مفاهیم امنیت

سپهر مقیسه

دکتر شهریاری

۹۸۳۱۱۰۳

پاییز ۱۴۰۱

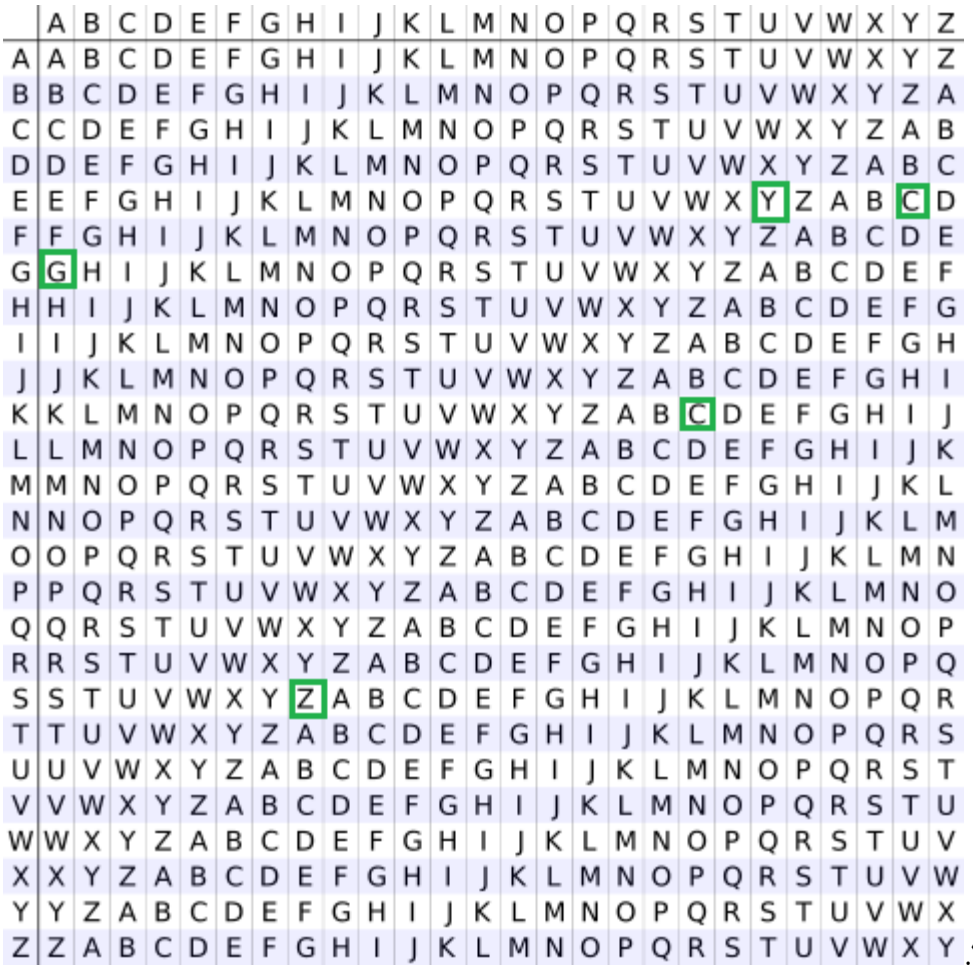
۱.خیر تفاوتی ندارد چرا که باقی مانده هر ضریبی از ۲۶ به ۲۶ یکسان استو همچنین از ۲۷ تا ۵۲ مانند همان ۱ تا ۲۶ عمل میکند.

۲.الف) ۱۰۰*۲/۹۹=۴۹۵۰ کلید

ب)در این حالت دیگر از هر فرد نیاز نیس به فرد دیگر کلید موجود باشد و هرکدام یک کلید به سمت رییس 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



۴.

Plain text : lifeisfullofsurprises

Key: Health

Keystream:healthhealthhealthhea

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 میکند.

۶.

چرا که از متن کدگزاری 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 xor 00= 00

Output=0000

0000 xor 1100=1100

2-

Counter=0001

P1=1001

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

00 xor 01 =01

OUTPUT=0101

0101 xor 1001= 1100

3-

Counter=0010

P2=1101

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

00 xor 10 =01

OUTPUT=1010

1010 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 Li+1=Ri. فرض میکنیم A=Ri و B=EP(A) و C=B xor ki و D=S(C) (که s همان s-boxرا نشان میدهد) و E=PC(D) حال اگر Ac=A’ و Bc=B’ و همچنین میدانیم که :

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

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

نتیجه میگیریم که :

$$C_c = B' \text{ XOR } \mathbf{k}_i' = B \text{ XOR } \mathbf{k}_i = C.$$

از انجا 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:

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