第三章作业

16337341 朱志儒

思考题

3.3 对于较小的 n=4 的分组，密码系统等同于传统代替密码；而对于较大的 n 的分组，密钥的规模是$n \times 2^n$位，然而这很难实现。

3.4 乘积密码是指依次使用两个或两个以上基本密码，所得结果的密码强度将强于所有单个密码的强度。

3.5 扩散：使明文的统计特征消散在密文中，这可以这可以通过让每个明文数字尽可能多得影响密文数字获得，等价的说每个密文数字被多个明文数字影响。

混淆：尽可能使密文和加密密钥间的统计关系更加复杂，以阻止攻击者发现密钥。

3.6 Feistel 结构的具体实现所依赖的参数和特征：分组长度、密钥长度、迭代轮数、子密钥产生算法、轮函数 F、快速软件加解密、简化分析难度。

3.7 雪崩效应：明文或密钥的某一位发生变化会导致密文的很多位发生变化。

习题

3.1 对于 n 位的明文分组，有 2^n 个不同的明文分组，2^n 个不同的密文分组，它们的取值范围是 0 到 2^n-1，由于映射是可逆的，所以是一对一映射。假设，明文 0 可以映射的值有 2^n 个，那么明文 1 可映射的值有 2^n-1 个，明文 2 可映射的值

有 2^n-2 个，依次类推，明文 2^n-1 可映射的值有 1 个，如此，对于 n 位的分组长度, 理想分组密码的不同可逆映射个数为$2^n \times (2^n - 1) \times (2^n - 2) \times \cdots \times 2 \times 1 = 2^n!$个。

3.2 由于$k_9 = k_8, k_{10} = k_7, \ldots, k_{16} = k_1$，所以加密过程与解密过程是相同的，故将密文 c 输入加密 oracle 得到的输出就是明文 m。

3.3 （a）我们只需确定剩余的 N-t 个明文 P_j 的概率，题中有$E[K, P_j] \neq E[K', P_j]$，对于所有剩余的 P_i 有$E[K, P_i] = E[K', P_i]$，所以概率为$1 - \frac{1}{(N-t)!}$。