarak: p=751; E_p (-1, 188), alınırsa eğri $y^2 = x^3 - x + 188$ olur; ve G=(0,376).
A'nın B'ye , P_m (562,201) eliptik noktasında şifreli bir mesaj göndereceğini ve A'nın k=386 seçtiğini farzedelim. B'nin açık anahtarı P_B=(201,5) dir. Buradan 386(0,376) = (676,558) ve (562,201) + 386(201,5) = (385,328) elede edilir. Böylece A şifreli metin olarak {(676,558),(385,328)} gönderir.

Eliptik Eğri Şifrelemenin Güvenliği

Günümüzdeki kriptografi algoritmalarında, açık anahtarlı kriptosistemler genellikle simetrik anahtarlı kriptosistemler için anahtar iletminde kullanılır. Son yıllarda organizasyonların 3DES'ten AES'e yöneldikleri görülür. Bu organizasyonlar da 1024 bit RSA genişçe kullanılırlar. Gelişmeler 2048 bit gibi daha uzun anahtar kullanımına yönelmeyi gerektirmektedir. Bu ise daha fazla bellek, maliyet ve hesaplama artışı demektir. Daha fazla güvenlik ndeniyle anahtar uzunluğunun artırılmasına karşı olarak eliptik eğri şifreleme kullanılarak anahtar değişimi ve şifrelemede bu problem giderilebilir. Tablo 7.2'de RSAve ECC 'nin farklı simetri şifreleme algoritmaları ile kullanıldığındaki anahtar uzunluğu bakımından karşılaştırılması görülmektedir.

Tabloyu incelediğimizde Aynı güvenlik seviyelerinde ECC'nin RSA' e göre anahtar uzunluğunun daha küçük olmasıyla daha az bellek gerektirdiği görülür.

Anahtar Uzunluğu	**Simetrik şifreleme Algoritması**	**RSA**	**ECC**
80		1536	160
112	3DES	4096	224
128	AES-128	6000	256
160	AES-192	10000	320

Tablo 7.2. Şifreleme algoritmalarının karşılaştırılmaları

Geleneksel ve açık anahtarlı şifreleme yöntemlerinin krşılşatırması tablo 7.3'te gösterilmiştir.

Geleneksel kriptolama(Gizli Anahtarlı)	**Açık anahtarlı Kriptolama**
Çalışma gereksinimi	***Çalışma gereksinimi***
Aynı algoritma aynı anahtar ile birlikte şifreleme ve deşifreleme ile birlikte kullanılır .	Bir algoritma ve iki anahtardan birisi şifreleme diğeri ise deşifreleme için kullanılır.
Gönderici ve alıcı algoritma ve anahtarı paylaşır.	Gönderici ve alıcının her biri, uygun anahtara sahip olmalıdır.
Güvenlik Gereksinimi	***Güvenlik Gereksinimi***
Anahtarın gizliliği korunmalıdır	İki anahtardan birisi gizlidir.
Başka bir bilgi gerektirmeden mesajı çözmek mümkün veya çok kolay olmalıdır.	Başka bir bilgi olmadan mesajın çözülmesi mümkün değil veya, çok kolay olmamalıdır.
Algoritma ve şifreli metin bilgisi anahtarı tahmin etmede yeterli olamamalıdır	Algoritma, şifreli metin bilgisi ve anahtarın birisinin elde edilmesi diğer anahtarı tahmin etmek için yeterli olmamalıdır.

Algoritma	*Enc/Dec*	*Sayısal İmza*	*Anahtar Değişimi*
RSA	**evet, Büyük bloklar için pratik değil**	**Evet**	**Evet**
LUC	**evet, Büyük bloklar için pratik değil**	**Evet**	**Evet**
DSS	**Hayır**	**Evet**	**Hayır**
Diffie-Hellman	**Hayır**	**Hayır**	**Evet**

Tablo 7.3. Simetrik ve asimetrik şifreleme özellikleri

7.4 Mesaj Doğrulama ve Özetleme Fonksiyonları (Hashing Functions)

Mesaj Doğrulama

Buraya kadar mesaj içeriğinin şifrelenmesiyle korunması üzerinde duruldu. Bu bölümde göndericinin doğrulanması yanında mesaj içeriğinin bütünlüğünün(değiştirmelere karşı) nasıl korunacağı üzerinde durulacaktır. Genellikle mesaj bütünlüğünün korunması elektronik ticaret uygulamalarında gizlilikten daha önde gelen bir husustur. Mesaj doğrulama şu kavramlari içerir. Mesaj bütünlüğünün korunması, göndericinin kimliğinin geçerliliği ve mesaj kaynağının kendisni inkar edememesi(non repudation). Bir doğrulayıcı üretmek için kullanılabilen üç adet fonksiyon vardır. Bunlar;

Mesaj şifreleme :(Şifrelenen mesaj onun doğrulanması görevini yapar

Mesaj doğrulama kodu(MAC): (Bir fonksiyon ile bir anahtar ile sabit uzunluklu olarak üretilen değer doğrulama için kullanılır

Hash(özet) fonksiyonu: (Herhangi uzunluktaki bir mesajdan açık bir fonksiyon ile üretilen sabit uzunluktaki özet değer doğrulama için kullanılır.

Güvenlik gereksinimleri

Bi ağdaki haberleşmenin içeriğinde aşğıda listelenen saldırılar tanınabilir.

İlk iki gereksinim mesaj gizliliği içerisinde değerlendirilir ve açıklanan şifreleme yöntemleriyle sağlanır. Diğer gereksinimler mesaj doğrulama içerisinde kalır. Bu noktada, kaynağından gelen mesajın değiştirlmemiş olması önemlidir. Aynı zamanda adres dizisi ve zamanlamadır. Sayısal imzanın kullanımı kaynağın inkar edilmesi ile ilgilidir.

- Mesaj içeriğini açıklama (Disclosure)
- Ağ trafiğinin analizi(traffic analysis)
- Gerçeği gizleme(masquerade)
- Mesaj içeriğini değiştirme(content modification)
- Mesaj sırasını değiştirme(sequence modification)
- Mesaj zamanlamasını değiştirme(timing modification)
- Kaynağın inkar edilmesi(source repudiation)
- Varışın inkar edilmesi(destination repudiation)

Mesaj şifreleme

Mesaj şifrelemenin kendisi, doğrulama işlevini sağlayabilir. Burada ,mesajın bütününün şifrelenmesi, sadece uygun anahtarları bilenlerin mesajı şifreleyebilmesi nedeniyle onun doğrulayıcısı olabilir. Böylece geçerli olan mesaj anlaşılabilir.(mesajın uygun yapıda olması veya değişikliğe karşı denetim bilgisi(checksum) bulunması).

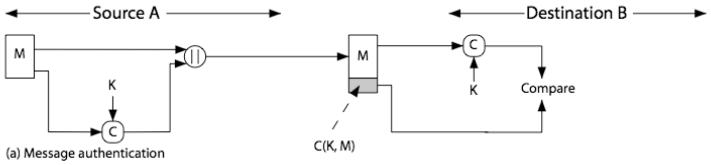
- Eğer simetrik şifreleme kullanılmış ise:
  - Alıcı, mesajın gönderici tarafından oluşturulduğunu bilir.
  - Kullanılan anahtarı sadece gönderici ve alıcı bilir
  - Eğer mesaj, denetim bilgisi içeren uygun yapıda ise, mesajın içeriği değiştirilemez

Açık anahtar teknikleri ile, sadece anahtar sahibi tarafından üretilebilien, sayısal imzalar kullanılabilir. Fakat mesajın sonunda iki açık anahtar işlemi gerekir.

Mesaj Doğrulama Kodu(MAC)

Diğer bir doğrulama tekniği, bir gizli anahtar ile sabit uzunlukta üretilen ve kriptografik control verisi veya Mesaj doğrulama kodu olarak bilinen ve mesajın sonuna eklenen bir veri bloğu ile yapılır. Bu teknikte, A ve B olarak adlandırılan iki haberleşme grubu bir K ortak anahtarını paylaşır. Bir MAC fonksiyonu ,şifrelemeye benzeyen ve deşifrelemede olduğu gibi ters çevrilme gerektirmez. Bu sonuç mesajın sonuna eklenir.

- Alıcı mesaj üzerinde aynı hesaplamayı yapar ve sonucu MAC ile karşılaştırır.
- Böylece göndericiden gelen mesajın değiştirilmediğini garanti eder. (Şekil 7. 7)



Şekil 7.7 : Mesaj doğrulama kodunun çalışması

Doğrulama ve gizliliği birlikte sağlamak için MAC şifreleme ile birleştirilebilir. Sadece doğrulama gerekli ise MAC kullanılır.
Gönderici ve alıcının her ikisi de anahtarı paylaştığı ve üretebildiği için MAC sayısal imza değildir.

MAC özellikleri
Bir C fonksiyonu tarafından üretilen bir MAC aynı zamanda kriptografik denetim bilgisidir. MAC kaynakta mesajın sonuna eklenir ve varışta yeniden hesaplanarak doğrulama yapılır.
MAC fonksiyonu,birçok farklı uzunluktaki mesajı aynı uzunluktaki özet değere dönüştürdüğü için çoktan bire bir fonksiyondur.

- Bir MAC kriptografik denetim değeridir(checksum)
  MAC = CK(M)
  - Değişken uzunluktaki M mesajını bir gizli K anahtarı kullanarak sabit uzunluktaki bir doğrulayıcıya şeklinde sıkıştırır
- CK bir çoktan bire fonksiyondur, bu fonksiyon ile potansiyel olarak birçok mesaj aynı MAC değerine sahip olabilir fakat bu sonucu elde etmek çok zordur.

MAC gereksinimleri
Bir MAC fonksiyonunun güvenliğini değerlendirmek için ona karşı olabilen saldırıları düşünmek gereklidir. Bundan sonra listelenen gereksinimleri sağlamak gereklidir.
İlk gereksinim, saldırganın anahtarı bilmese dahi,verilen MAC ile uyuşan bir başka mesajı oluşturduğu mesaj yerine koyma saldırısı ile ilgilidir.
İkinci gereksinim, seçilen bir şifresiz metin tabanlı brute-force saldırısını önlemeyle ilgilidir.
Son gereksinim, doğrulama algoritmasının, mesajın belirli bir parçasının diğerlerine göre daha zayıf olmamasını dikte eder. Özetle;

- Saldırı çeşitlerini dikkate alır
- MAC aşağıdakileri sağlamalıdır:
  1. Bilinen bir mesaj ve MAC için aynı MAC'a sahip bir başka mesaj bulunması verimsiz olmalıdır.
  2. MAC, düzenli dağıtılmış olmalıdır
  3. MAC, mesajın bütün bitlerine bağlı olmalıdır

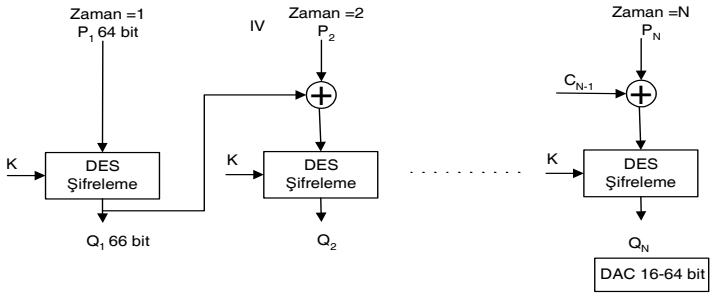
DES'teki block cipher chaining modu, son bloğu göndermek suretiyle ayrı bir doğrulayıcı üretilmesinde kullanılabilir. Bu, DES-CBC tabanlı veri doğrulama algoritması(DAA) ile yapılır.(Şekil 7.8.)
Algoritma, DES'in şifre blok zinciri(CBC) çalışma modu olarak bir sıfır başlangıç vektörü ile tanımlanabilir. Yetkilendirilecek veri, 64 bitlik bloklar şeklinde gruplandırılır. D1,D2, Dn
.Eğer gerekliyse, son blok, 64 bit elde etmek için sağına sıfır koyularak düzenlenir. DES kriptolama algoritması kullanılarak, E, ve gizli anahtar K, bir veri yetkilendirme kodu(DAC) aşağıdaki şekilde hesaplanır.

- $O_1 = Ek\ (D_1)$
- $O_2 = Ek\ (D_2 \oplus O_1)$
- $O_3 = Ek\ (D_3 \oplus O_2)$

……

- $O_n = Ek(D_n \oplus O_{n-1})$

DAC, ya bütün bloğu içerir yada, en soldaki M biti 16<= M <=64.olarak içerir



Şekil 7.8 : DES CBC modunun MAC üretim için kullanılması

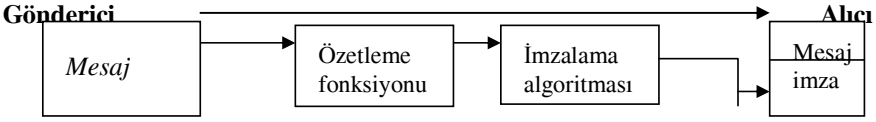
Hash Fonksiyonları

Temel kriptografik terimlerden biri "Kriptografik özetleme fonksiyonu" veya diğer adıyla tek yönlü özetleme fonksiyonu (one-way hash function) dur.

Tanım : Değişik uzunluktaki bit dizilerini sabit uzunluklu bit dizilerine taşıyan polinomsal zamanda kolay hesaplanabilen fonksiyona "Özetleme fonksiyonu" denir. Görüntü kümesindeki sabit uzunluklu oluşan bu bit dizisine ise "Özet-değer" (Hash-value) adı verilir.

Kriptografik olarak Özetleme fonksiyonları değişken m uzunluklu mesajları sabit n uzunluklu mesajlara indirgemek amacıyla kullanılırlar ($m>n$). Seçilen h özetleme fonksiyonu iki farklı m_1 ve m_2 mesajlarını aynı özet değerine taşımamalı ($h(m_1) \neq h(m_2)$) ve verilen bir y özet-değerinden bu değere ait m mesajı polinomsal zamanda hesaplanamamalıdır.

Özetleme fonksiyonlarının kriptografide kullanımı daha çok sayısal imza ve veri bütünlüğünün korunması alanlarında yaygındır. Sayısal imza uygulamalarında uzun mesajlar öncelikle bilinen bir Özetleme fonksiyonu ile sabit uzunluklu kısa bir diziye özetlenmeli ve bu özet-değer imzaya girmelidir.



Şekil 7. 9 Şifrelenmemiş bir mesajın bütünlüğünün ve doğruluğunun korunması için özetlenip imzalanması.

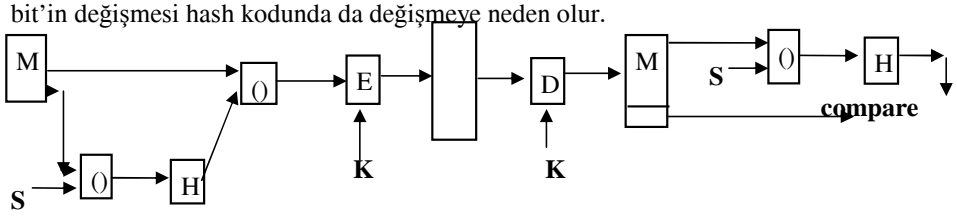
Özetleme fonksiyonu bilginin bütünlüğünü sağlamak için de kullanılabilmektedir. Fonksiyonun tanım kümesindeki her mesajı görüntü kümesinde farklı bir özet-değerine taşıması gerektiği düşünülürse içeriği değiştirilmiş bir mesajın özet-değeri de farklı çıkacaktır. Dolayısıyla mesajı alan kişi mesajı kendisinin de bildiği Özetleme fonksiyonundan geçirecek ve elde ettiği özet-değerle kendisine gönderilen özet-değeri karşılaştıracaktır. Mesajın bütünlüğünün korunduğunun

ispatı için bu iki değerin uyuşması gerekmektedir. Virüs koruması ve yazılım korsanlığının önlenmesi Özetleme fonksiyonlarının diğer özel uygulamalarındandır.

Özetleme fonksiyonları yukarıda da belirtildiği gibi herkesçe bilinebilen ve gizli anahtarı olmayan tek-yönlü fonksiyon uygulamalarıdır. Eğer belli bir mesajın değiştirilip değiştirilmediğini tespit etmeye yönelik kullanılırlarsa "Değişiklik tespit kodları" (Modification Detection Codes) adını alırlar. Bu alanla ilgili olarak gizli bir anahtar içeren ve veri bütünlüğünün yanı sıra verinin kaynağının doğrulanması işleminde de kullanılan Özetleme fonksiyonlarına "Mesaj doğrulama kodları" (Message Authentication Codes) adı verilir.

Hash Fonksiyonu

Mesaj yetkilendirme kodunun bir çeşidi, tek yönlü hash fonksiyonu olarak çok sık kullanılır. Mesaj yetkilendirme kodu olarak, bir hash fonksiyonu, değişken uzunluklu M mesajını giriş olarak alır ve çıkış olarak sabit uzunluklu, mesaj özeti denilen H(M) hash kodu üretir. Hash kodu, mesajın bütün bitlerinin bir fonksiyonudur ve hata bulma özelliği vardır. Mesajdaki bir veya birkaç bit'in değişmesi hash kodunda da değişmeye neden olur.



Şekil 7.10 Hash Fonksiyonunun temel Kullanımı: Yetkilendirme ve gizlilik sağlar.

Özetleme fonksiyonunun amacı, bir dosya,mesaj veya diğer bir veri bloğunun parmak izini üretmektir.

Güvenli özetleme(hash) fonksiyonlarının özellikleri aşağıda verilmiştir. Esas olarak iki mesaj için aynı özet değerini bulmak çok zor olmalı ve özet açık bir şekilde mesajla ilişikili olmamalıdır.(mesajın karmaşık doğrusal olmayan bir fonksiyonu olmalıdır). Özetleme fonksiyonları ve blok şifreleyicilerin tasarımı arasında birçok benzerlik bulunur.

- H herhangi boyutlu bir M mesajına uygulanabilir
- H sabit uzunlukta bir çıkış(h) üretir
- H(M), verilen bir M mesajı için kolay üretilebilir
- Verilen bir h değeri için, H(x)=h yı sağlayan x'i bulmak hesaplama bakımından verimsizdir. Bu H(x)'in tekyönlü özelliğidir
- Verilen bir x bloğu için H(y)= H(x) olan y≠x gibi bir y değerini bulmak hesaplama bakımından verimsizdir. Bu özellik "weak collision resistance" dır.
- H(y)=H(x) için, bir (x,y) çifti bulmak hesaplama bakımından verimsizdir. Bu özellik "strong collision resistance" dır.

Basit Hash Fonksiyonları

Bütün hash fonksiyonları aşağıdaki genel prensipleri kullanarak çalışır. Giriş, n bitlik blok dizisi olarak görülür. Giriş her defasında bir blok olarak n-bitlik hash fonksiyonunu üretmek için işlenir. En basit hash fonksiyonu, her bloğun bit bit XOR işlemne tabi tutulmasıdır. Bu aşağıdaki gibi açıklanır:

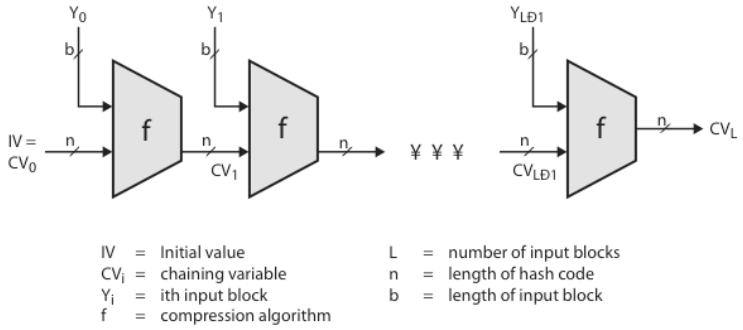
$$C_i = b_{i1} \oplus b_{i2} \oplus \ldots\ldots\ldots\oplus b_{im}$$

C_i: hash kodunun i. biti, $1 <= i <= n$;**bij :** j.'inci bloktaki I'inci. Bit

Genel hash algoritmasının blok şeması Şekil 7.11'de verilmiştir.

$CV_0 = IV$

$CV_i = f(CV_{i-1}, Y_{i-1})$ $1 \le i \le L$
$H(M) = CV_L$ (CV :Chaining Value)



Şekil 7.11. Özetleme fonksiyonu genel yapısı

Bugün sıklıkla kullanılan Özetleme fonksiyonlarına örnek olarak 1992'de Ron Rivest tarafından geliştirilmiş MD5 (message-digest algorithm) algoritması gösterilebilir. NIST ve NSA'nın ortaklaşa geliştirmiş olduğu SHA (secure hash algorithm) ise yine NIST'ın Özetleme fonksiyonları için belirlediği standart olan SHS (secure hash standard) içerisinde yeralmış ve kullanımı yaygın olan bir özetleme algoritmasıdır. Önemli özetleme fonksiyonlarının özellikleri Tablo 7. 3'te verilmiştir.

Adı	Blok Uz.(bit)	Max mesaj	Sonuç(bit)	Adım sayısı	Mantık F.	Ek sabit
MD5	512	∞	128	64(4x16)	4	64
SHA1	512	2^{64} -1	160	80(4x20)	4	4
RipeMD-160	512	2^{64} -1	160	160(5x16 çift)	5	4

Tablo 7.3 Önemli Özetleme fonksiyonlarının özellikleri

7.5 Kimlik Doğrulama ve Sayısal İmzalar

Bir belgenin elektronik ortamda imzalanmasındaki amaçlar aşağıdaki şekilde özetlenebilir.

- İmzayı atan şahsın kimliğinin imzadan anlaşılması
- Şahıs imzayı reddettiği durumda bunun ispatının yapılabilmesi
- İmzanın sahtesinin atılamaması, aksi durumda ispatının yapılabilmesi
- İmza tarihinin bilinebilmesi(imza içerisine koyulması)
- Belgenin içeriğinin değiştirilme riskine karşı imzanın metin ile ilişkilendirilmesi
- Eğer belge içeriğinin üçüncü şahıslar tarafından bilinmesi istenmiyor ise belge ayrıca şifrelenerek iletilir ve saklanır.

Bunların yanında sayısal imzanın elde edilmesi ve kime ait olduğunun anlaşılması kolay olmalıdır.

Sayısal İmza ve El ile Atılan İmzanın Karşılaştırılması

Geleneksel el ile atılan imzanın, standart yöntemi olmaması(bazıları ismini yazdığı halde bazıları anlaşılmaz çizgiler çizerler) nedeniyle imzanın doğrulanması işlemi oldukça zordur. Diğer handikap, el ile atılan imzanın kolaylıkla taklit ve kopya edilebilmesidir. Bir başka dezavantaj ise herbir sayfasının imzalanması gereken çok sayfalı dökümanlarda, her sayfanın imzalandığının kontrol edilmesi gerekliliğidir. Bunlara karşı sayısal imzanın aşağıdaki avantajlarının olduğu kolaylıkla söylenebilir.

Sayısal imza uygulamasıyla;

- İmzalanan verinin bütünlüğü (değiştirilmemesi) sağlanır.
- İmza atacak şahsın bu yetkiye sahip olup olmadığı(yetkilendirme) sağlanır.
- İmza atanın bu imzayı inkar edememesi sağlanır.,
- İmzanın atıldığı tarih-saat damgasının olması(imzanın ne zaman atıldığının bilinmesi sağlanır)
- Hız ve verimlilik sağlanır.
- İstenirse gizlilik sağlanır.

Ağ üzerinde hareket eden verilerin geldikleri adresten tam olarak gönderildiği şekliyle gidecekleri yere ulaşmaları amacıyla veriler ve paketler değişik şekillerde özetlenirler. Bu şekilde kullanılan özetleme fonksiyonları (Hash Functions), verileri tek yönlü bir matematiksel fonksiyona tabi tutup özet değeri oluştururlar. Bu özet değer paket içerisinde yollanır. En çok kullanılan özetleme fonksiyonları SHA (Secure Hash Algorithm) ve MD5 algoritmalarıdır. Başka bir yolda veri paketinin sonuna her paket için bir tane üretilen CRC (Cyclic Redundancy Check) kodu veya toplam kontrol bilgisinin (CS) eklenmesidir.

Verilerin ağ üzerinde doğrulanmasının dışında ayrıca gerçekten üzerinde yazılı olan adresten gelip gelmediğinin kontrolü ise sayısal imza algoritmaları ile sağlanmaktadır. Sayısal imza algoritmalarında, veriyi gönderen adresin kendisine ait gizli bir anahtarla verinin kendisi, imzalama algoritmasına girer ve çıkan bilgi bize o pakete ait imzayı vermektedir. Paketin alıcısı ise, imzanın doğrulanması aşaması için, imzanın doğruluğunu kontrol eder. Sayısal imza algoritmaları olarak, aynı zamanda açık anahtarlı kripto sistem algoritması amacıyla kullanılan RSA ve ElGamal algoritmaları kullanılabilir. Bunlara ek olarak DSA (Digital Signature Algoritm) imza algoritması ve pek çok özel tür algoritmada kullanılabilmektedir.

Ağ ve internet güvenliğinde bugün yaygın olarak kullanılan kimlik doğrulama uygulamaları arasında Kerberos protokolünü sayabiliriz. Kerberos daha çok gizli anahtarlı şifreleme üzerine kurulu bir sistem olmakla beraber istemci sunucu arasındaki diyalogların doğrulanmış bir şekilde yapılması işlemini yönetir.

X.509 dizin doğrulama servisi ise X.500 dizin servisinin kullanımı ile yaygınlaşan bir kimlik doğrulama standardıdır. X.509 dizin servisi daha çok açık anahtarlı kripto sistemler üzerine kuruludur. Bu serviste hiyerarşik bir düzende yer alan kullanıcılar arasındaki haberleşmelerde servisin kullanıcılara sağladığı sertifikalar söz konusudur. Her sertifika, verinin göndereceği adresin kimlik numarası ve ona ait açık anahtarı içermektedir. Sertifikaların içeriğinin değiştirilmesinin engellenmesi amacıyla sertifikalar belli bir sertifikasyon otoritesi sunucu tarafından imzalanır. Dolayısıyla veri gönderecek adresteki birim alıcıya ait sertifika, sertifika otoritesinden (CA - Certification Authority) elde eder, altındaki imzayı kontrol eder. Sertifikanın doğruluğundan emin olduktan sonra içeriğinde yer alan açık anahtarı kullanarak alıcıya mesajı şifreleyerek gönderir.

Sayısal imzalar ve İmza Algoritmalarının özellikleri

- Gizli anahtar imza üretirken açık anahtar imzaları doğrulamakta kullanılır
- Sadece sahibi sayısal imza üretebilir buradan mesajı kimin ürettiğini doğrulamakta kullanılır
- Genellikle mesajın tamamı imzalanmaz(değişen bilgi iki katına çıkar), fakat mesajın özeti imzalanır,
- Bir özet fonksiyonu mesajı alır ve mesaja bağlı olan sabit uzunluklu(tipik olarak 64 to 512 bit) bir değer üretir

- Başka bir mesajın aynı özet değerini üretmesi çok zor olmalıdır(aksi halde bazı sahtecilik mümkün olur)

Sayısal imza için gereksinimler:

- İmza, imzalanacak mesaja bağlı olan bir sayısal bit paterni olmalıdır.
- İmza, sahteciliği ve inkarı önlemek için göndericiye özel bilgileri taşımalıdır.
- Sayısal imzayı üretmek kolay olmalıdır.
- Sayısal imzayı tanımak ve doğrulamak kolay olmalıdır.
- Verilen bir sayısal imza için bir mesaj üretmek veya, verilen bir mesaj için sayısal imza üretmek, hesaplanabilirlik açısından verimsiz olmalıdır.
- Sayısal imza bellekte kaybedilmemelidir.