2 密码理论与技术

古典加密技术

密码分析：希望利用某些先验知识从密文恢复出明文，或者也得到了变换的窍门Key。

- 统计规律是密码分析的重要依据；
- 分析过程经验和相关知识很关键；
- 密码分析可以细分为：
  - 唯密文攻击：从已知的密文中恢复出明文或密钥；
  - 已知明文攻击：利用已知密文和一些明文+密文来分析明文；
  - 选择明文攻击：可选定任意明文-密文对进行攻击；
  - 选择密文攻击：分析者能选择不同的被加密的密文，并能得到对应的解密的明文。

基本术语

- 明文 M (plaintext)：变换前的原始消息；
- 密文 C (cyphertext)：变换后的消息；
- 密钥 K (key)：用于密码变换的，只有发送者和接收者拥有的秘密消息；
- 加密 $C = E(M, K_1)$ (encryption)：使用特定密钥把明文转化为密文的数学方法；
- 解密 $M = D(C, K_2)$ (decryption)：使用特定密钥把密文转化为明文的数学方法；
- **密码系统**可以表示为 $(\mathcal{M}, \mathcal{C}, \mathcal{K}, E(\cdot,\cdot), D(\cdot,\cdot))$。
  - $\mathcal{M}$ 是可能明文的有限集（明文空间）；
  - $\mathcal{C}$ 是可能密文的有限集（密文空间）；
  - $\mathcal{K}$ 是可能密钥的有限集（密钥空间）。

解密算法唯一性：$D(E(M, K_1), K_2) = M$。

密码体制的分类

- **单钥体制**（对称算法）：$K_1 = K_2$，或可以互相推导；古典加密技术都是单钥体制。
- **双钥体制**（公钥算法）：K_1 和 K_2 不能互相推导。

公钥体制

- 系统中，加密密钥称**公开密钥**（Public key，**公钥**）可以公开发布；而解密密钥称**私人密钥**（private key，**私钥**）。
- 加密解密：$C = E(M, PK)$，$M = D(C, SK)$；
- 数字签名：$S = Sig(M, SK)$，$0 \text{ or } 1 = Ver(S, PK)$

Kerckhoff假设：假设敌手 Oscar 知道正在使用的密码体制 $(\mathcal{M}, \mathcal{C}, \mathcal{K}, E(\cdot,\cdot), D(\cdot,\cdot))$，只是不知道选用的具体密钥 $K \in \mathcal{K}$。换言之，一个密码系统的安全性都应该基于密钥的安全性，而不是基于算法细节的安全性。

- 含义：安全性仅仅基于密钥的安全性；
- 原因：容易保存、容易分享、防止反向工程、容易更换。
- **结论**：公开的密码学设计。这样的算法可以经历更多的实践检验，更容易发现漏洞，避免反向工程

的危害，利于构建标准。