

1. 设理想分组密码的分组长度为 n 位，解释以下说法：
 - (a) 存在 $2^n!$ 种可逆映射。
 - (b) 存储密钥需要 $n2^n$ 比特。
 - (c) 如果 (a) 正确，那么区分 $2^n!$ 种可逆映射应该只需要 $\log_2(2^n!)$ 个比特就可以，而 $\log_2(2^n!) < n2^n$ （例如 $n = 2$ 时， $\log_2(2^2!) = \log_2 24 = 4.6$ ，而 $2 \times 2^2 = 8$ ），所以密钥长度应为 $\log_2(2^n!)$ 比特。这个分析为什么与 (b) 矛盾。
2. 考虑一个密钥长度为 128 位的 16 轮 Feistel 密码，密钥为 k 。修改 Feistel 密码的轮密钥使用方式，使前 8 轮的轮密钥 k_1, k_2, \dots, k_8 仍由密钥扩展算法确定，而后 8 轮的轮密钥满足 $k_9 = k_8, k_{10} = k_7, \dots, k_{16} = k_1$ 。现在截获了使用该修改版 Feistel 密码加密的密文 c ，密钥 k 未知。假设再给你一次使用这个修改版 Feistel 密码加密任何消息并获得密文的机会（即具有一次选择明文攻击的能力），讨论如何解密 c 得到对应的明文。
3. 考虑 DES 中由 S_1 盒第一行定义的代替，给出对应这个代替，类似于课件 Ch2-1 第 8 页的代换密码。
4. 在有限域 $GF(2^4)$ 中，素多项式 $m(x) = x^4 + x + 1$, $f(x) = x^3 + x + 1$, $g(x) = x^2 + 1$, 计算 $f(x) \cdot g(x)$ 。
5. 求 $x^3 + x + 1$ 在有限域 $GF(2^4)$ 中模素多项式 $x^4 + x + 1$ 的乘法逆元。