Lab 4: ChopChop Attack

1. Encrypted Algorithm

	Data block 1	Data block 2	Data block 3	ICV
Plaintext	AC	DB	E3	**94**
Keystream	5B	2A	3D	4E
Ciphertext	**F7**	**F1**	**DE**	**DA**

```
PS D:\junior\1\无线与物联网安全\lab4> python .\encrypt.py
输入最多三个16进制数作为明文，用’,’分开：ac,db,e3
输入比明文多1个16进制数，用’,’分开：5b,2a,3d,4e
The ICV is:0x94
['0xf7', '0xf1', '0xde', '0xda']
```

2 ChopChop Attack

Guess	New ICV	Accepted?
0x10	0x2d	**No**
0x3c	0x1	**No**
0x61	0x5c	**No**
0xe6	0xdb	**Yes**

攻击原理

首先假设明文为[D_1,D_2,D_3,I], 密钥为[K_1,K_2,K_3,K_4], 得到的密文是[R_1,R_2,R_3,R_4].

一次chop

一次chop后的明文为[D_1,D_2,J_1], 密文是[R_1,R_2,S_1].

利用“If the guess for the chopped byte is correct, the packet will be a valid WEP packet. It will thus be accepted by the access point. If it is invalid, it will be silently discarded.” 我们可以通过暴力搜索直接得到符合要求的密文S_1， 使得S_1 ^ K_3 == J_1.

之后直接上算式吧：

$$D_1 \oplus D_2 == J_1$$
$$D_3 \oplus K_3 == R_3$$
$$J_1 \oplus K_3 == S_1$$
$$D_1 \oplus D_2 \oplus D_3 == I$$

最后化简可得

$$I == R_3 \oplus S_1$$

由于S是可以暴力搜索破解的，R3是已知的密文，因此可以直接算出I的值。

知道I的值就可以通过$I \oplus R_4$ 得到K_4

二次chop

二次chop后的明文为[D_1,D_2,J_2], 密文是[R_1,R_2,S_2].

与第一次类似，由于J_2 == D_1 , 这次的计算更加简单了。

很容易得到

$$D_1 \oplus D_2 == S_2 \oplus R_2$$

因此，最终结果为

$$D_3 == I \oplus D_1 \oplus D_2 == R_3 \oplus S_1 \oplus S_2 \oplus R_2$$

攻击程序的运行截图