现代密码学第三次作业

2050249 徐正扬

2024 年 5 月 5 日

3.1 设 y 是算法 3.1 在输出为 x 时的输出，π_S 和 π_P 与例 3.1 中的定义相同。换言之

$$y = \mathrm{SPN}(x, \pi_S, \pi_P, (K^1, K^2, \cdots, K^{N_r+1}))$$

这里 $(K^1, K^2, \cdots, K^{N_r+1})$ 是密码编排方案。试找出代换 π_S^* 和 π_P^*，满足

$$x = \mathrm{SPN}(y, \pi_S^*, \pi_P^*, (L^{N_r+1}, L^{N_r}, \cdots, L^1))$$

其中，L^i 是 K^i 的置换。

证明. 令 $\pi_S^* = \pi_S^{-1}$ 和 $\pi_P^* = \pi_P^{-1}$，下证这样的代换满足题意。

首先，$\forall r \in (1, N_r - 1), \forall i \in (1, m)$，下列式子均满足

- $w^{r-1} \oplus K^r = u^r \iff w^{r-1} = u^r \oplus K^r$，$r = N_r$ 时也成立
- $\pi_S(u^r_{<i>}) = v^r_{<i>} \iff u^r_{<i>} = \pi_S^{-1}(v^r_{<i>})$，$r = N_r$ 时也成立
- $(v^r_{\pi_P(1)}, \cdots, v^r_{\pi_P(\ell_m)}) = w^r \iff v^r = (w^r_{\pi_P^{-1}(1)}, \cdots, w^r_{\pi_P^{-1}(\ell_m)})$
- $v^{N_r} \oplus K^{N_r+1} = y \iff v^{N_r} = K^{N_r+1} \oplus y \iff y \oplus v^{N_r} = L^1$

即 SPN 算法中每个步骤均可逆，因此 SPN 算法可逆，故取 π_S^* 和 π_P^* 分别为 π_S 和 π_P 的逆置换即可。 □

3.2 证明解密一个 Feistel 密码相同于对密文使用加密算法，但密钥编排方案要逆序使用。

证明. 首先我们有

$$\begin{cases} L_i = R_{i-1} \\ R_i = L_{i-1} \oplus f(R_{i-1}, K_i) \end{cases}$$

那么

$$\begin{cases} L_{i-1} = R_i \oplus f(L_i, K_i) \\ R_{i-1} = L_i \end{cases}$$

显然，解密算法与加密算法相同，逆置 K_i 即可 □

3.3 设 $DES(x, K)$ 表示使用 DES 在密钥 K 下对明文 x 进行加密，假定 $y = DES(x, K)$ $y' = DES(c(x), c(K))$，这里 $c(\cdot)$ 表示对其自变量按比特位取反。试证明 $y' = c(y)$(即如果把明文和密钥都按比特位取反，则密文同样是按比特反取反)。注意证明这一点只需要使用 DES 的总体描述——与 S 盒的实际结构和系统的其它部件无关。

证明. 首先我们证明

$$f(A,B)=f(c(A),c(B))$$

由于 $f(A,B)=P(S(E(A)\oplus B))$，等价于要证明

$$S(E(A)\oplus B)=S(c(E(A))\oplus c(B))$$

这是显然的。因此，我们有

$$\begin{aligned}c(R_i)&=c(L_{i-1}\oplus f(R_{i-1},K_i))\\&=c(L_{i-1})\oplus f(R_{i-1},K_i))\\&=c(L_{i-1})\oplus f(c(R_{i-1}),c(K_i))\end{aligned}$$

此外，$L_i=R_{i-1} \iff c(L_i)=c(R_{i-1})$

因此，对加密的每个步骤均有

$$\begin{cases}c(L_i)=c(R_{i-1})\\c(R_i)=c(L_{i-1}\oplus f(R_{i-1},K_i))\end{cases}$$

所以，$DES(c(x),c(K))=c(y)=y'$ □

3.7 设明文分组序 $x_1,\cdots,x_n$ 产生的密文分组序列为 $y_1,\cdots,y_n$。假设一个密文分组 y 在传输时出现了错误 (即某些 1 变成了 0，或者相反)。证明不能正确解密的明文分组数在应用 ECB 或 OFB 模式时为 1; 在应用 CBC 或 CFB 模式时为 2

证明.

1. 在 ECB 和 OFB 模式下，如果某个 y_i 出现错误，那么只有对应的 x_i 无法正确解密。其他 $x_j(j\neq i)$ 仍然可以正确解密。
2. 在 CBC 和 CFB 模式下，假设 y_i 出现错误，那么 $x_i=d_K(y_i)\oplus y_{i-1}$ 和 $x_{i+1}=d_K(y_{i+1})\oplus y_i$ 均无法正确解密（这是因为 y_i 出错会导致 y_{i-1} 无法正确恢复。）

□