SPN加解密

题目 | #645

题目配置 »

题目名：SPN加解密

编号：645

测试点：11

时间限制：100 ms

空间限制：81920 KiB

完成状态：未提交

通过率：0 / 0

评测全部测试点：否

Special Judge：未启用

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，$\pi_S : \{0,1\}^l \to \{0,1\}^l$ 和 $\pi_P : \{1,\ldots,lm\} \to \{1,\ldots,lm\}$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 $(K^1,\ldots,K^{Nr+1})$，我们使用算法来加密明文 x。

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

$w^0 \leftarrow x$

for $r \leftarrow 1\ to\ Nr-1$

$.u^r \leftarrow w^{r-1} \oplus K^r$

do $.for\ i \leftarrow 1\ to\ m$

.do $v^r_{<i>} \leftarrow \pi_s(u^r_{<i>})$

$.w^r \leftarrow (v^r_{\pi(1)}, \ldots, v^r_{\pi(lm)})$

$u^{Nr} \leftarrow w^{Nr-1} \oplus K^{Nr}$

for $i \leftarrow 1\ to\ m$

do $v^{Nr}_{<i>} \leftarrow \pi_s(u^{Nr}_{<i>})$

$y \leftarrow v^{Nr} \oplus K^{Nr+1}$

output(y)

设 $l = m = Nr = 4$,

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:

$K = (k_1, \ldots, k_{32})$. 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)

提交题目


提交记录