

SPN Encryption/Decryption

请实现SPN加解密算法

密码体制 代换-置换密码

设  $l, m$  和  $Nr$  都是正整数,  $\pi_S : \{0, 1\}^l \rightarrow \{0, 1\}^l$  和  $\pi_P : \{1, \dots, lm\} \rightarrow \{1, \dots, lm\}$  都是置换。设  $P = C = \{0, 1\}^{lm}$ ,  $K \subseteq ((0, 1)^{lm})^{Nr+1}$  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。对一个密钥的排列为  $(K^1, \dots, K^{Nr+1})$ , 我们使用算法来加密明文  $x$ 。

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

```
w0 ← x
for r ← 1 to Nr − 1
    . ur ← wr−1 ⊕ Kr
do . for i ← 1 to m
    . do vr<i> ← πs(ur<i>)
    . wr ← (vrπ(1), ..., vrπ(lm))
uNr ← wNr−1 ⊕ KNr
for i ← 1 to m
    do vNr<i> ← πs(uNr<i>)
y ← vNr ⊕ KNr+1
output(y)
```

设  $l = m = Nr = 4$ ,

$\pi_S, \pi_P$  如下定义:

```
z      0123456789ABCDEF
πS(z) E4D12FB83A6C5907
z      1234 567 8 910111213141516
πP(z) 159132610143 71115 4 81216
```

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  $K$ )

0010 0110 1011 0111 (明文  $x$ )

0011 1010 1001 0100 1101 0110 0011 1111 (密钥  $K$ )

Output: (密文  $y$ )

1011 1100 1101 0110 (密文  $y$ )

