第 1 章：密码学简介

1.4 基本概念

赵俊舟

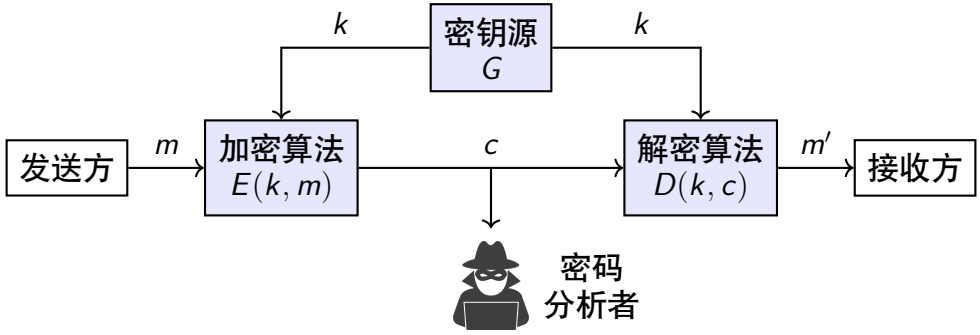
junzhou.zhao@xjtu.edu.cn

2025 年 2 月 20 日

密码学基本术语

- Cryptology：保密学，源自希腊语；
- Cryptography：密码编码学，研究如何将明文转换为密文；
- Cryptanalysis：密码分析学，研究如何破译密文得到明文或获得密钥；
- Cipher：加密方法；
- Encipher, encryption：将明文转换成密文的过程；
- Decipher, decryption：将密文还原成明文的过程；
- Plaintext (cleartext)：原始的可读数据，称为消息或明文；
- Ciphertext (cryptogram)：加密后得到的密文；
- Key：密钥，对加密与解密过程进行控制的参数

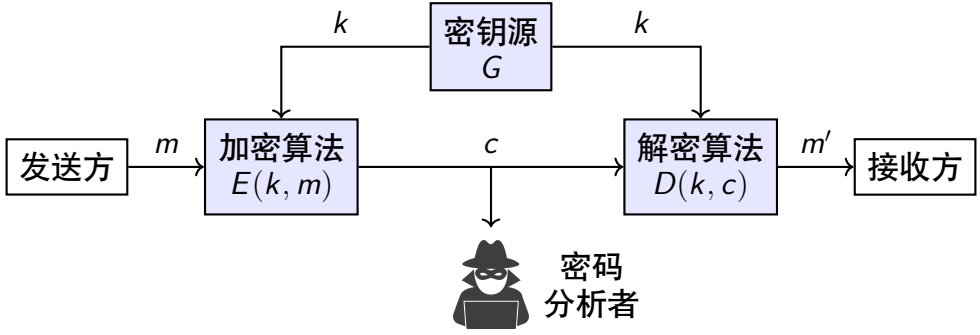
保密通信系统的一般模型



由定义在空间 $(\mathcal{K}, \mathcal{M}, \mathcal{C})$ 上的运算 (G, E, D) 构成，其中

- $\mathcal{K}$ 为密钥空间，$\mathcal{M}$ 为明文空间，$\mathcal{C}$ 为密文空间
- $G\colon \{0,1\}^* \mapsto \mathcal{K}$ 为密钥生成函数或密钥源
- $E\colon \mathcal{K} \times \mathcal{M} \mapsto \mathcal{C}$ 为加密运算，并且 $c = E(k, m)$
- $D\colon \mathcal{K} \times \mathcal{C} \mapsto \mathcal{M}$ 为解密运算，并且 $m = D(k, c)$

保密通信系统的要求



- **正确性**：$D(k, E(k, m)) = m$
- **保密性**：由密文或明密文推测密钥和明文，在计算上不可行。
- **Kerckhoffs 准则**：系统的安全性不依赖于对加解密算法的保密，而是密钥。
- **计算效率**：加解密算法的计算效率应足够高，便于系统实现。

理论安全、计算安全与实际安全

- 理论安全要求密码分析者不能由密文获取关于明文的任何信息。根据香农定理，要实现理论安全，要求密钥长度不能短于明文长度，因此理论安全不切实际。
- 计算安全考虑密码分析者的实际运算能力，如果一个运行时间最多为 t 的敌手最多只能以概率 ϵ 成功破解加密体制，则称该加密体制计算安全。
  - 例如，一个敌手使用目前最先进的计算机运行时间不超过 200 年，破解密码体制的概率不超过 2^{-60}。
- 实际安全将一个密码体制的安全构建在一个数学难题之上，此时密码体制的安全性等于该数学问题的困难程度。这时候，只要证明了该问题困难程度符合安全需求，那么可以认为密码体制是实际安全的。

密码体制的分类

- 对称密码体制：加解密密钥相同，加密能力和解密能力是结合在一起的，开放性差；
- 非对称密码体制：加解密密钥不同，从一个密钥导出另一个密钥是计算上不可行的，加密能力和解密能力是分开的，开放性好。
- 流密码：也称序列密码，明文以比特流或字节流的形式进行加解密；
- 分组密码：明文按照定长进行分组，然后对分组整体进行加解密。
- 确定型密码：当明文和密钥确定后，密文也就唯一地确定了；
- 概率型密码：当明文和密钥确定后，密文产生不确定。

密码攻击类型（Threat Model）

对密码分析者攻击能力的假设：除了知道加解密算法，还知道下面信息：

- 唯密文攻击：知道密文；
- 已知明文攻击：除了知道密文外，还知道一些明密文对；
- 选择明文攻击：知道密文，且可选择一些明密文对用于密码分析；
- 选择密文攻击：知道密文，且可选择一些密文及其对应明文对用于密码分析；
- 选择文本攻击：同时可选择明文或选择密文。

从上往下，密码分析者的攻击能力逐渐增强。