MM PG COLLEGE FATEHABAD

Introduction to Cryptography
M.Com. 1st Sem.

Departments of Computer Science
MM PG College Fatehabad

What is Cryptography

- Cryptography
  - In a narrow sense
    - Mangling information into apparent unintelligibility
    - Allowing a secret method of un-mangling
  - In a broader sense
    - Mathematical techniques related to information security
    - About secure communication in the presence of adversaries
- Cryptanalysis
  - The study of methods for obtaining the meaning of encrypted information without accessing the secret information
- Cryptology
  - Cryptography + cryptanalysis

Security Attacks

- Passive attacks
  - Obtain message contents
  - Monitoring traffic flows

- Active attacks
  - Masquerade of one entity as some other
  - Replay previous messages
  - Modify messages in transmit
  - Add, delete messages
  - Denial of service

Objectives of Information Security

- Confidentiality (secrecy)
  - Only the sender and intended receiver should be able to understand the contents of the transmitted message
- Authentication
  - Both the sender and receiver need to confirm the identity of other party involved in the communication
- Data integrity
  - The content of their communication is not altered, either maliciously or by accident, in transmission.
- Availability
  - Timely accessibility of data to authorized entities.

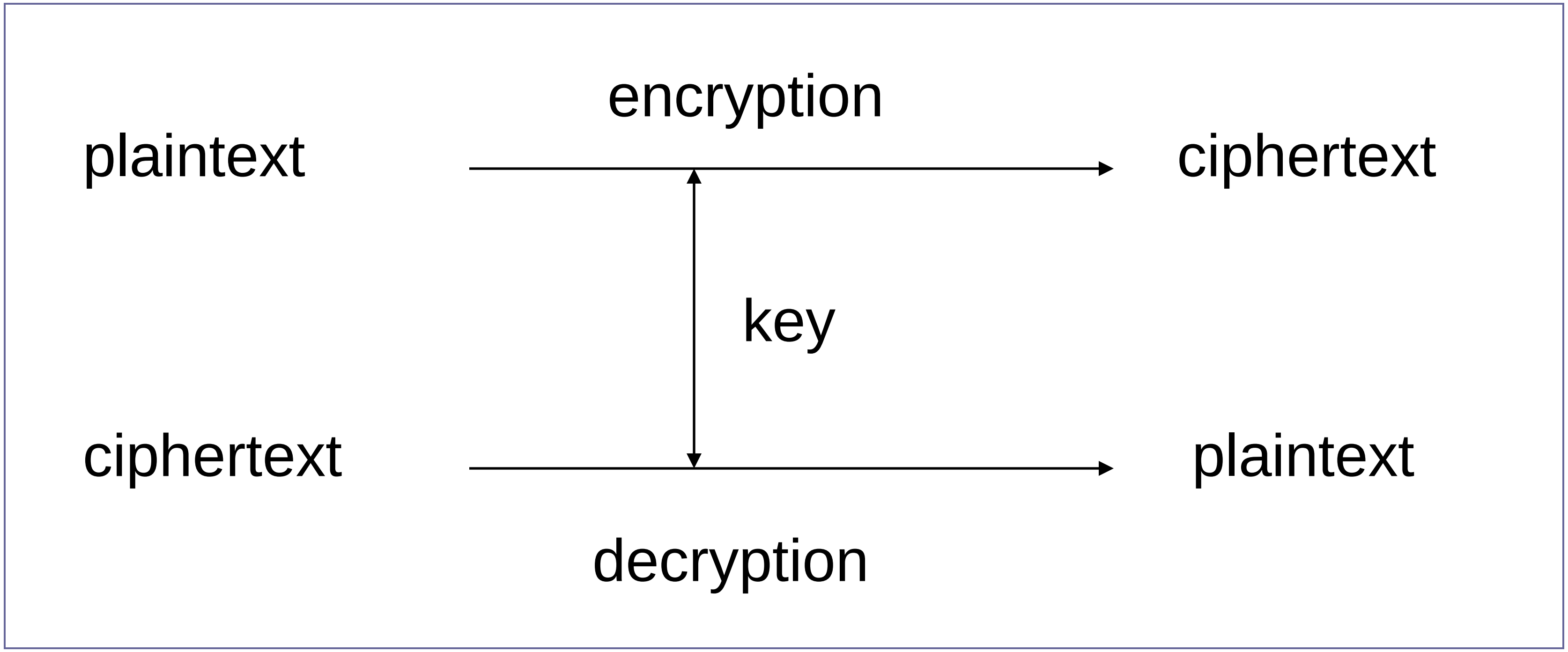
Objectives of Information Security

- Non-repudiation
  - An entity is prevented from denying its previous commitments or actions
- Access control
  - An entity cannot access any entity that it is not authorized to.
- Anonymity
  - The identity of an entity if protected from others.

Types of Cryptographic Functions

- Secret key functions
- Public key functions
- Hash functions

Secret Key Cryptography



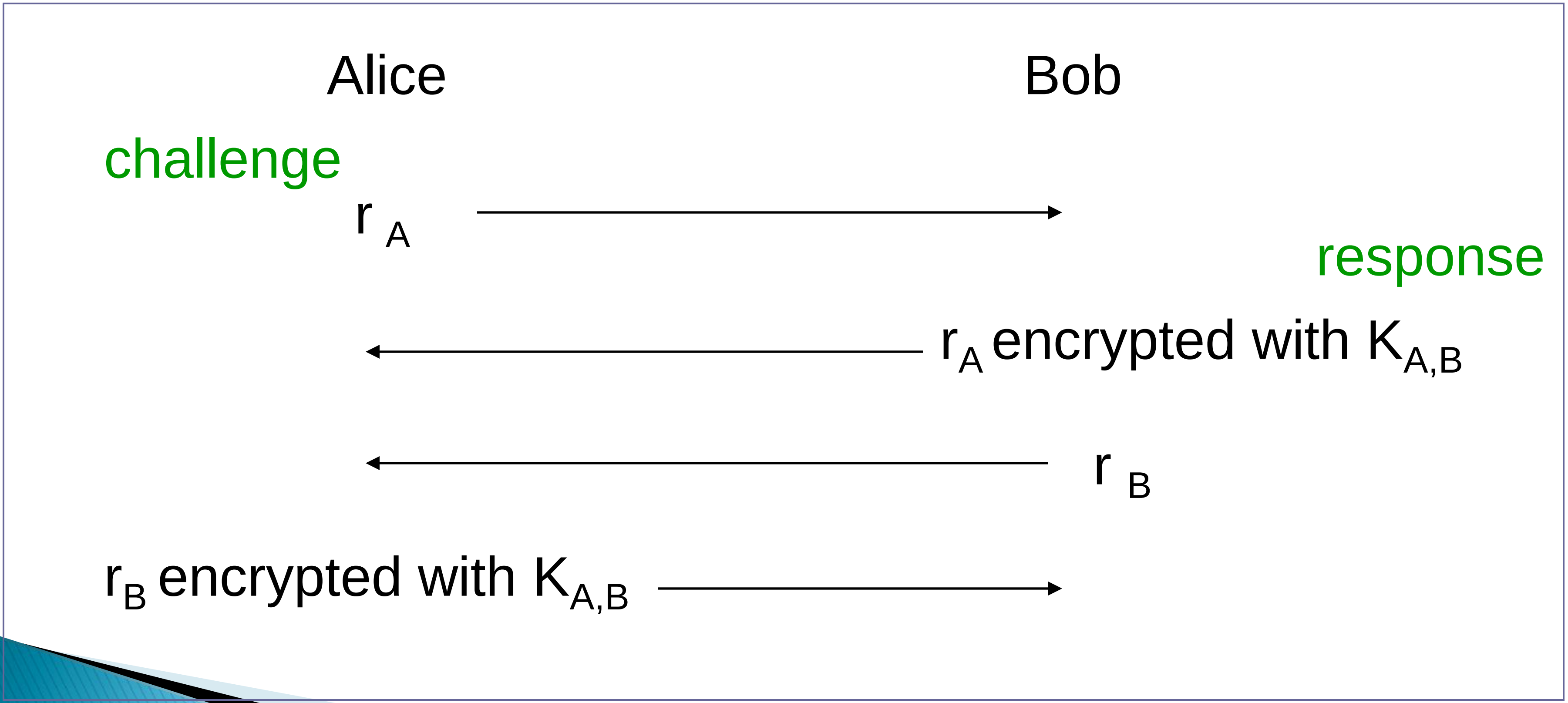
- Using a single key for encryption/decryption.
- The plaintext and the ciphertext having the same size.
- Also called *symmetric* key cryptography

SKC: Security Uses

- Transmitting over an insecure channel
  - The transmitted message is encrypted by the sender and can be decrypted by the receiver, with the same key
  - Prevent attackers from eavesdropping
- Secure storage on insecure media
  - Data is encrypted before being stored somewhere
  - Only the entities knowing the key can decrypt it

SKC: Security Uses

- Authentication
  - Strong authentication: proving knowledge of a secret without revealing it.



Alice

Bob

challenge

r_A

response

r_A encrypted with $K_{A,B}$

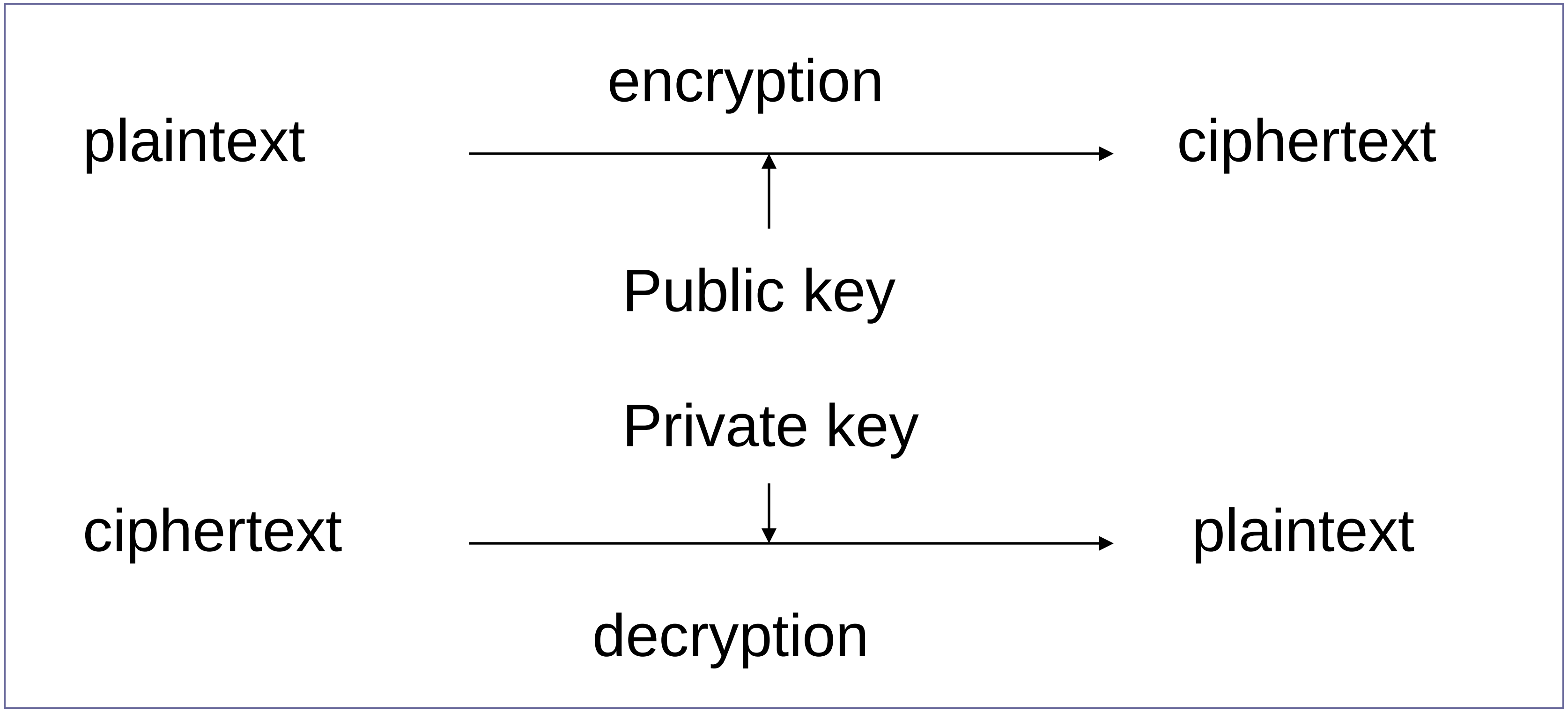
r_B

r_B encrypted with $K_{A,B}$

SKC: Security Uses

- Integrity Check
  - Noncryptographic checksum
    - Using a well-known algorithm to map a message (of arbitrary length) to a fixed-length checksum
    - Protecting against accidental corruption of a message
    - Example: CRC
  - Cryptographic checksum
    - A well-know algorithm
    - Given a key and a message
    - The algorithm produces a fixed-length message authentication code (MAC) that is sent with the message

Public Key Cryptography



encryption

plaintext

ciphertext

Public key

Private key

ciphertext

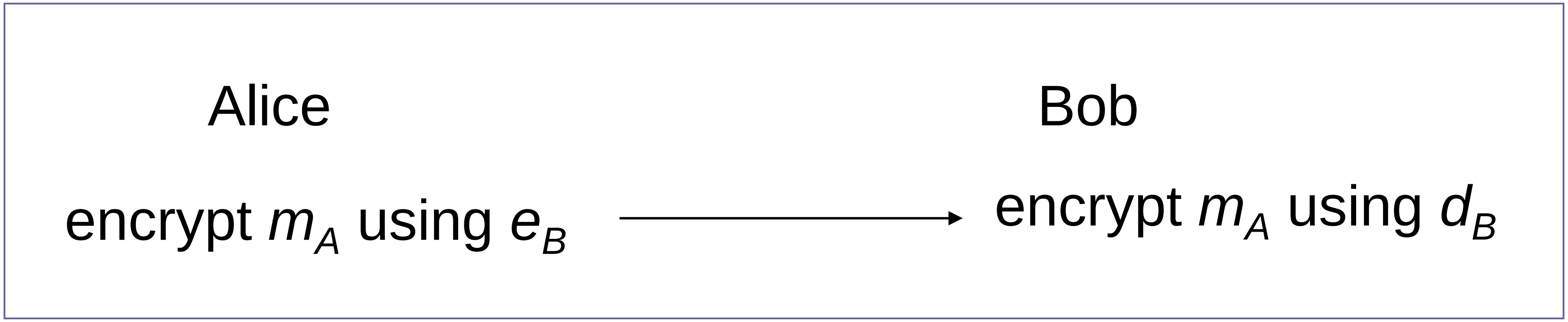
plaintext

decryption

- Each individual has two keys
  - a private key (d): need not be reveal to anyone
  - a public key (e): preferably known to the entire world
- Public key crypto is also called asymmetric crypto.

PKC: Security Uses

- Transmitting over an insecure channel



Alice

encrypt m_A using e_B

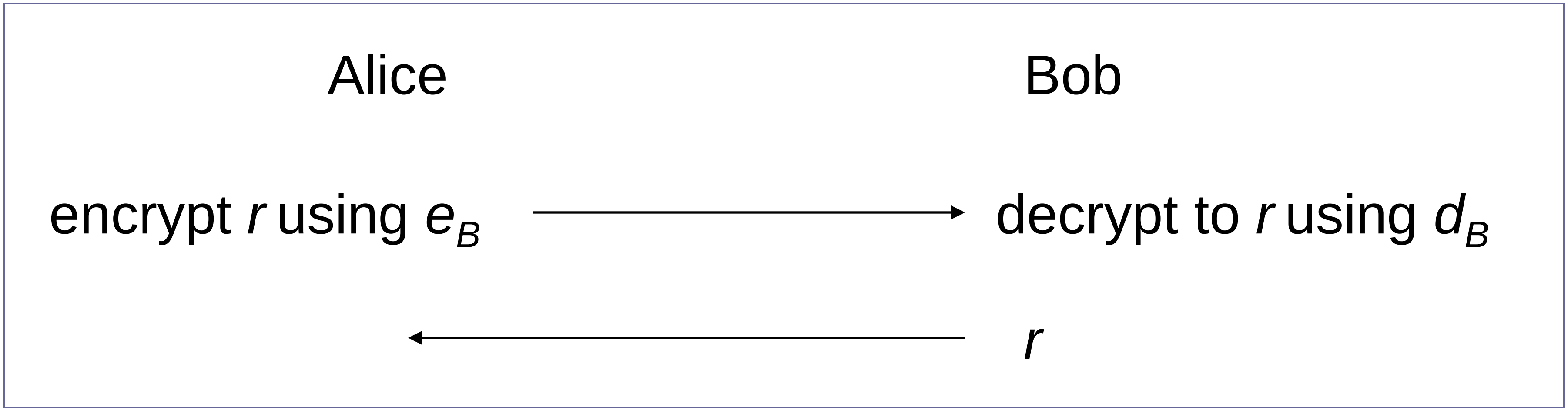
Bob

encrypt m_A using d_B

- Secure storage on insecure media
  - Data is encrypted with the public key of the source, before being stored somewhere
  - Nobody else can decrypt it (not knowing the private key of the data source)

PKC: Security Uses

- Authentication



Alice

Bob

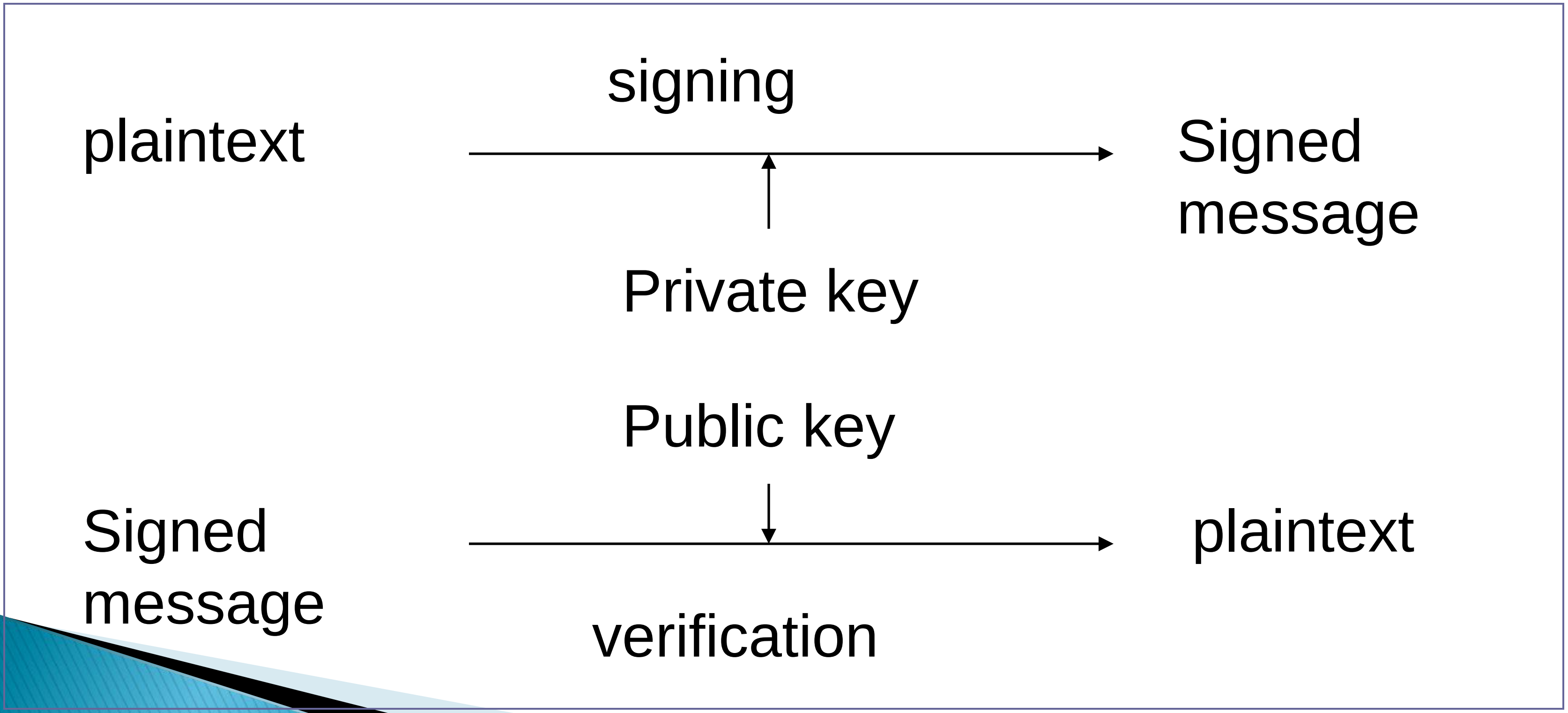
encrypt r using e_B

decrypt to r using d_B

r

PKC: Security Uses

- Digital Signatures
  - Proving that a message is generated by a particular individual
  - Non-repudiation: the signing individual can not be denied, because only him/her knows the private key.



signing

plaintext

Signed message

Private key

Public key

Signed message

plaintext

verification

Hash Functions

- Cryptographic hash function
  - A mathematical transformation that takes a message of arbitrary length and computes it a fixed-length (short) number.

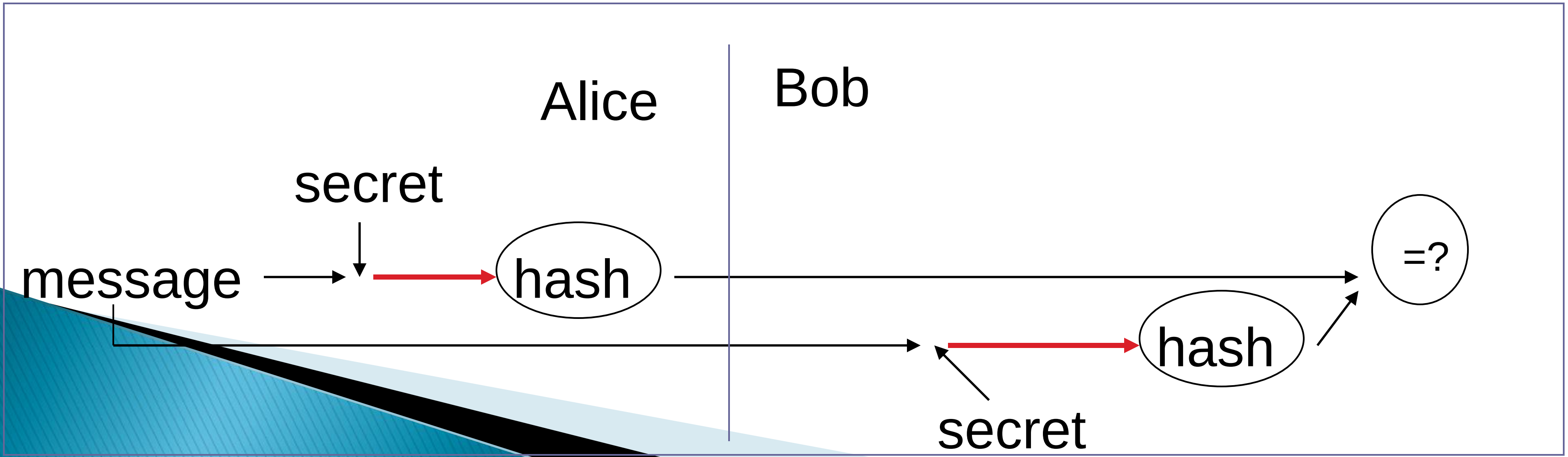
- Properties

  (Let the hash of a message *m* be *h(m)*)

  - For any *m*, it is relatively easy to compute *h(m)*
  - Given *h(m)*, there is no way to find an m that hashes to *h(m)* in a way that is substantially easier than going through all possible values of m and computing *h(m)* for each one.
  - It is computationally infeasible to find two values that hash to the same thing.

Hash Functions: Security Uses

- Password hashing
  - The system store a hash of the password (not the password itself)
  - When a password is supplied, it computes the password’s hash and compares it with the stored value.
- Message integrity
  - Using cryptographic hash functions to generate a MAC



Hash Functions: Security Uses

- Message fingerprint
  - Save the message digest of the data on a tamper-proof backing store
  - Periodically re-compute the digest of the data to ensure it is not changed.
- Downline load security
  - Using a hash function to ensure a download program is not modified
- Improving signature efficiency
  - Compute a message digest (using a hash function) and sign that.

Cryptographic Algorithms: Agenda

- Attacks on cryptographic algorithms
- Definition of security
- Some cryptographic algorithms: basic facts

Attacks: Types

- Brute force search
  - Assume either know/recognize plaintext
  - Simply try every key

- Cryptoanalysis
  - Ciphertext only
    - With the ciphertext
    - Plaintext is recognizable
  - Known plaintext
    - <cipher, plaintext> pairs are known
  - Chosen plaintext
    - Select plaintext and obtain ciphertext to attack

Birthday Attacks

- Principle
  - Assume: A function yields any of n different outputs with equal probability, where n is sufficiently large.
  - After evaluating the function for about 1.2*squart(n) arguments, we expect to find a pair of different arguments, x_1 and x_2, such that f(x1)=f(x2).

- Attack: message replay
- Solution: increase the size of the output

Meet-in-the-Middle Attacks

- Principle
  - build a table of keys
  - Compute f(k,m) for every key
    - f is an encryption function, m is a known message
  - Eavesdrop a value f(k’,m)
  - If f(k’,m)=f(k,m), then there is a good chance k’=k.

Meet-in-the-Middle Attacks

- An attack example
  - Assume:
    - a new encryption function: $F(k1,k2,m)=f(k1,f(k2,m))$
    - A pair (P,C) is known
  - Attacker:
    - Encrypt P, i.e., computing f(k2,P), for all possible values of k2; store the values in a table
    - Decrypt C, i.e., computing $f^{-1}(k1,C)$, for all possible values of k1, and for each result check the table
    - A match reveals a possible combination of the keys

Security Definition

- Unconditional Security
  - The system cannot be defeated, no matter how much power is available by the adversary.

- Computational security
  - The perceived level of computation required to defeat the system using the best known attack exceeds, by a comfortable margin, the computational resources of the hypothesized adversary.
  - e.g., given limited computing resources, it takes the age of universe to break cipher.

Security Definition

- Provable security
  - The difficulty of defeating the system can be shown to be essentially as difficult as solving a well-known and supposedly difficult problem (e.g., integer factorization)
- Ad hoc security
  - Claims of security generally remain questionable
  - Unforeseen attacks remain a threat

Secret Key Cryptographic Algorithms

- DES (Data Encryption Standard)
- 3DES (Triple DES)
- IDEA (International Data Encryption Algorithm)
- AES (Advanced Encryption Standard)

DES (Data Encryption Standard)

- Authors: NSA & IBM, 1977

- Data block size: 64-bit (64-bit input, 64-bit output)
- Key size: 56-bit key

- Encryption is fast
  - DES chips
  - DES software: a 500-MIP CPU can encrypt at about 30K octets per second

- Security
  - No longer considered secure: 56 bit keys are vulnerable to exhaustive search

Triple-DES (3DES)

- $C = DES_{k3}(DES_{k2}(DES_{k1}(P)))$.

- Data block size: 64-bit
- Key size: 168-bit key; effective key size: 112 (due to man-in-the-middle attack)

- Encryption is slower than DES

- Securer than DES

IDEA (International Data Encryption Algorithm)

- Authors: Lai & Massey, 1991

- Data block size: 64-bit
- Key size: 128-bit

- Encryption is slower than DES
- Security
  - Nobody has yet published results on how to break it

- Having patent protection

AES (Advanced Encryption Standard)

- Authors: Daemen & Rijmen

- Block size:128-bit
- Key size: 128-bit, 192-bit, 256-bit

- Encryption is fast

- Security
  - As of 2005, no successful attacks are recognized.
  - NSA stated it secure enough for non-classified data.