

SPN Encryption/Decryption & Linear Cryptanalysis

请实现 SPN 加密算法

密码体制 代换-置换网络

设 ℓ, m 和 Nr 都是正整数, $\pi_s: \{0,1\}^\ell \rightarrow \{0,1\}^\ell$ 和 $\pi_p: \{1, \dots, \ell m\} \rightarrow \{1, \dots, \ell m\}$ 都是置换。

设 $\mathcal{P} = \mathcal{C} = \{0,1\}^{\ell m}$, $\mathcal{K} \subseteq (\{0,1\}^{\ell m})^{Nr+1}$ 是由初始密钥 K 用密钥编排算法生成的所有可能的密钥编排方案之集。对一个密钥编排方案 (K^1, \dots, K^{Nr+1}) , 我们使用算法来加密明文 x 。

算法 SPN($x, \pi_s, \pi_p, (K^1, \dots, K^{Nr+1})$)

```

 $w^0 \leftarrow x$ 
for  $r \leftarrow 1$  to  $Nr-1$ 
do
 $u^r \leftarrow w^{r-1} \oplus K^r$ 
for  $i \leftarrow 1$  to  $m$ 
do  $v'_{\langle i \rangle} \leftarrow \pi_s(u^r_{\langle i \rangle})$ 
 $w^r \leftarrow (v'_{\pi_p(1)}, \dots, v'_{\pi_p(\ell m)})$ 
 $u^{Nr} \leftarrow w^{Nr-1} \oplus K^{Nr}$ 
for  $i \leftarrow 1$  to  $m$ 
do  $v^{Nr}_{\langle i \rangle} \leftarrow \pi_s(u^{Nr}_{\langle i \rangle})$ 
 $y \leftarrow v^{Nr} \oplus K^{Nr+1}$ 
output( $y$ )
    
```

设 $\ell = m = Nr = 4$,

π_s, π_p 如下定义:

z	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$\pi_s(z)$	E	4	D	1	2	F	B	8	3	A	6	C	5	9	0	7

z	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\pi_p(z)$	1	5	9	13	2	6	10	14	3	7	11	15	4	8	12	16

密钥编排算法:

$K = (k_1, \dots, k_{32})$ 定义 K^r 是由 K 中从 k_{4r-3} 开始的 16 个连续的比特

Sample:

Input: (明文 x , 密钥 K)

0010011010110111 (明文 x)

00111010100101001101011000111111 (密钥 K)

Output: (密文 y)

1011110011010110 (密文 y)