No. 密码第三章

Date. / /

3.1

$\pi_S^* = \pi_S^{-1}$

$\pi_P^* = \pi_P^{-1}$

3.2

假设密文经过N轮加密后为(L_N, R_N)

解密从最后一轮开始逆向操作：

∵加密时最后一轮：$(L_N, R_N) = (R_{N-1}, L_{N-1} \oplus F(R_{N-1}, K_N))$

∴解密第一轮：$L_{N-1} = R_N \oplus F(L_N, K_N)$，$R_{N-1} = L_N$

∴同理，逐轮逆向操作可以完全恢复明文

3.3

设明文x和密钥K的取反为$C(x)$和$C(K)$

在DES的每一轮中：

轮函数F的输入是R_i和子密钥K_i。由于F由异或和置换组成，且$C(R_i \oplus K_i) = C(R_i) \oplus C(K_i)$，因此$F(C(R_i), C(K_i)) = C(F(R_i, K_i))$。

下一轮的左部分$L_{i+1} = R_i$，右部分$R_{i+1} = L_i \oplus F(R_i, K_i)$。

对于取反的输入$(C(L_i), C(R_i))$和取反的密钥$C(K_i)$下一轮结果为：

$C(L_{i+1}) = C(R_i)$，$C(R_{i+1}) = C(L_i) \oplus C(F(R_i, K_i)) = C(L_i \oplus F(R_i, K_i))$。

∴每一轮的加密结果均为取反后的值

∴$y' = C(y)$

No.
Date. / /

3.7 ① ECB模式

加密：每个明文x_i独立加密，即 $y_i = e_k(x_i)$

解密：每个密文分组独立解密，$x_i = d_k(y_i)$

∴若y_i发生错误，仅影响 $x_i = d_k(y_i)$的解密结果。其它分组y_j($j \neq i$)的解密不受影响

∴错误分组数为1

② OFB模式

加密：先生成一个密钥流$S_i = e_k(S_{i-1})$，初始$S_0 = IV$，密文$y_i = x_i \oplus S_i$

解密：重新生成相同的密钥流$S_i = e_k(S_{i-1})$，明文$x_i = y_i \oplus S_i$

∴y_i若错误，仅影响$x_i = y_i \oplus S_i$的解密结果。由于S_i不依赖密文，后续$S_{i+1}, S_{i+2}, \cdots$不受影响

∴错误组数为1

③ CBC模式

加密：$y_i = e_k(x_i \oplus y_{i-1})$，初始$y_0 = IV$

解密：$x_i = d_k(y_i) \oplus y_{i-1}$

∴若y_i发生错误
- 影响x_i：$x_i = d_k(y_i) \oplus y_{i-1}$，$y_i$错则$x_i$错
- 影响x_{i+1}：$x_{i+1} = d_k(y_{i+1}) \oplus y_i$，$y_i$错则$x_{i+1}$也错
- 不影响x_{i+2}, x_{i+3}：后续分组仅依赖y_{i+1}, y_{i+2}，不受影响

∴错误组数为2

④ CFB模式

加密：$y_i = x_i \oplus e_k(y_{i-1})$，初始$y_0 = IV$

解密：$x_i = y_i \oplus e_k(y_{i-1})$

∴若y_i发生错误
- 影响x_i：$x_i = y_i \oplus e_k(y_{i-1})$，$y_i$错则$x_i$错
- 影响x_{i+1}：$x_{i+1} = y_{i+1} \oplus e_k(y_i)$，$y_i$错则$x_{i+1}$错
- 不影响x_{i+2}, x_{i+3}，后续分组仅依赖y_{i+1}, y_{i+2}，不受影响

∴错误组数为2