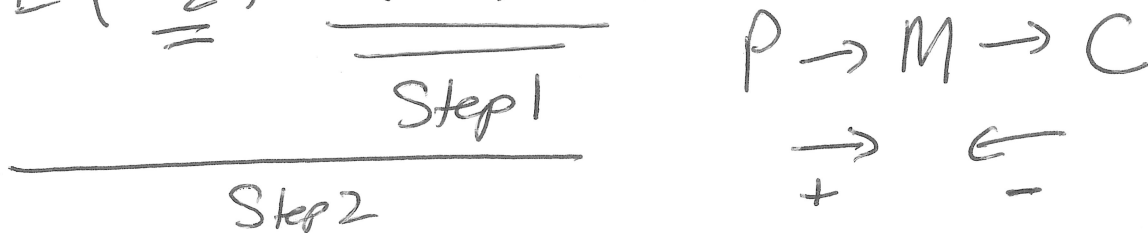


① Double Des, Triple DES

② ~~Cipher~~ Block Cipher Modes

Double DES

$$C = E(\underline{K_2}, \underline{E(K_1, P)})$$



Flaw: Meet in the Middle Attack

Matching plaintext  $P'$  with ciphertext  $C'$   
 Don't know  $K_1$ , or  $K_2$ .

Try all possible keys  $X_1, X_2, X_3, \dots, X_{2^{56}}$

$E(X_1, P') = M_1$ $E(X_2, P') = M_2$ $\vdots$ $E(X_{2^{56}}, P') = M_{2^{56}}$	Store in hash table/map $M_1 = X_1$ $M_2 = X_2$ $\vdots$ $M_{2^{56}} = X_{2^{56}}$	Time Memory $O(n)$ $n = 2^{56}$ keyspace
--	--	---

Next Try all possible decryption keys for step 2  
 $Y_1, Y_2, \dots, Y_{2^{56}}$

$D(Y_1, C') \rightarrow M'_1$  (look up if  $M'_1$  is in our table)  
 $D(Y_2, C') \rightarrow M'_2$  keep track of all  
 $D(Y_{2^{56}}, C')$  pairs  $X_i, Y_j$  that meet in middle

# Triple DES

2 possible implementations

$$1) C = E(k_3, \underbrace{E(k_2, \underbrace{E(k_1, P))}_{\text{step 1}})}_{\text{step 2}})_{\text{step 3}}$$

meet in middle  $2^{112}$  steps forward

$2^{56}$  backward or vice versa but run-time is

$O(n^2)$  where  $n = 2^{56}$ .

$$2) C = E(k_1, E(k_2, E(k_1, P)))$$

Just use 2 keys instead of 3, same amt of time/memory to break!

7th edition

Source: Cryptography + Network Security by  
Stallings (Chapter 7)  
7.1

# Block Cipher Modes

All our discussion of DES, AES describe encrypting a single block.

## Electronic Codebook Mode

① Intuitive Ans

$$P = P_1 P_2 P_3 \dots P_n$$

$$C = C_1 C_2 C_3 \dots C_n$$

for  $i=1$  to  $n$

$$C_i = E(K, P_i)$$

Just use the algorithm  $n$  times and encrypt each block!

Can be done in parallel!  
Drawback: lots of info w/ same key!

## Cipher Block Chaining Mode

$$C_0 = IV \text{ (initialization vector)}$$

for  $i=1$  to  $n$

$$C_i = E(K, C_{i-1} \oplus P_i)$$

random #  
agreed upon

$$P_1 = 1011 \rightarrow C_1 = 0010$$

$$P_2 = 0101$$

$$C_1 \oplus 0010$$

$$\underline{0111}$$

etc.

$$\rightarrow C_2 = 1001$$

Better  $\rightarrow$  not all items encrypted are plaintext, almost random.

$\rightarrow$  previous ciphertext

Drawback: Done in serial, can't do parallel!

## Output Feedback Mode

$$K_0 = IV$$

for  $i=1$  to  $n$

$$K_i = E(K, K_{i-1})$$

$$C_i = P_i \oplus K_i$$

Can be parallelized.

Stream can be precomputed  
(it's always the same)

## Cipher Feedback Mode

$$C_0 = IV$$

for  $i=1$  to  $n$

$$K_i = E(K, C_{i-1})$$

$$C_i = P_i \oplus K_i$$

Can't NOT be parallelized

bit stream will be  
different each time

## Counter Mode

for  $i=1$  to  $n$

$$K_i = E(K, \text{Counter}[i])$$

$$C_i = P_i \oplus K_i$$

0, 1, 2, 3, ... of  
 $x, x+1, x+2, \dots$  of  
 $x, f(x), f(f(x)), \dots$   
↳ guaranteed to be unique...

# QUIZ NOTES

---

$\sim \frac{1}{2}$  DES,  $\sim \frac{1}{2}$  AES

MixCols  $\rightarrow$  one row one col  $\} \rightarrow$  one cell  
you MUST attempt to calculate the correct cell for  
any credit! (1-based indexes 1,2,3,4)

---

each question specifies format of answer  
(binary, decimal, hex), pts are taken off if  
you don't use the requested format!

---

Make sure you use the right S-box for  
DES!

---

There is a bitwise op coding question!

---

look @ multiplication in AES field so  
you can reason about it.