

暗号の歴史と進化

- 古代ギリシャ、ローマ時代
  - 戦争や外交で秘密の伝達手段
  - 単純な文字置換（シーザー暗号）
- 中世以降
  - キーワードで何段階にもずらす仕組み（ヴィジュネル暗号）
- 解読に必要
  - ✔ 文字を入れ替え、見えなくする仕組み
  - ✔ 解き明かす方法



エニグマとの攻防

- 20世紀
  - 暗号は機械によって自動化
  - （代表例）エニグマ暗号機



アラン・チューリング

- 解読装置「ボンベ」を開発
- 脳を使った推理や発想の力
- ⇒ 暗号理論の基礎を築く

現代と未来の暗号

- 現代の暗号
  - 数学的な仕組み
  - 「公開鍵暗号」の画期的な発明
  - ネット時代の暗号通信の基盤



- PGPソフトウェア登場
  - 個人でも安全にメールを暗号化
- 量子暗号が登場
  - 理論上は完全に安全な通信が可能
  - 量子技術はまだ研究段階