work1

姓名：吴浩哲

学号：2223612444

1. 根据攻击环境或者敌手能力的不同，简述五种攻击类型。

1. 唯密文攻击(Ciphertext-onlyattack)：密码分析者能利用的资源仅为同一密钥加密的一个或多个密文，这是对密码分析者最不利的情况（截获的部分密文）。
2. 已知明文攻击(Known-plaintextattack)：密码分析者者能够获得某些明密文的对应关系，这是密码算法至少需要抵抗的一种攻击（截获的部分密文和对应的明文）。
3. 选择明文攻击(Chosen-plaintextattack)：密码分析者能够选择明文并获得相应的密文，这是对密码分析者十分有利的情况（加密黑盒子，可加密任意明文得到相应的密文）。
4. 选择密文攻击(Chosen-ciphertextattack)：密码分析者能够选择密文并获得相应的明文，这也是对密码分析者十分有利的情况（解密黑盒子，可解密任意密文得到相应的明文）。
5. 选择文本攻击(Chosentextattack)：密码分析者能够选择明文并获得相应的密文也能够选择密文并获得相应的明文（加密黑盒子和解密黑盒子）。

2. 解释无条件安全（完美保密）和计算安全。

1. 无条件安全：对密码体制的任何攻击，都不优于（对明文）完全盲目的猜测，这样的密码体制就称为无条件安全的（或完善保密的）。
2. 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。

3. 简述针对哈希函数的四种攻击。

1. 原像攻击：给定 n 比特的哈希值 H，找到消息 M，满足 $h(M)=H$。
2. 第二原像攻击：给定消息 M_1，找到另一个数据串 M_2，满足 $h(M_1)=h(M_2)$ 且 $M_1 \neq M_2$。
3. 碰撞攻击：找到两个消息 (M_1,M_2)，满足 $h(M_1)=h(M_1)$ 且 $M_1 \neq M_2$。
4. 长度扩展攻击：给定 n 比特的杂凑值 $h(M)$，其中 M 为未知的非空数据串，找到任意数据串 N 和 n 比特的 H’，满足 $h(M \parallel N)=H$’。

4. 简述密码分析中，区分和分割的含义。

1. 区分指通过构造特定的统计或代数特征（称为区分器），将目标密码算法与理想随机函数区分开来。例如：
    - 差分分析中，利用明文差分与密文差分的非均匀分布作为区分依据。

- 线性分析中，依赖明文、密文和密钥之间的高偏差线性近似关系。区分器的有效性直接决定了攻击的成功率，其核心是发现密码算法的非随机性弱点。

2. 分割是一种分治策略，通过将密钥或数据划分为独立部分分别求解，以降低计算复杂度：

   - **密钥分割**：将密钥拆分为子块（如 K_1 和 K_2），优先求解计算量较小的子块（如 K_1），再逐步恢复剩余部分。例如分割攻击可将穷举复杂度从 $O(2^{m+n})$ 降至 $O(2^m + 2^n)$。
   - **数据分割**：如密码分割（Cryptosplit）技术，将明文或密文划分为多个随机分布的份额（如 N 份），通过分散存储或处理增强安全性。

5. 用现代密码学的视角分析移位代换密码、乘数密码、仿射密码、多项式代换密码的安全性。

1. 移位代换密码（如凯撒密码）
   - 密钥空间极小（仅 26 种可能的密钥），可通过暴力破解轻松攻破。
   - 明文统计特征（如字母频率）直接暴露在密文中，易受频率分析攻击。
2. 乘数密码
   - 密钥需与字母表长度互质（如英文为 26，有效密钥仅 12 个），密钥空间有限。
   - 仍保留单字母替换特性，频率分析有效。
3. 仿射密码
   - 结合移位和乘数密码，密钥空间稍大（$12 \times 26 = 312$种可能），但仍有限。
   - 加密函数为线性方程（$y \equiv (ax + b) mod 26$），易受已知明文攻击（解方程组即可恢复密钥）。
4. 多项式代换密码
   - 多表代换（如维吉尼亚密码）通过轮换多个替换表混淆频率特征，安全性优于单表代换。
   - 但若密钥较短或重复使用，仍可通过分组频率分析破解。
   - 多项式密码系统（如基于 LWE 问题的后量子密码）安全性较高，但古典多项式代换仍依赖有限数学变换，易受代数攻击。