10%笔记. 30%作业. 30%期中. 30%期末.

演变历史：古典密码.

- Caesar cipher. A→D. B→E.
- shift cipher. A→A+key mod 26.
- mono-alphabetic substitution cipher. $f: \{A, B, \dots, Z\} \to \{A, B, \dots, Z\}$ 双射.
- Vigenere cipher. $f_1, f_2, \dots, f_k$. 依次加密.
- Enigma. key. pos_1. pos_2. pos_3. 一般不会循环.
  - 三个可转的双射转盘构成. 一直旋转. 由映射及初始位置解密.

加密涉及的变量：

明文空间 M. 密钥空间 K. 加密函数 Enc: $K \times M \to C$.
密文空间 C. 密钥生成 Gen: $\to K$ 解密函数 Dec: $K \times C \to M$.

一个加密算法：(M, C, K, Gen, Enc, Dec).

定义 —假设(如假设大整数质因数分解很难)→ 安全性证明 + 正确性保障.

安全性证明
- Key Recovery Attack.
- Message Recovery Attack.
- Semantically Secure: "Eve learns nothing useful"
  (即：有无密文不影响猜测消息的明文或key或Dec等参数/函数.

Semantically Secure. All dist D_m. All $g: M \to T$. All Eve. $\exists S$.

$\Pr[Eve(Enc(k,m), g(m)) = f(m)] = \Pr[S(g(m)) = f(m)]$.

$\Updownarrow$

Distinguisher ($\to 0/1$). "Can't tell the ciphertexts of two distinct messages"

↓

$\forall D$ m_0, m_1. $\Pr[D(Enc(k,m_0)) \to 0] = \Pr[D(Enc(k,m_1)) \to 0]$.

$\Updownarrow$

Perfect Secrecy. $\forall m_0, m_1, c$.

$\Pr[Enc(k,m_0)=c] = \Pr[Enc(k,m_1)=c]$.

· 推论: $|K|<|M|$ 否则 对一个密文, 枚举k可得到明文不为某些值.

⇒ 密钥加密具有同等难度, 难以安全传输.

不能保护的消息. 如: 多次传输/密钥泄露/... 如何?

· One-time Pad. Random 0/1 字符串. 与原文异或.

Perfect Secure

↓ 减弱

Statistical Secure

|

δ-Secure — 允许P的误差<δ.

↓

computational Secure

|

t-Secure. — 允许δ误差并限制运行时间t. (的量级).

$(t(\lambda), S(\lambda))$.

λ - Security parameter $\approx$ key length.

$K_1, \cdots, K_\lambda$.

$M = \{0,1\}^*$

$C = \{0,1\}^*$

$Gen(1^\lambda) \to K_\lambda$

$Enc : K \times M \to C$.

$Dec : K \times C \to M$.

$poly(\lambda) = \bigcup_k O(\lambda^k)$. 多项式级速度

$negl(\lambda) = \bigcap_k O(\frac{1}{\lambda^k})$. 可忽略性.

Definition.

- Correctness.
- Security
  - Eveadropper (被动攻击).
  - Active

| 单条消息 | 多消息. |

- Perfect Securecy
- Stastical
- Computational.
  - poly time adversary
  - negl "advantage"