# 密码学初探

密码系统 主要由三部分：发送方，接收方和破译方。

密码系统提供的主要功能：

1. 秘密性
2. 鉴别性
3. 完整性
4. 不可否认性

三种破译方式

1. 唯密文攻击法
2. 已知明文攻击法
3. 选择文攻击法

选择明文攻击

选择密文攻击