One Time Pad (OTP): provely secure

① only use key once

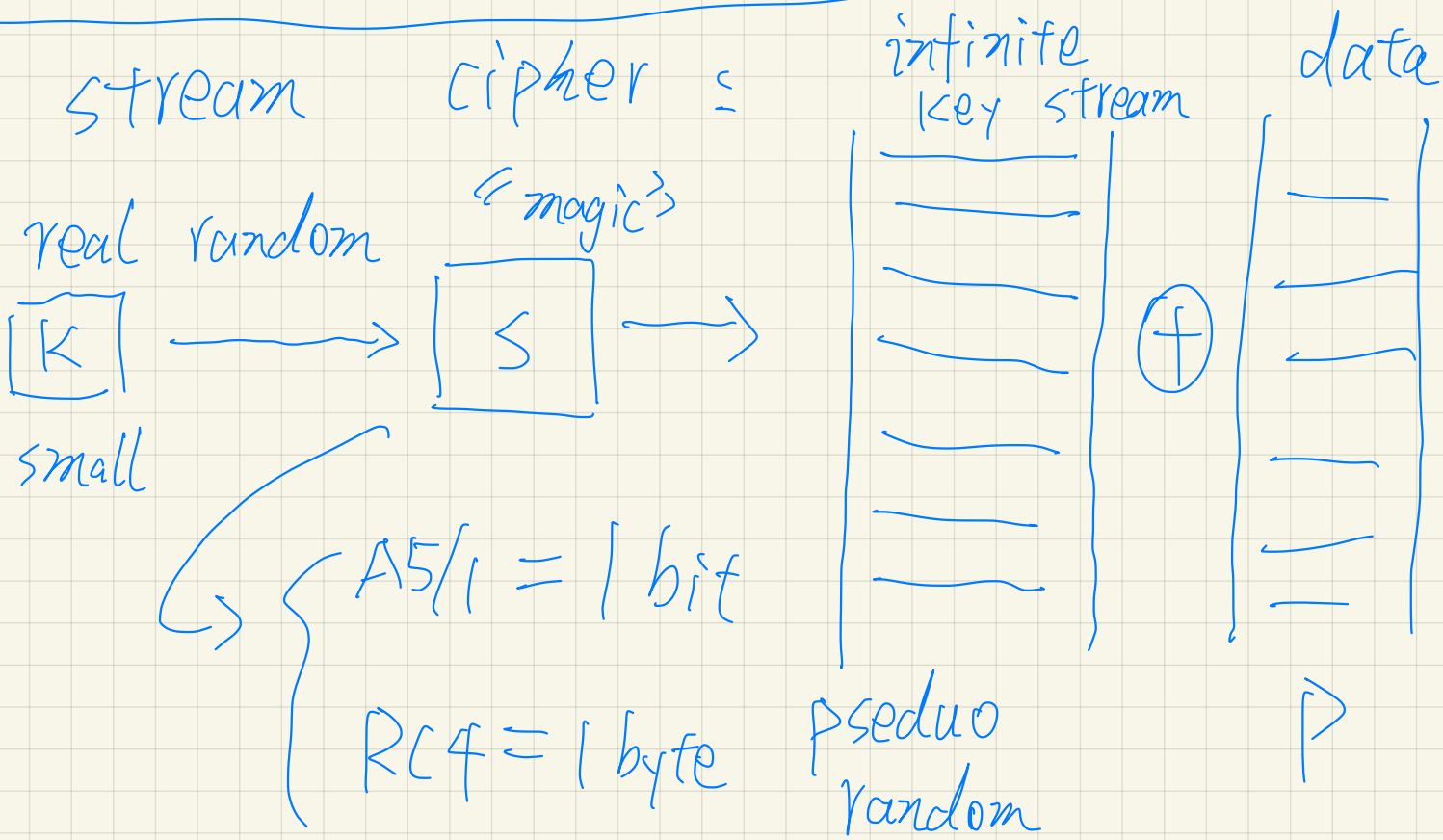
$$P_1 \oplus K \quad P_2 \oplus K \Rightarrow C_1 \oplus C_2 = P_1 \oplus K \oplus P_2 \oplus K = P_1 \oplus P_2$$

② K must have same length as msg

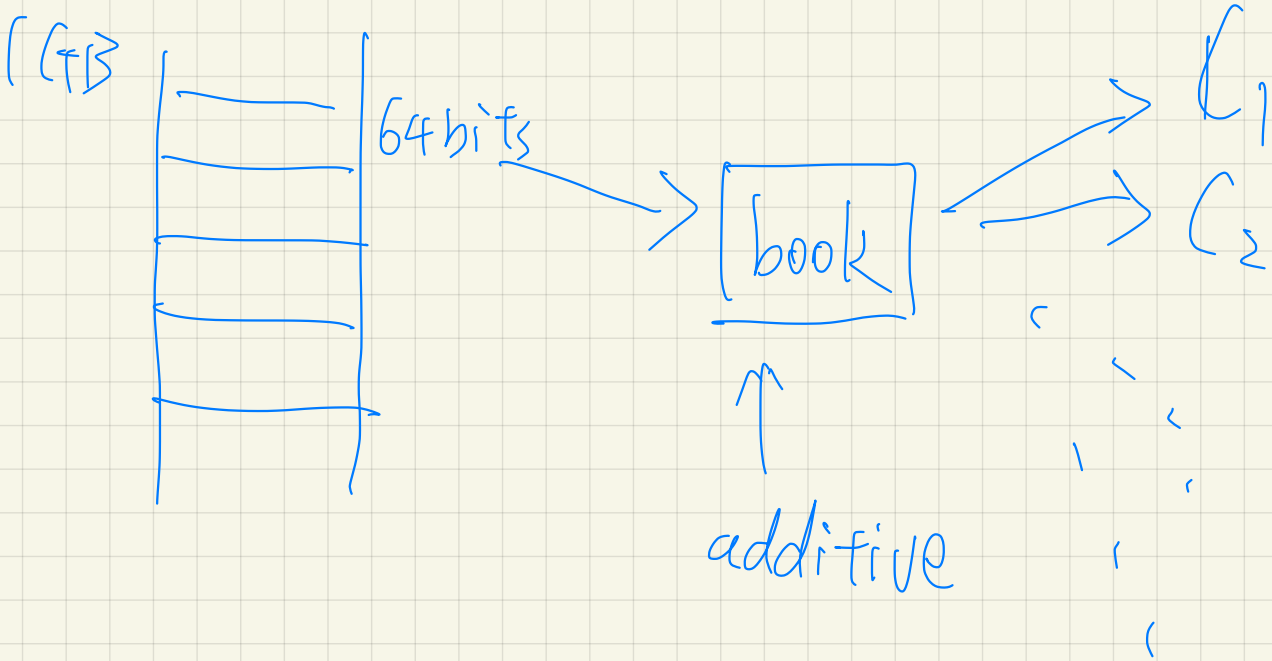
③ K real random

---

stream cipher:



code book cipher $\Rightarrow$ block cipher



block cipher :

- AES : standard
- DES : was standard
- TEA :
  - malware
  - ransomware

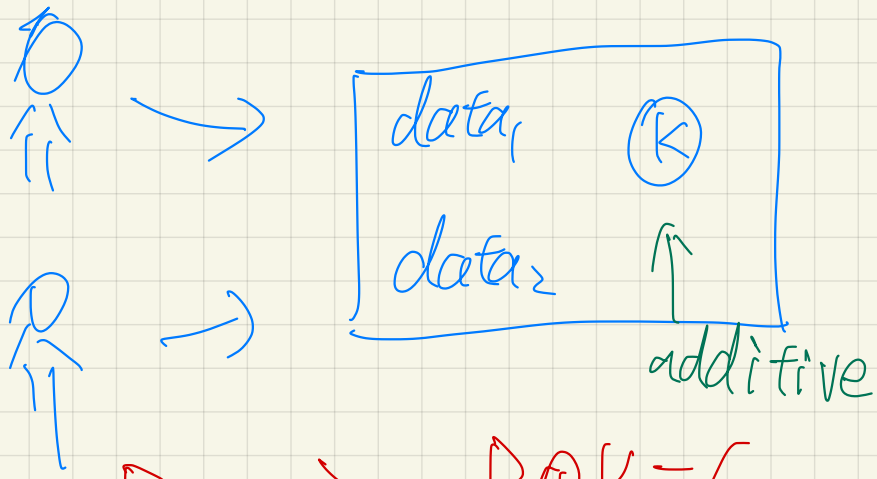
$P \oplus K = C$

① confidentiality

② crypto analysis

"attack"

③ reuse



$P_1 \oplus K \Rightarrow C_1$

$P_2 \oplus K \Rightarrow C_2$

$C_1 \oplus C_2 = P_1 \oplus K \oplus P_2 \oplus K$

$= P_1 \oplus P_2$

$P \longrightarrow P \oplus K = C$

$P \oplus C = P \oplus P \oplus K = K$

$P \oplus K \oplus A = C$

$P \oplus C = P \oplus K \oplus A \oplus P = K \oplus A$

Block cipher

S-box $\quad S[P \oplus K] = C$

① non-secret

② non-linear function

$$P \oplus C = P \oplus S[P \oplus K]$$

$$S \longrightarrow \boxed{S^{-1}}$$

$$S^{-1}[C] = S^{-1} \circ S[P \oplus K] = P \oplus K$$

$$P \oplus C \Longleftrightarrow K$$

$$C = S[K \oplus P] \oplus K$$

K_1 $\quad K_1 \neq K_2$ related $\quad K_2$

$$P \oplus C = S[K \oplus P] \oplus K \oplus P$$

$$S^{-1} \Rightarrow \quad S^{-1} \circ \underbrace{\left(S[K \oplus P] \oplus K\right)}_{C}$$

$$C = S[K_1 \oplus P] \oplus K_2$$

1992

John Daemen

K_1 n bits

K_2 n bits

$\frac{n}{2}$

$K \leftarrow \underline{2n}$ bits

K_1 128 bits

K_2 128 bits

2^{64}

$$K_5 \oplus S[K_4 \oplus S[K_3 \oplus \underbrace{S[K_2 \oplus S}_{\text{round}}[K_1 \oplus S[K_0 \oplus P]]]]]$$

more rounds $\Rightarrow$ better security $\Rightarrow 2^{\frac{n}{2}}$

more rounds $\Rightarrow$ slow

---

optimal configuration:

DES: 16 rounds

$K = 56$ bits

$\vdots$

$K_1 \cdots K_{16} = 48$ bits

AES: 10 ~ 14 rounds

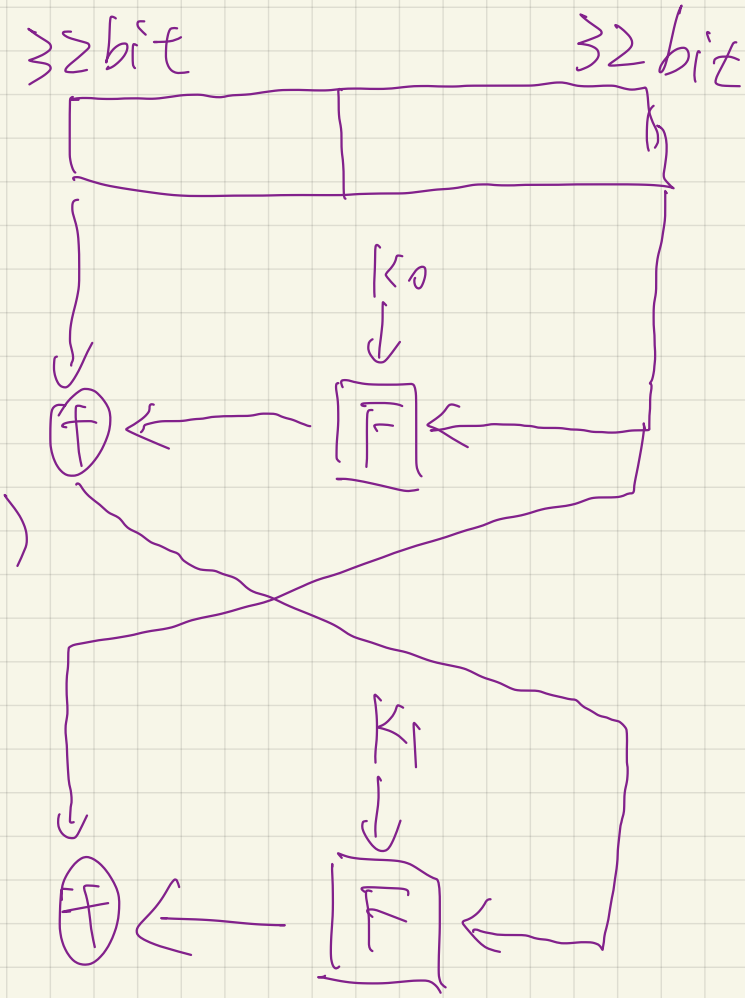
$K = 128, 192, \underbrace{256 \text{ bits}}$

$P = 128$ bits

$2^{\frac{n}{2}}$

$= 2^{118}$

Feistel:



$$L_{i+1} = R_i$$

$$R_{i+1} = L_i \oplus F(R_i, K_i)$$

$$\vdots$$

$$C = (L_{n+1}, R_{n+1})$$

16 rounds $\Rightarrow$ DES

2-DES:

56

① $C = E(\underset{\sim}{K}, E(\underset{\sim}{K}, P))$

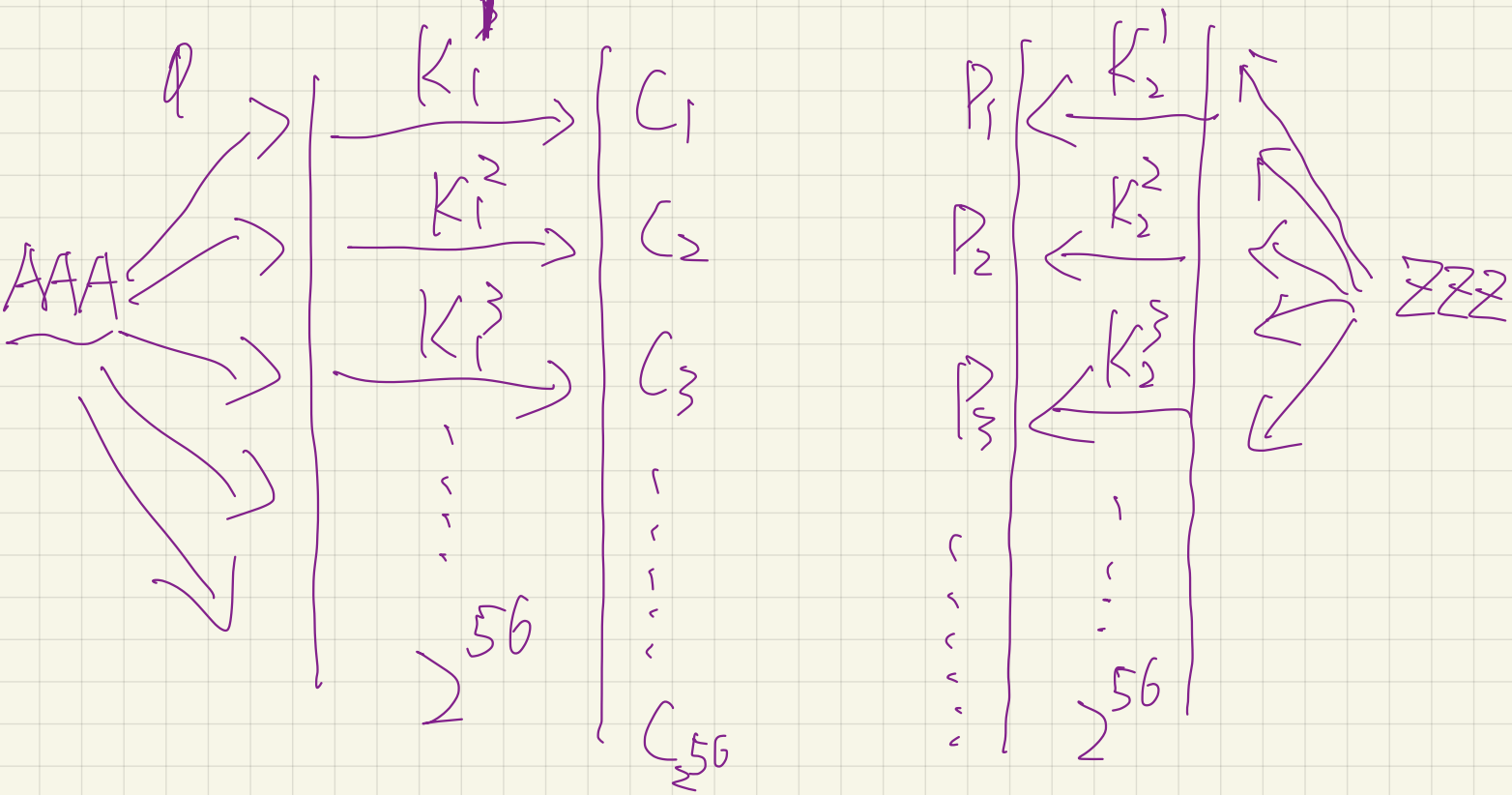
56 bits

② $C = E(K_1, E(K_2, P))$

56 56

meet-in-the-middle

$\underline{AAA} \xrightarrow[E]{K_1} ??? \xrightarrow[E]{K_2} ZZZ$



$$C_{32} = P_{56}$$

$$AAA \xrightarrow{K_1^{32}} \cdots \xrightarrow{K_2^{56}} ZZZ$$

$$2^{56} + 2^{56} = 2^{57}$$

3-DES: $\underline{112}$

① $C = E(K_1, E(K_2, E(K, P)))$

112 bits

$$\boxed{\text{3-DES}} \longrightarrow \boxed{\text{DES}}$$

② $C = E(K_1, D(K_2, E(K_1, P)))$

112 bits

$\boxed{\text{3-DES}} \longrightarrow \boxed{\text{DES}}$

$K_1 = K_2$

$$\underset{P}{\boxed{1\text{ bit}}} \longrightarrow \underset{\text{S-box}}{\boxed{E}} \longrightarrow \underset{C}{\boxed{1\text{ bit}}}$$

C \ P	0	1
0	50%	50%
1	50%	50%

$$C \not\Rightarrow P \quad \text{independent}$$

C \ P	0	1
0	90%	10%
1	10%	90%

$$\begin{cases} C = P & 90\% \\ C \neq P & 10\% \end{cases}$$

ill-designed

$x_0 x_1 x_2$

		$x_1 x_2$			
		00	01	10	11
x_0	0	10 ✓	00 ✓	10 ✓	00 ✓
	1	00 ✗	10 ✗	01 ✓	11 ✓

$x_0 x_1 x_2 \to y_0 y_1$

secure?

$y_1 = x_0$

$\frac{6}{8} = 75\%$

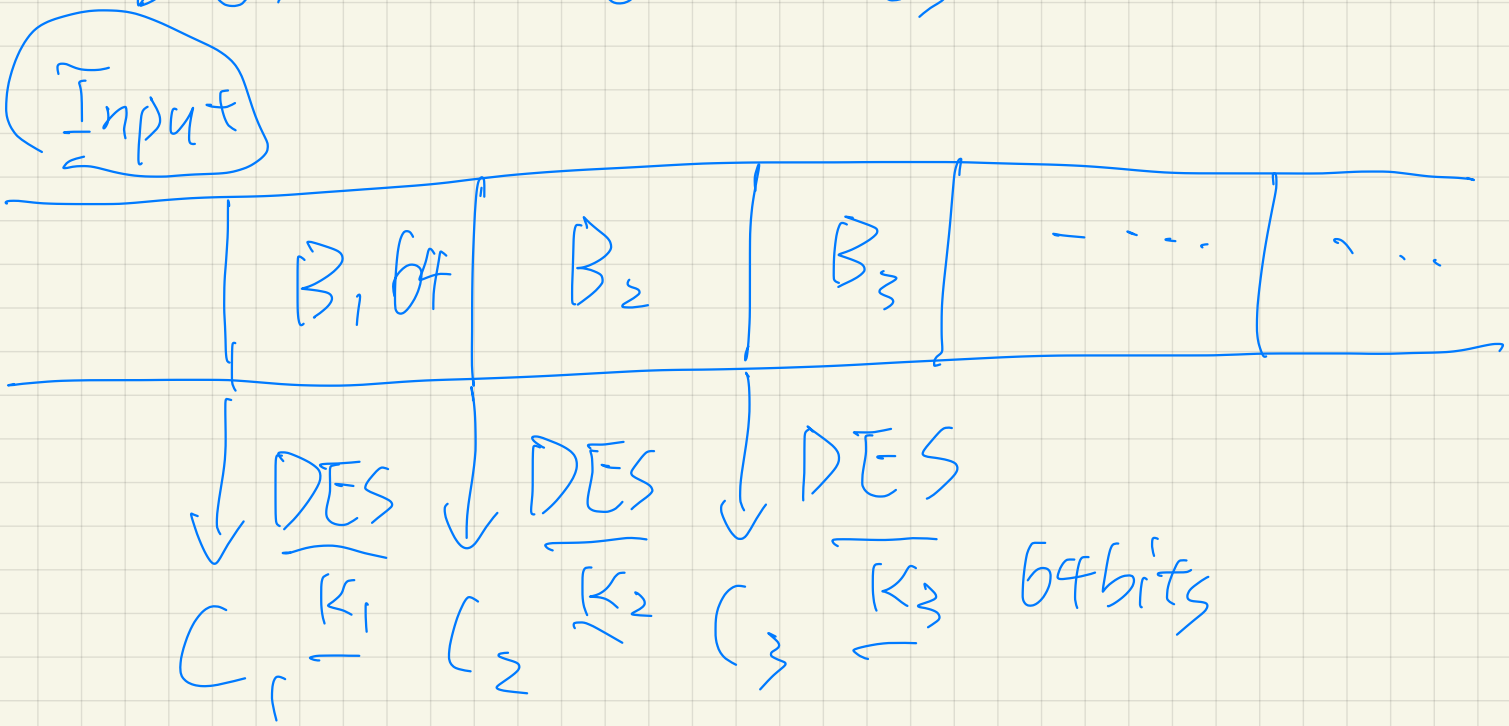
$y_1 \neq x_0$

25%

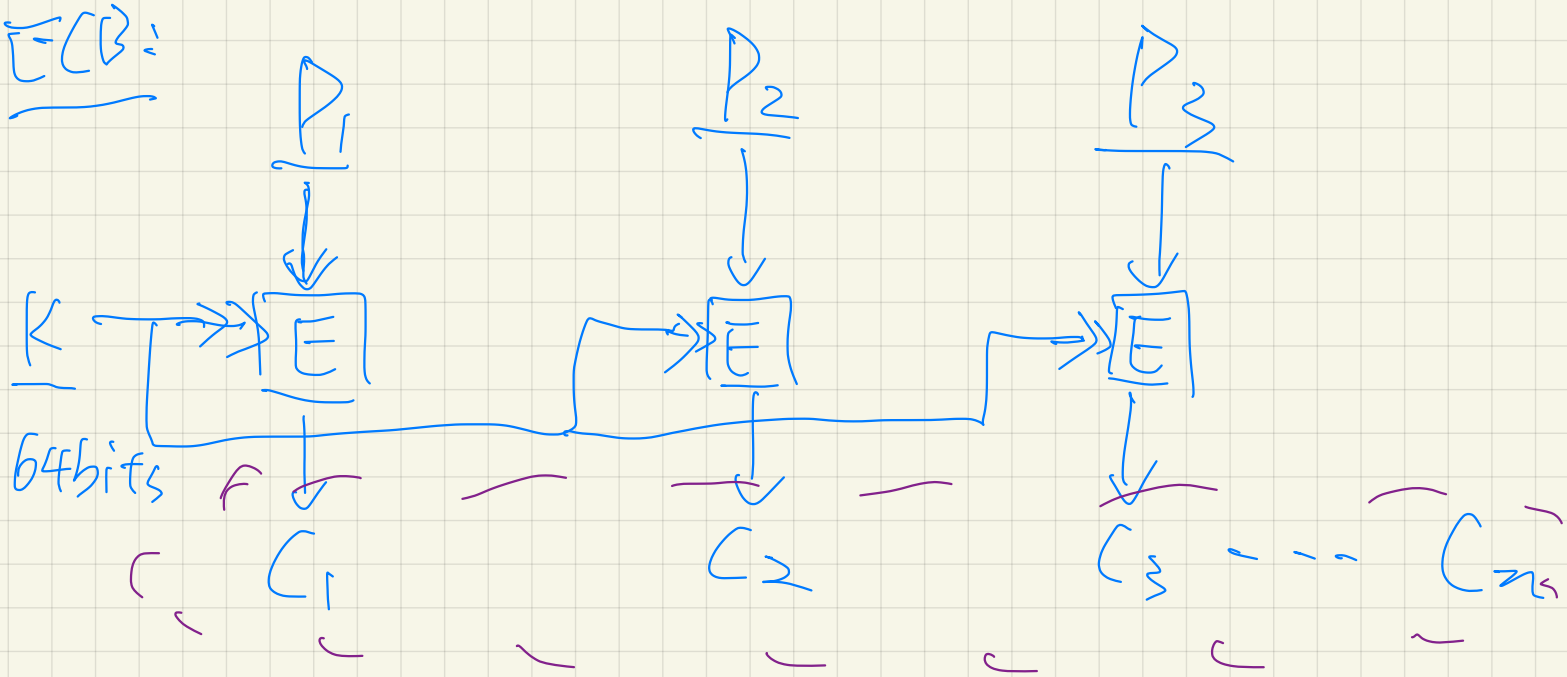
$y_1 = 1 \Rightarrow x_0 = 1$

75%

DES: 64 bits

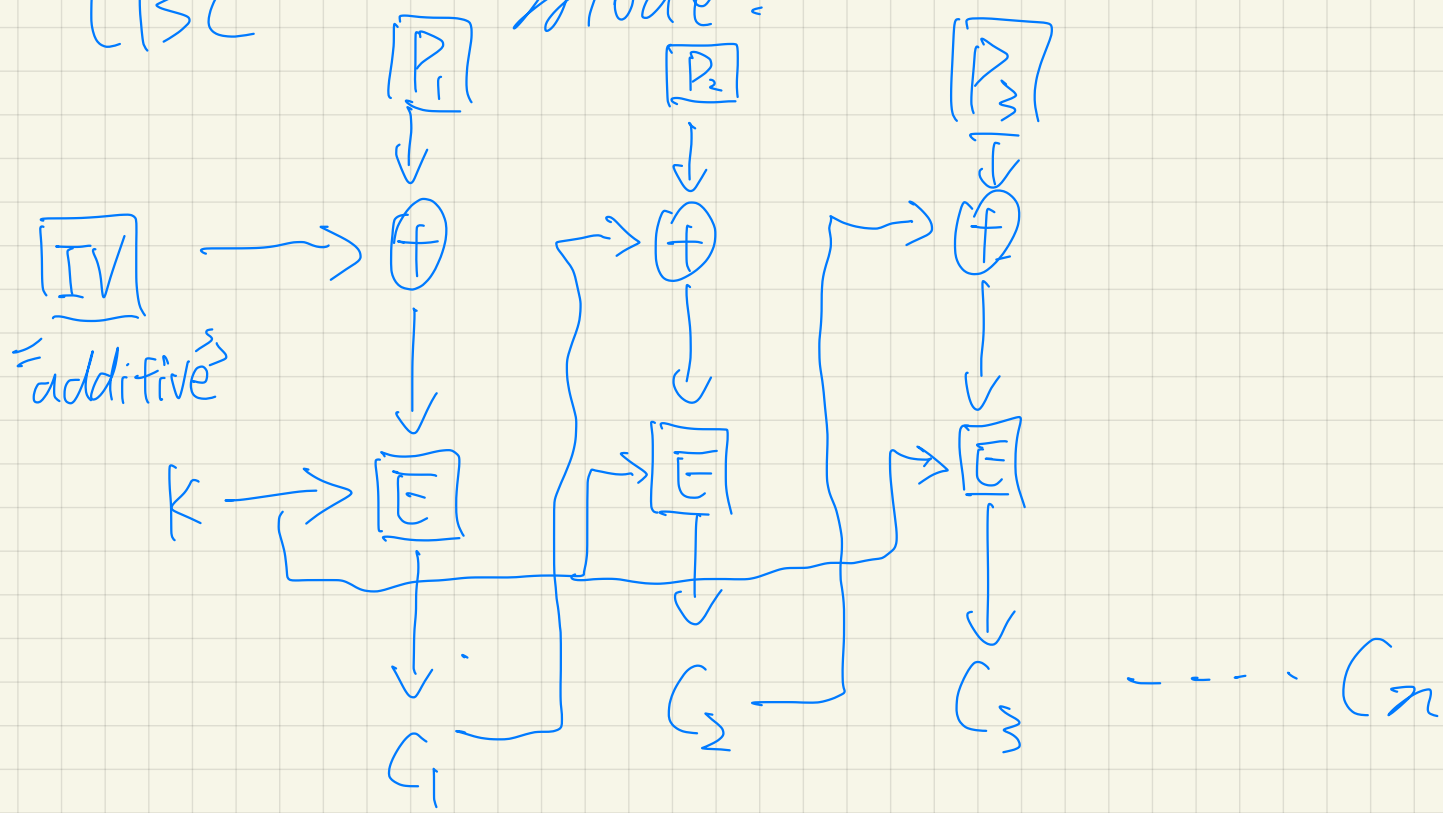


ECB:



$P_2 = P_{51}$ $C_2 = C_{51}$

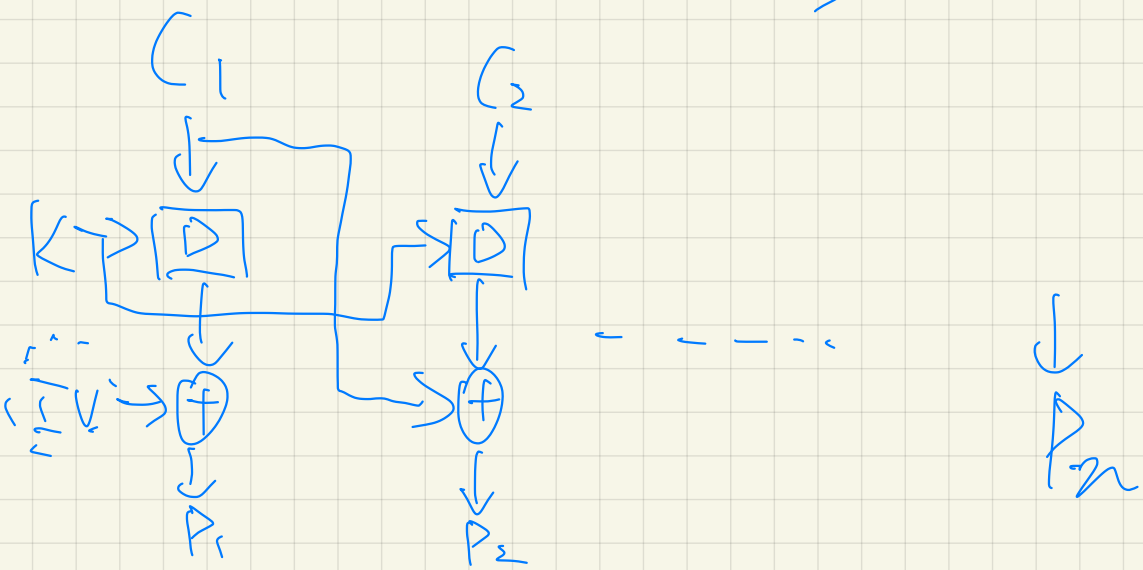
CBC mode:



$$IV \,||\, C_1 \,||\, C_2 \,||\, C_3 \,||\, \cdots \,||\, C_n$$

$$P_2 = P_3$$

$$C_2 \neq C_3$$



$A \longrightarrow B$

$P = P_1 \| P_2 \| P_3 \cdots \xrightarrow{K_1} C_1 \| C_2 \| C_3 \cdots$

$P = P_1 \| P_2 \| P_3 \cdots \xrightarrow{K_2} C_1' \| C_2' \| C_3' \cdots \underline{C_n'}$

IV C_1 C_2 C_3 $\cdots$ C_n C_n'

B: ① confidentiality:

$\underline{C_1 \| C_2 \| C_3 \cdots} \xrightarrow{K_1} P_1 \| P_2 \| P_3 \cdots$

② Integrity:

$\underline{P_1 \| P_2 \| P_3 \cdots} \xrightarrow{K_2} C_1' \| C_2' \| \cdots C_n'$

$K_1 \neq K_2$

related

$K_1 \leftarrow C \qquad K_2 \leftarrow I$

$A \longrightarrow B$

$$C = C_1 \| C_2 \| C_3 \| C_4 \cdots \| \underbrace{C_n \; C_n'}_{XXX}$$

$$P_n = C_{n-1} \oplus D_K(C_n) \qquad P_n' = C_{n-1}' \oplus D_K(C_n)$$

$$P_{n-1} = C_{n-2} \oplus D_K(C_{n-1}) \qquad P_{n-1}' = C_{n-2}' \oplus D_K(C_{n-1}')$$

$$\vdots \qquad \vdots$$

decrypt

$$P_1 = IV \oplus D_K(C_1) \qquad P_1' = IV \oplus D_K(C_1')$$

$$MAC = E_K(P_n \oplus E_K(P_{n-1} \oplus E_K(\cdots \oplus E_K(P_1 \oplus IV))))$$

MAC

$$MAC' = E_K(P_n' \oplus \underbrace{E_K(P_{n-1}' \oplus E_K(\cdots \oplus E_K(P_1' \oplus IV))}_{C_{n-1}'})$$

C_1'

$$MAC' = E_K(P_n' \oplus C_{n-1}')$$

$$= C_n = MAC$$

Encrypt then MAC:

$$\boxed{P} \xrightarrow[K_1]{} \boxed{C} \xrightarrow[K_2]{} MAC$$

✓ OpenSSL

1. I ☆
2. decrypt

MAC then encrypt:

$$\boxed{P} \xrightarrow[K_2]{} MAC \xrightarrow[K_1]{} \boxed{P+MAC}$$

✗

1. decrypt
2. I

Encrypt and MAC:

$$\boxed{P} \xrightarrow{K_1} \boxed{C}$$

$$\boxed{P} \xrightarrow{K_2} \boxed{MAC}$$

✗

1. decrypt
2. I

stop before decrypt