密码学简介

刘卓

1 介绍

密码学 (Cryptography) 是研究以加密的形式发送信息的方法，只有掌握此加密技术的特定人群才能破解加密获得有效信息。

一些关键词：

- 明文 (Plaintext)：加密前的信息。
- 密文 (Ciphertext)：加密后的信息。
- 加密 (Encryption): 通过特定的加密技术将明文转化为密文的行为。
- 解密（Decryption)：由掌握加密技术的特定人群将密文转化为明文的行为。
- 发件人（Sender)：*Alice*.
- 收件人 (Receiver)：*Bob*.
- 攻击者（Attacker)：*Eva*.
- n-gram: 由 n 个字母组成的字符串。
- 密钥 (Key): 密钥通常是一系列数字或符号，用于确定明文转换为密文的算法。只使用一次的键称为一次性键盘/键。
- 密钥空间 (Key Space): 用 K 表示，密钥的所有可能。
- 明文 (Plaintext): 用 M 表示，明文消息的集合。
- 密文空间（Ciphertext space)：用 C 表示，所有在特定的加密事务中可能出现的明文消息。

2 加密主要方法

- **替换**（Substitution）：n 个字母的明文替换成 n 个字母密文。
- **换位**（Transposition）：将原始信息的字符按照某些特定的模式重新排列。

现代的加密方式是以上两种的混合。

3 加密解密过程

明文，由 *Alice* 通过密钥加密，变成密文。通过选定途径，发送给 *Bob*，*Bob* 通过密钥进行解密，得到明文。

4 密码学假设

- 发送方和接收方之间没有安全的通信通道。
- 信息的安全性是因为攻击者不知道加密中使用了何种特定密钥，以及加密方式。如果攻击者一旦知道密钥及加密方法，密文则被破译。
- 攻击者有三种攻击方式
  1. 纯密文攻击：攻击者只需要掌握密文来恢复明文。
  2. 明文攻击：攻击者通过掌握一些关于原始明文的信息来恢复明文。
  3. 选择性明文攻击：攻击者通过获得与其选择的明文对应的密文来部分破解密文。