Assignment 2 solution analysis

To get the decryption function , we should analysis the encryption function

Encryption function :

It encrypts blocks with block size 16 byte and it consist of 32 round

Each round has 2 steps :

First step:

a, b, c, d = b ^ F(a | F(c ^ F(d)) ^ F(a | c) ^ d), c ^ F(a ^ F(d) ^ (a | d)), d ^ F(a | F(a) ^ a), a ^ 31337

second step :

a, b, c, d = c ^ F(d | F(b ^ F(a)) ^ F(d | b) ^ a), b ^ F(d ^ F(a) ^ (d | a)), a ^ F(d | F(d) ^ d), d ^ 1337

then in the decryption process :

firstly change steps order , then let's analysis the equations :

the idea is when a= b ^ 5 then also b = a ^ 5

then the solution is :

for each round :

```
second step
original_a = a
d = d ^ 1337
a = c ^ F(d | F(d) ^ d)
b = b ^ F(d ^ F(a) ^ (d | a))
c = original_a ^ F(d | F(b ^ F(a)) ^ F(d | b) ^ a)
# first step
original_a = a
a = d ^ 31337
d = c ^ F(a | F(a) ^ a)
c = b ^ F(a ^ F(d) ^ (a | d))
b = original_a ^ F(a | F(c ^ F(d)) ^ F(a | c) ^ d)
```

notice we saved the original value of a because it is edited before use