

مفاهیم امنیت

سپهر مقیسه

دکتر شهریاری

۹۸۳۱۱۰۳

پاییز ۱۴۰۱

۱. خیر تفاوتی ندارد چرا که باقی مانده هر ضربی از ۲۶ به ۲۶ یکسان است و همچنین از ۲۷ تا ۵۲ مانند همان ۱ تا ۲۶ عمل میکند.

۲. الف) $100 * 2/99 = 4950$ کلید

ب) در این حالت دیگر از هر فرد نیاز نیست به فرد دیگر کلید موجود باشد و هر کدام یک کلید به سمت رئیس نیاز دارند پس ۱۰۰ کلید

۳.

- Kpa
- Cpa
- Coa
- Mitm : در این روش حمله کننده پیام و یا کلید میان فرستنده و گیرنده را به کمک یک تونل مخفی پیدا میکند
- Acpa

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Plain text : lifeisfullofsurprises

Key: Health

Keystream:healthhealthhea

در هر مرحله از حروف متن برای پیدا کردن ستون و از حروف کلید برای پیدا کردن سطر استفاده میکنیم.

پس در مرحله اول داریم

سطر h و ستون l که میشود s پس همینگونه ادامه میدهیم:

Cipher text: smfp bz mylw hm zyrakpzis

۵.

زیرا در اخر تمام ۱۲۸ بیت را جایگزین میکنند.

۶.

چرا که از متن کدگذاری قبلی برای انجام استفاده میکند برای همین ممکن است خطا بدهد در حالی که ofb از subkey قبل از xor شدن استفاده میکند. و دیگر از سایر بلاک ها نمیگیرد.

.۷

1-

Counter :0000

P0:1100

$F(x, key) = 00$

$00 \text{ xor } 00 = 00$

Output=0000

$0000 \text{ xor } 1100 = 1100$

2-

Counter=0001

P1=1001

$F(KEY, X) = F(01, 1101) = 01$

$00 \text{ xor } 01 = 01$

OUTPUT=0101

$0101 \text{ xor } 1001 = 1100$

3-

Counter=0010

P2=1101

$F(KEY, X) = F(10, 1101) = 10$

$00 \text{ xor } 10 = 10$

OUTPUT=1010

$1010 \text{ xor } 1101 = 0111$

4-

Counter=0011

P3=0101

F(11, 1101)=01

00 xor 01 =01

OUTPUT=1101

1101xor 0101= 1000

C=1100 1100 0110 1000

۸. جایگشت ها، جایگشت انتخابی و چرخش کلید همه به یک نوع عمل میکنند.

در هر مرحله طبق الگوریتم میدانیم که $L_{i+1}=R_i$. فرض میکنیم $A=R_i$ و $B=EP(A)$ و $C=B \text{ xor } k_i$ و $D=S(C)$ (که همان s-box را نشان میدهد) و $E=PC(D)$ حال اگر $A_c=A'$ و $B_c=B'$ و همچنین میدانیم که :

$$a' \text{ XOR } b' = 1 \text{ XOR } a \text{ XOR } 1 \text{ XOR } b = a \text{ XOR } b ,$$

$$a' \text{ XOR } b = 1 \text{ XOR } a \text{ XOR } b = (a \text{ XOR } b)' .$$

نتیجه میگیریم که :

$$C_c = B' \text{ XOR } k_i' = B \text{ XOR } k_i = C.$$

از آنجا که به این نتیجه رسیدیم، خروجی s-box ها به شکل مشابه هستند . پس بعد از مرحله i ام خروجی سمت راست به اینگونه است:

$$R_i = E_c \text{ XOR } L_{i-1}' = E \text{ XOR } L_{i-1}' = R_i'$$