现代密码学

3.1. $SPN(x, \pi_s, \pi_p, (k_1, k_2 \dots k_{N_r+1}))$.

$w_0 \leftarrow x$

for $r = 1$ to $N_r - 1$

$$\begin{cases} u_r = w_{r-1} \oplus k_r \\ v_r = \pi_s(u_r) \\ w_r = \pi_p(v_r) \end{cases}$$

$u_{N_r} = w_{N_r-1} \oplus k_{N_r}$

$v_{N_r} = \pi_s(u_{N_r})$

$y = v_{N_r} \oplus k_{N_r+1}$

~~$SPN(y, \pi_s^*, \pi_p^*, (L_{N_r+1}, \dots, L_1))$~~

~~$w_0 \leftarrow y$~~

~~for $r = 1$ to $N_r - 1$~~

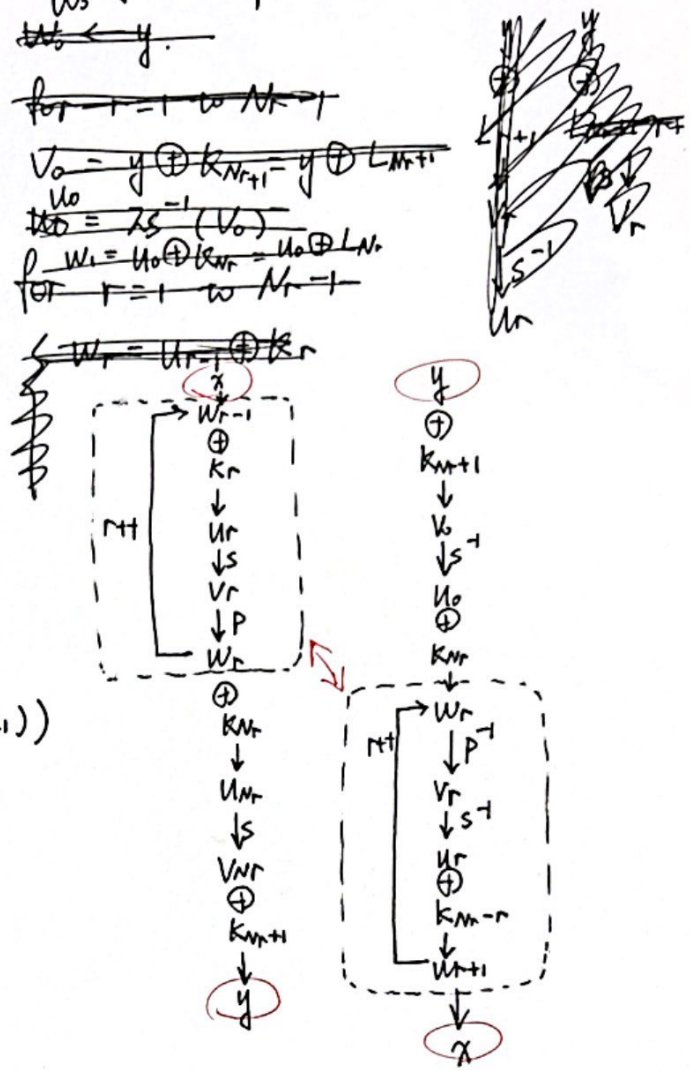
~~$v_0 = y \oplus k_{N_r+1} = y \oplus L_{N_r+1}$~~

~~$u_0 = \pi_s^{-1}(v_0)$~~

~~$w_1 = u_0 \oplus k_{N_r} = u_0 \oplus L_{N_r}$~~

~~for $r = 1$ to $N_r - 1$~~

~~$w_r = u_{r-1} \oplus k_r$~~



$SPN(y, \pi_s^*, \pi_p^*, (L_{N_r+1}, L_{N_r}, \dots L_1))$

~~$w_0 \leftarrow y$~~

$v_0 \leftarrow y \oplus k_{N_r+1}$

$u_0 \leftarrow \pi_s^{-1}(v_0)$

$w_1 \leftarrow u_0 \oplus k_{N_r}$

for $r = 1$ to $N_r - 1$

$$\begin{cases} v_r = \pi_p^{-1}(w_r) \\ u_r = \pi_s^{-1}(v_r) \\ w_{r+1} = u_r \oplus k_{N_r - r} \end{cases}$$

$x \leftarrow w_{N_r}$.

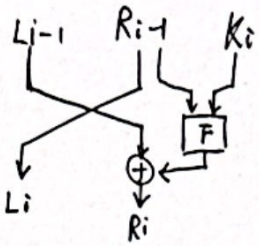
$\therefore \pi_s^* = \pi_s^{-1}$, $\pi_p^* = \pi_p^{-1}$.

数	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
π_s^*	E	3	4	8	1	C	A	F	7	D	9	6	B	2	0	5

z	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
π_p^*	1	5	9	13	2	6	10	14	3	7	11	15	4	8	12	16

3.2.

Feistel 型密码.



对第 i 轮：

$L_i = R_{i-1}$

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

设 Feistel 型密码有 N_r 轮. 明文为 x, 密文为 y.

归纳法证明.

① ~~$R_{N_r} L_{N_r} = IP(y)$~~ $y = R_{N_r} L_{N_r} = L_0' R_0'$

② $i=1$.

$\begin{cases} L_1' = R_0' = L_{N_r} = R_{N_r-1} \\ R_1' = L_0' \oplus f(R_0', k_0') = R_{N_r}^{0} \oplus f(L_{N_r}, K_{N_r}) = L_{N_r-1} \end{cases}$

③ $i=k$.

$\begin{cases} L_k' = R_{k-1}' \\ R_k' = L_{k-1}' \oplus f(R_{k-1}', k_k') \end{cases}$ (假设).

由于已证明 $\begin{cases} L_{k-1}' = R_{N_r-k+1} \\ R_{k-1}' = L_{N_r-k+1} \end{cases}$

$\therefore L_k' = L_{N_r-k+1} = R_{N_r-k}$ (假设).

$R_k' = \cancel{L_{k-1}'} \oplus f(L_{N_r-k+1}, \cancel{k_k'}\ k_{N_r-k+1}) = L_{N_r-k}$ (证毕)

$\cancel{R_{N_r-k+1}}$ (假设).

$\therefore$ 最终由第 N_r 轮输出 $L_{N_r}' R_{N_r}' = R_0 L_0$

将 $R_0 L_0$ 交换得 $x = L_0 R_0$.

$\therefore$ 得证.

3.3.

对于 k: $k \to (k_1, k_2, \dots k_{16})$. 由置换函数得出 若置换不变. 则 $c(k) \to (c(k_1) c(k_2), \dots c(k_{16}))$

对于轮函数: $\longrightarrow c(R_{i-1}) = c(L_i)$.

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

$\hookrightarrow c(L_{i-1}) \oplus f(c(R_{i-1}), c(k_i))$.

~~函数中 A 的 48bit 扩展 $E(A)$.~~

$f(c(R_{i-1}), c(k_i))$.

先将 $c(R_{i-1})$ 扩展为 48bit. $E(c(R_{i-1}))$.

$E(c(R_{i-1})) = c(E(R_{i-1}))$.

再 $E(c(R_{i-1})) \oplus c(k_i) = c(E(R_{i-1})) \oplus c(k_i)$

• 因为两者都异或. 所以异或结果不变.

即 $f(c(R_{i-1}), c(k_i)) = f(R_{i-1}, k_i)$.

$\therefore$ ~~R_i~~ $c(L_{i-1}) \oplus f(R_{i-1}, k_i)$

$= c(R_i)$.

~~$\therefore R_i =$~~

$\because$ 每一轮函数的输出都为原 $L_i R_i$ 异或

$\therefore$ 最终的结果为 $c(y)$.

$\therefore$ 得证

3.7. $x_1 x_2 \dots x_n \to y_1 y_2 \dots y_n$

ECB：解密方式为分组密码加解密对. 又.分组之间相互不影响. 所以只影响出错的那一位所在的分组.

OFB：~~同ECB.~~ 但 y_i 出错 S_i 行无关. 除出错的 y_i 外其余都可以正确通过 $x_i = y_i \oplus s_i$ 解出. s_i 由统一的 e_k 求出.

CBC：设出错的为 y_i

$x_i = d_k(y_i) \oplus y_{i-1}$ →有误.

$x_{i+1} = d_k(y_{i+1}) \oplus y_i$ →有误.

其余：e.g. $x_{i-1} = d_k(\text{改}y_{i-1}) \oplus y_{i-2}$. →不涉及 y_i. 正确

$x_{i+2} = d_k(y_{i+2}) \oplus y_{i+1}$ →不涉及 y_i. 正确.

又：因为是密文出错. 不会影响到后续所有分组.

加密时会用到上一分组的密文 y_{i-1}. 但解密~~不涉及到~~不会使用的文 x_i.

CFB：设出错的为 y_i.

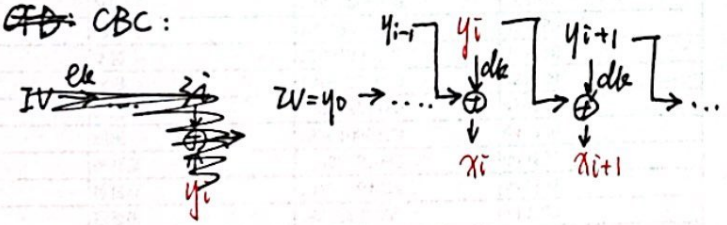
~~$s_{i+1} = e_k(y_i)$~~ x_i 由 $= y_i \oplus s_i$

$x_{i+1} = y_{i+1} \oplus$ 由 $s_{i+1} = y_{i+1} \oplus$ 新 $e_k(y_i)$. } →使用了 y_i. 有误.

其余分组均正确. 理由同上.

图解：

~~CFB~~ CBC：



CFB：