03 Block Cipher

2021 Spring

Information Security

Teacher: Po-Wen Chi

neokent@gapps.ntnu.edu.tw

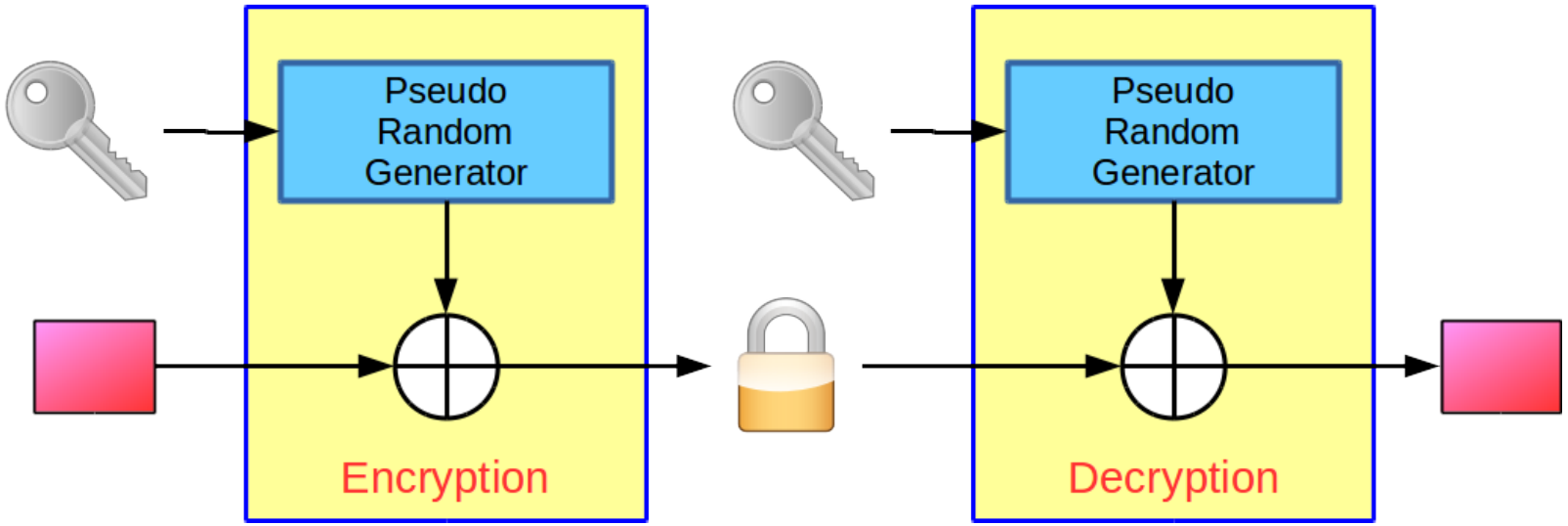
March 9, 2021

Department of Computer Science and Information Engineering,

National Taiwan Normal University

What is Block Cipher?

Stream Cipher



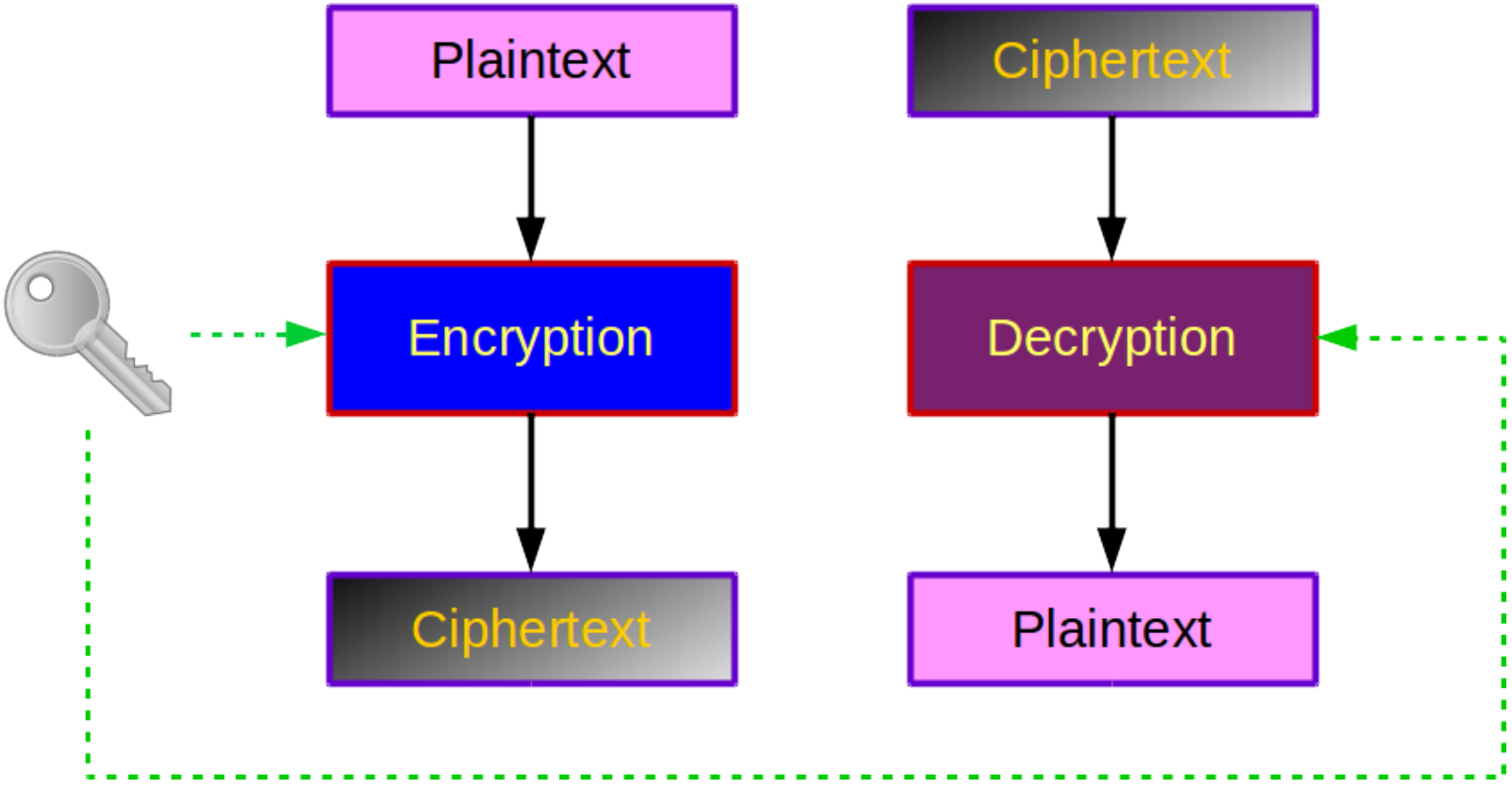
Encryption and **Decryption** are the same algorithm.

Informal Definition

Block Cipher

A block cipher is one in which a block of plaintext is treated as a whole and used to produce a ciphertext block of equal length.

Block Cipher



Encryption and **Decryption** are normally two different algorithms.

Definition

Pseudo Random Function

$F : K \times X \to Y$ such that exists an efficient algorithm to evaluate $F(k, x)$.

Pseudo Random Permutation

$E : K \times X \to X$ such that

1. Exists an efficient deterministic algorithm to evaluate $E(k, x)$.
2. E is an one-to-one function.
3. Exists an efficient inversion algorithm.

Definition

Pseudo Random Function

$F : K \times X \to Y$ such that exists an efficient algorithm to evaluate $F(k, x)$.

Pseudo Random Permutation

$E : K \times X \to X$ such that

1. Exists an efficient deterministic algorithm to evaluate $E(k, x)$.
2. E is an one-to-one function.
3. Exists an efficient inversion algorithm.

Actually, a block cipher is a Pseudo Random Permutation function.

What can PRF Do?

- Undoubtedly, you can use PRF to create a PRG.
  - How?
- This also implies that PRF can be used to construct a stream cipher.
- We will discuss PRF later.

What can PRF Do?

- Undoubtedly, you can use PRF to create a PRG.
  - How?
  - $G(k) = F(k, 0)||F(k, 1)|| \ldots ||F(k, t-1)$.
- This also implies that PRF can be used to construct a stream cipher.
- We will discuss PRF later.

What can PRP Do?

- PRPs are **block ciphers**.
- Functionally speaking, a PRP is also a PRF.
  - A PRP is a PRF where $X = Y$ and is efficiently invertible.

Quiz

Is is possible to use a block cipher to construct a stream cipher?

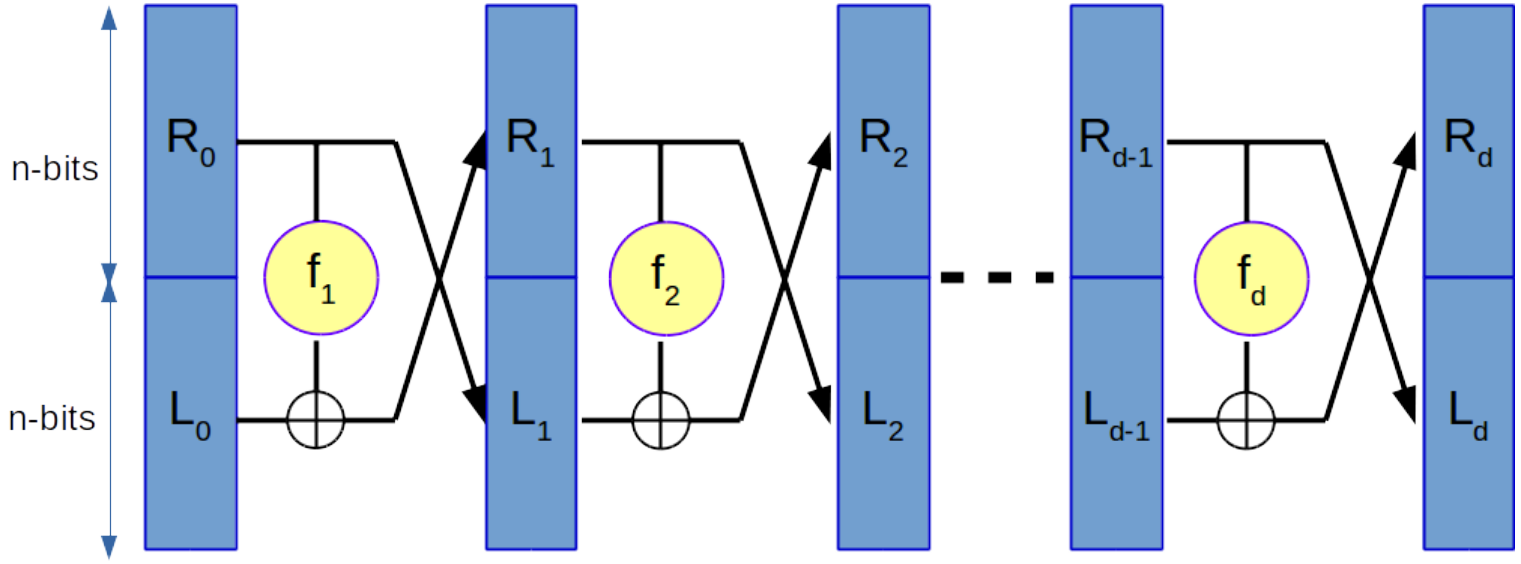
Quiz

Is is possible to use a block cipher to construct a stream cipher?

YES.

Feistel Cipher

Feistel Network



$f_1, f_2, \ldots, f_d : \{0,1\}^n \to \{0,1\}^n$ are PRF.

$$\begin{cases} R_i = L_{i-1} \oplus f_i(R_{i-1}) \\ L_i = R_{i-1} \end{cases}$$

Quiz

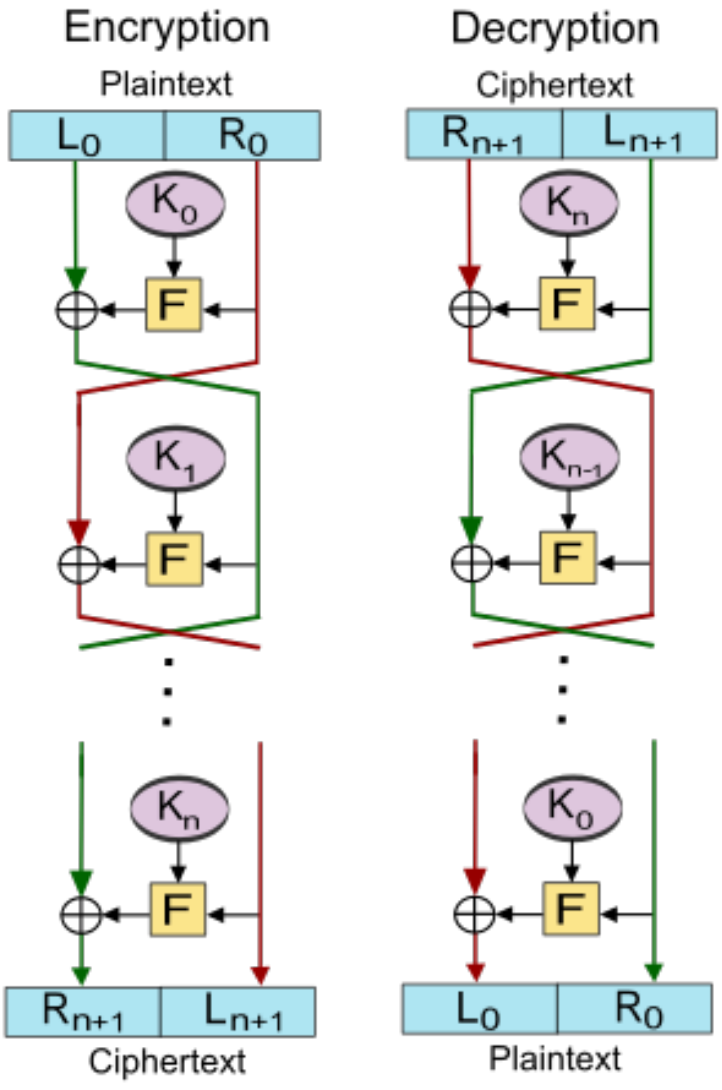
How to invert Feistel Networks?

Quiz

How to invert Feistel Networks?

$$\begin{cases} R_{i-1} = L_i \\ L_{i-1} = R_i \oplus f_i(L_i) \end{cases}$$

Feistel Network



- For all function f, the Feistel network is invertible.
  - Even f is not invertible.
- The encryption circuit and the decryption circuit are the same.

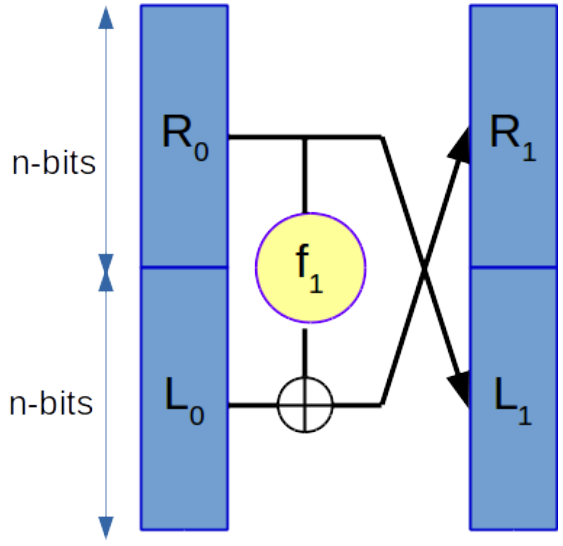
Feistel Network is a Secure Cipher

What is a secure cipher??

Conditions:

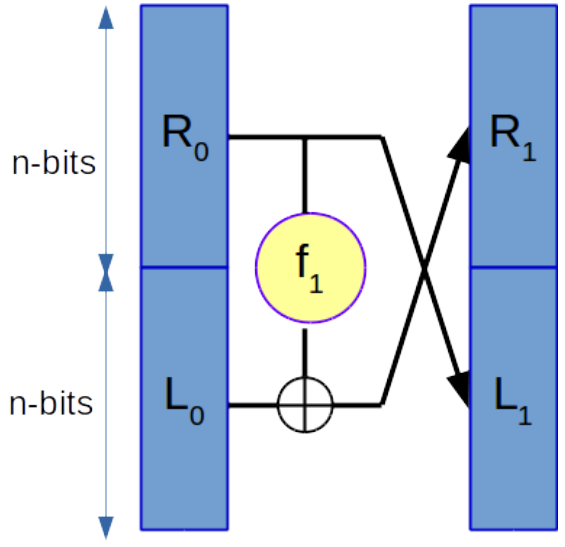
1. $f : K \times \{0,1\}^n \to \{0,1\}^n$ is a secure PRF.
2. 3-round and above.
3. Keys are independent.

Why 3-round Above?



Can you generate m_0, m_1 and determine which one is encrypted when receiving c?

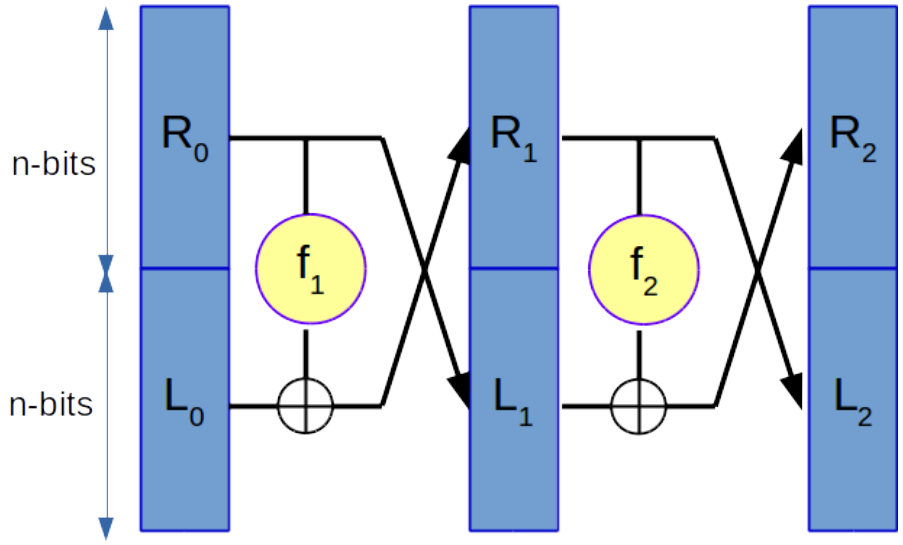
Why 3-round Above?



Can you generate m_0, m_1 and determine which one is encrypted when receiving c?

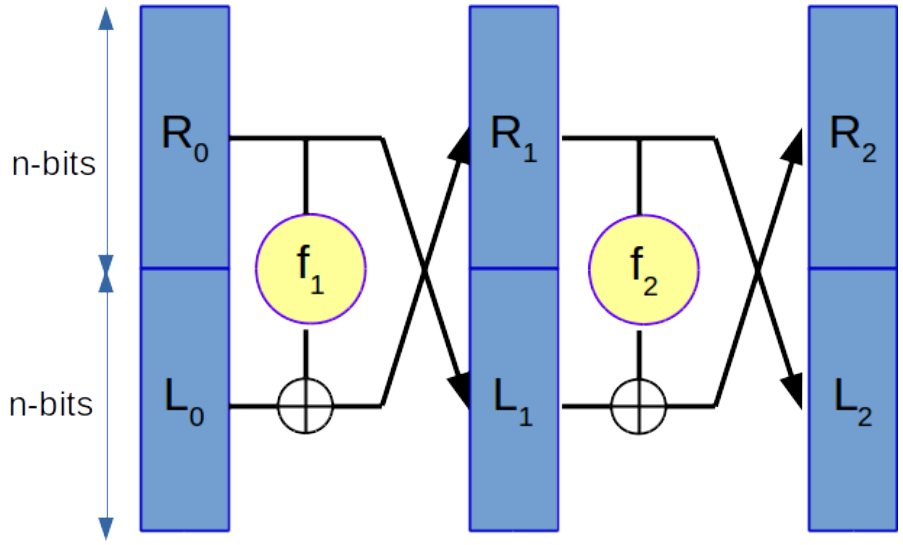
- Just choose two messages with different R_0.

Why 3-round Above?



Can you generate m_0, m_1 and determine which one is encrypted when receiving c?

Why 3-round Above?

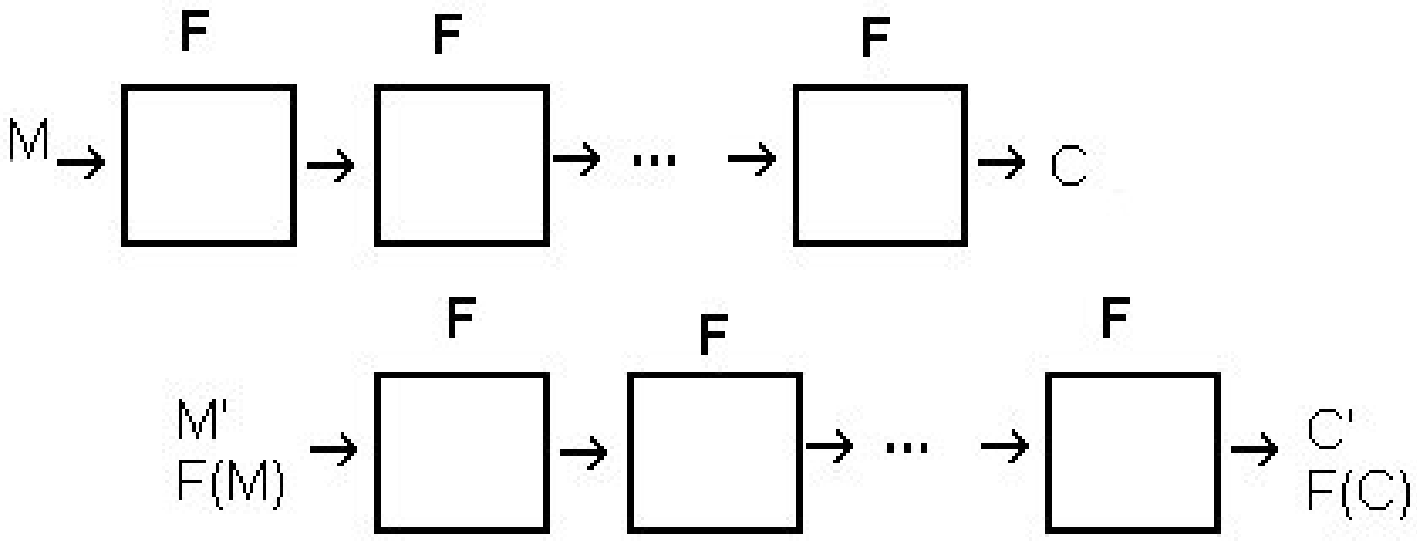


Can you generate m_0, m_1 and determine which one is encrypted when receiving c?

If $E(L, R) = (L', R')$, then $E(L \oplus T, R) = (L' \oplus T, R'')$.

Why Keys must be Independent?

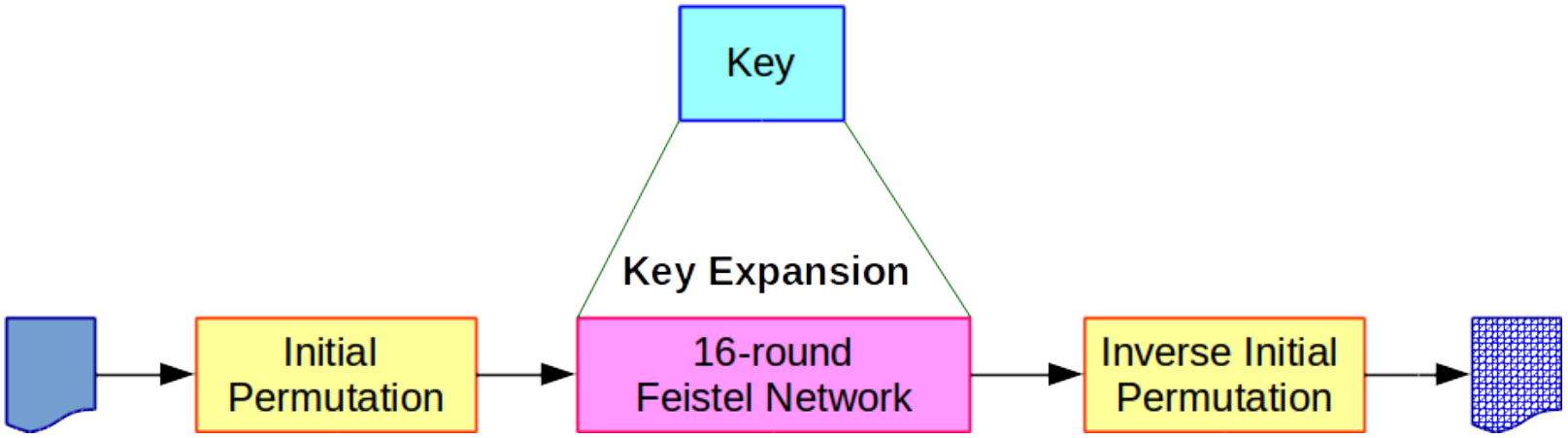
Slide attack.



Do you know what this means? This is your homework.

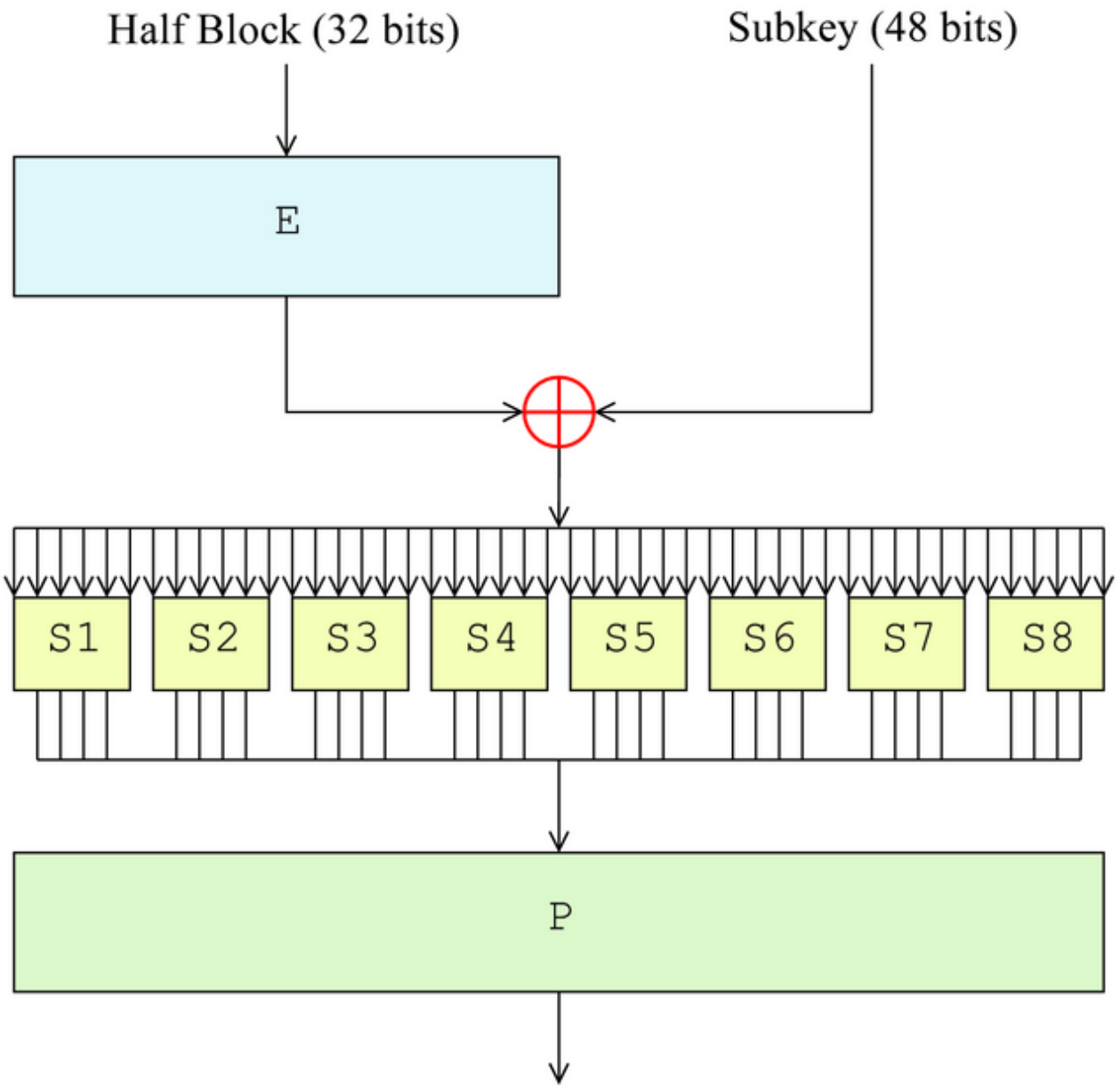
DES

Data Encryption Standard

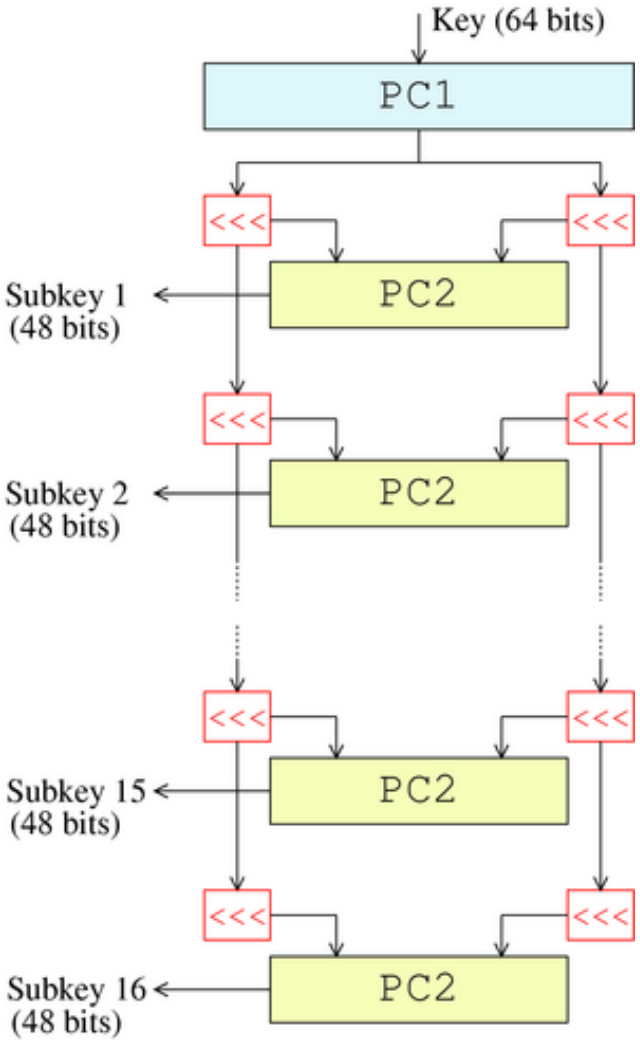


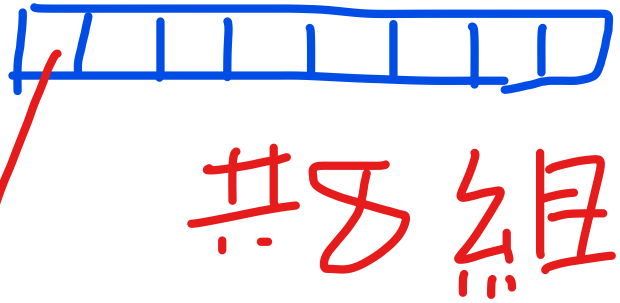
The block size is 64 bits.

The Feistel Function



DES Key Schedule





- DES actually has a key length of 64 bits, however 8 bits are used for parity, therefore the effective key length is 56 bits.

S-Boxes

S_1																
	x0000x	**x0001x**	**x0010x**	**x0011x**	**x0100x**	**x0101x**	**x0110x**	**x0111x**	**x1000x**	**x1001x**	**x1010x**	**x1011x**	**x1100x**	**x1101x**	**x1110x**	**x1111x**
0yyyy0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0yyyy1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
1yyyy0	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
1yyyy1	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
S_2																
	x0000x	**x0001x**	**x0010x**	**x0011x**	**x0100x**	**x0101x**	**x0110x**	**x0111x**	**x1000x**	**x1001x**	**x1010x**	**x1011x**	**x1100x**	**x1101x**	**x1110x**	**x1111x**
0yyyy0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
0yyyy1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
1yyyy0	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
1yyyy1	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

What if S-Box is Bad ...

- What is a bad S-Box?

What if S-Box is Bad ...

- What is a bad S-Box?
- Suppose S-Box is

$$S(x_1, x_2, x_3, x_4, x_5, x_6) = (x_2 \oplus x_3, x_1 \oplus x_4 \oplus x_5, x_1 \oplus x_6, x_2 \oplus x_3 \oplus x_6)$$

$$S(\overrightarrow{x}) = B \cdot \overrightarrow{x}$$

The output will be also linear combination.

Brute Force Attack

- Exhaustive Search Attack.
- How long do you need to search all 2^{56} possible keys?
- Quiz:
  Do you think it is very easy to get the plaintext and ciphertext pair??

Cracking DES

- Jun. 1997. The DESCHALL Project breaks a message encrypted with DES for the first time in public.
- Jul. 1998. The EFF's DES cracker (Deep Crack) breaks a DES key in 56 hours.
- Jan. 1999. Together, Deep Crack and distributed.net break a DES key in 22 hours and 15 minutes.
- Apr. 2006. The Universities of Bochum and Kiel, breaks DES in 9 days at a $10,000 hardware cost.

My Opinion

Is DES secure enough? **No**.

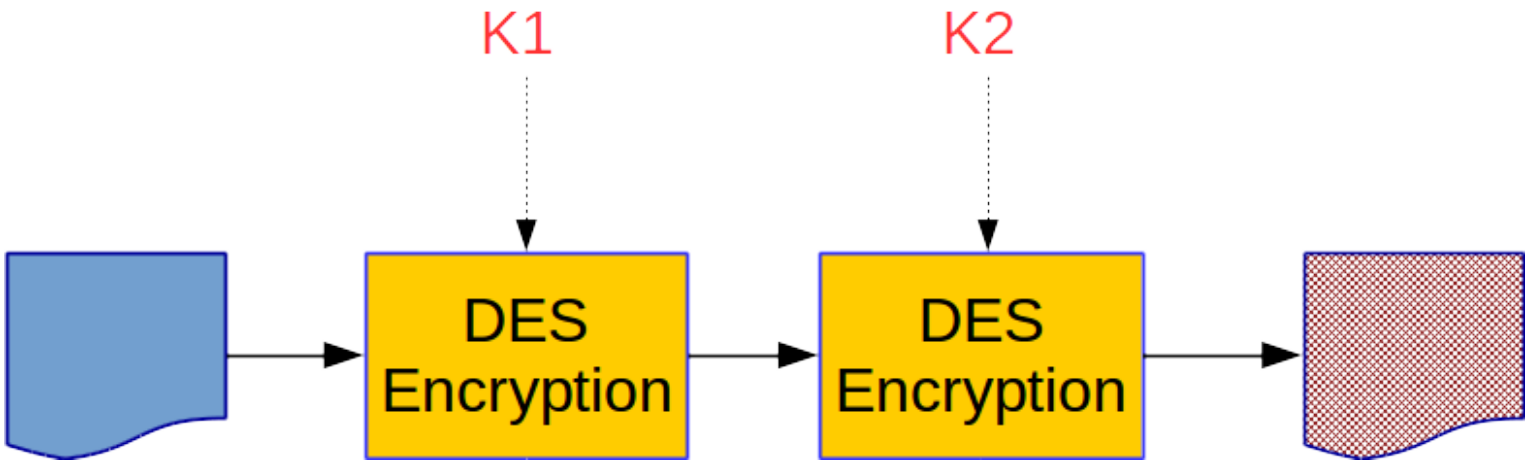
Is DES cracked? **No**.

DES is not safe because the computation power is over its design instead of DES has been cracked.

Triple DES

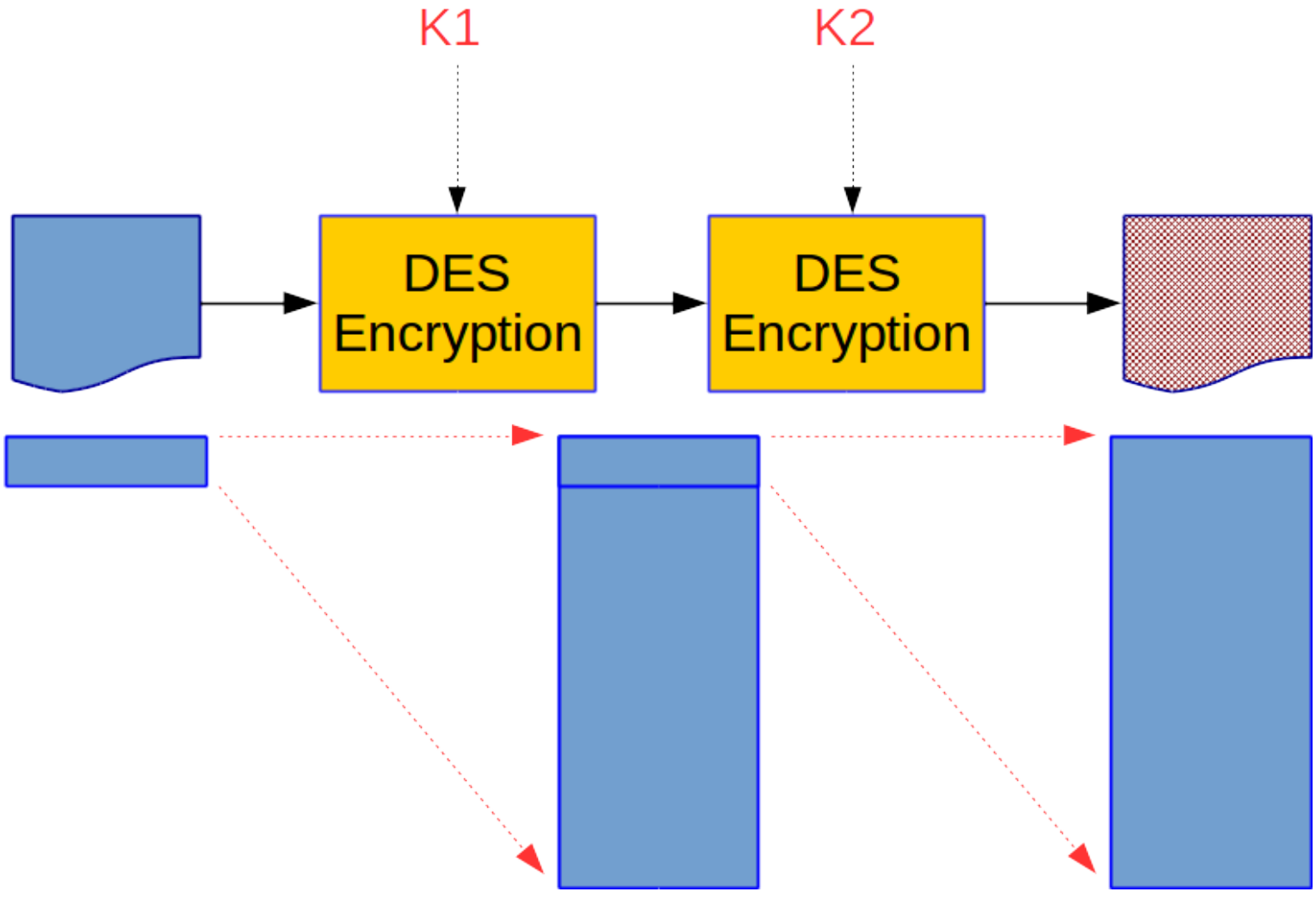
Increase DES Keys

- DES is not secure enough because of short keys.
- How about double the key size? Like the figure below so that key size will be 112 bits.



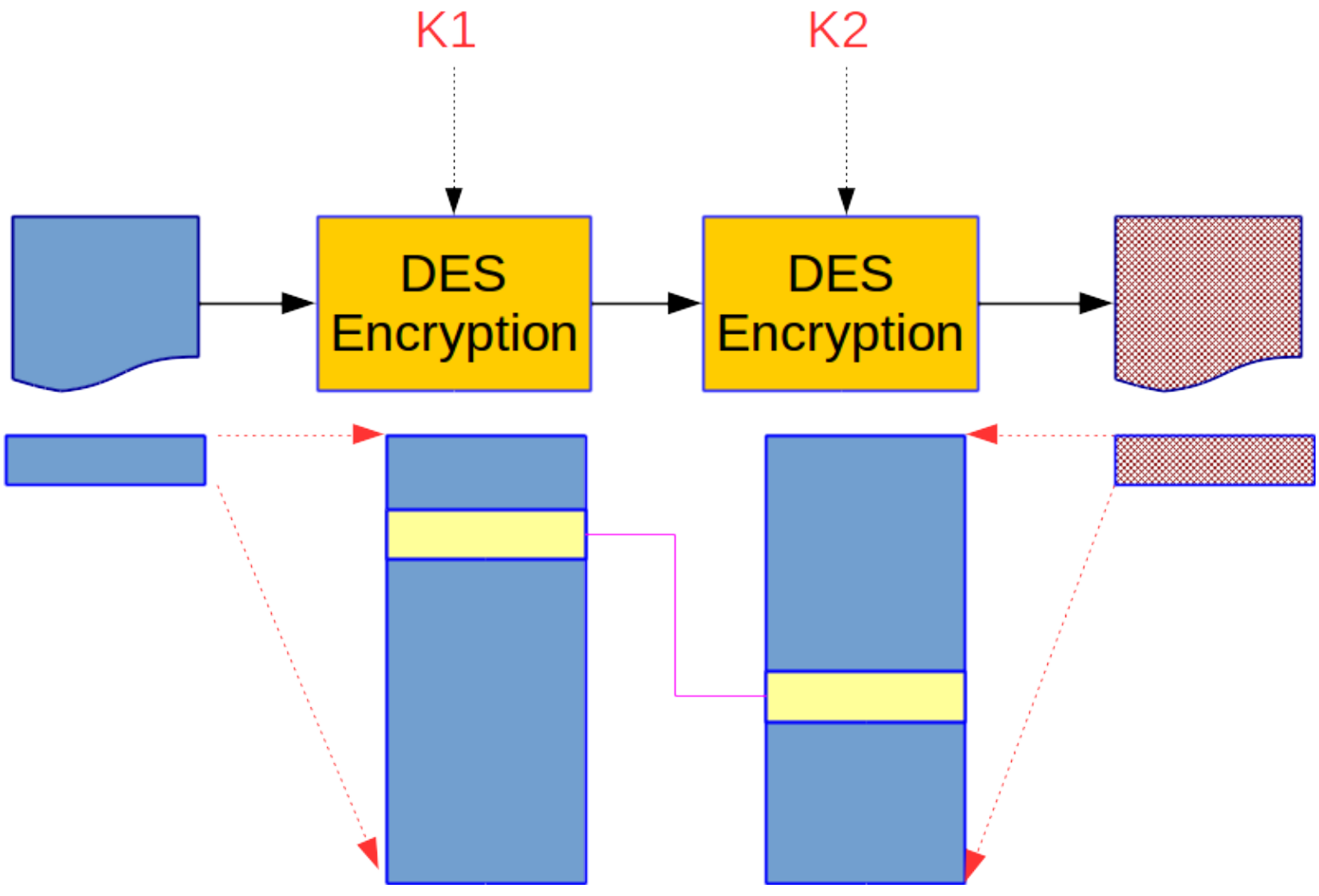
Unfortunately, it does not work. Why?

Trivial Thinking



Possible keys are $2^{56} \times 2^{56} = 2^{112}$.

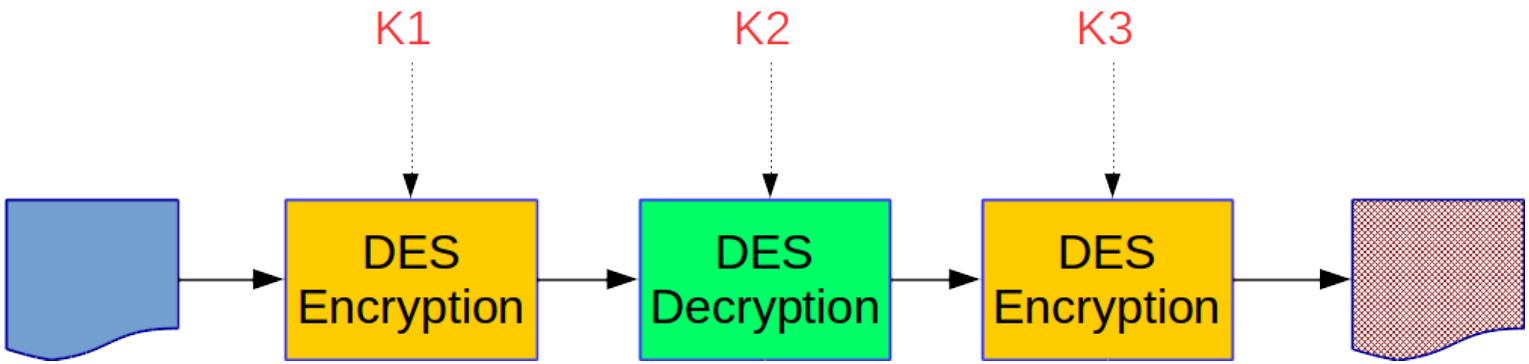
Meet in the Middle Attack



Only $2 \times 2^{56} = 2^{57}$.

Triple DES

- Meet in the middle attack still works.
- So the effective key size is 112 bits instead of 168 bits.



Quiz

Why not three encryption blocks?

AES

DES is Not Secure Anymore ...

- 1997: NIST publishes request for proposal.
- 1998: 15 submissions.
- 1999: NIST chooses 5 finalists.
- 2000: NIST chooses Rijndael as AES.

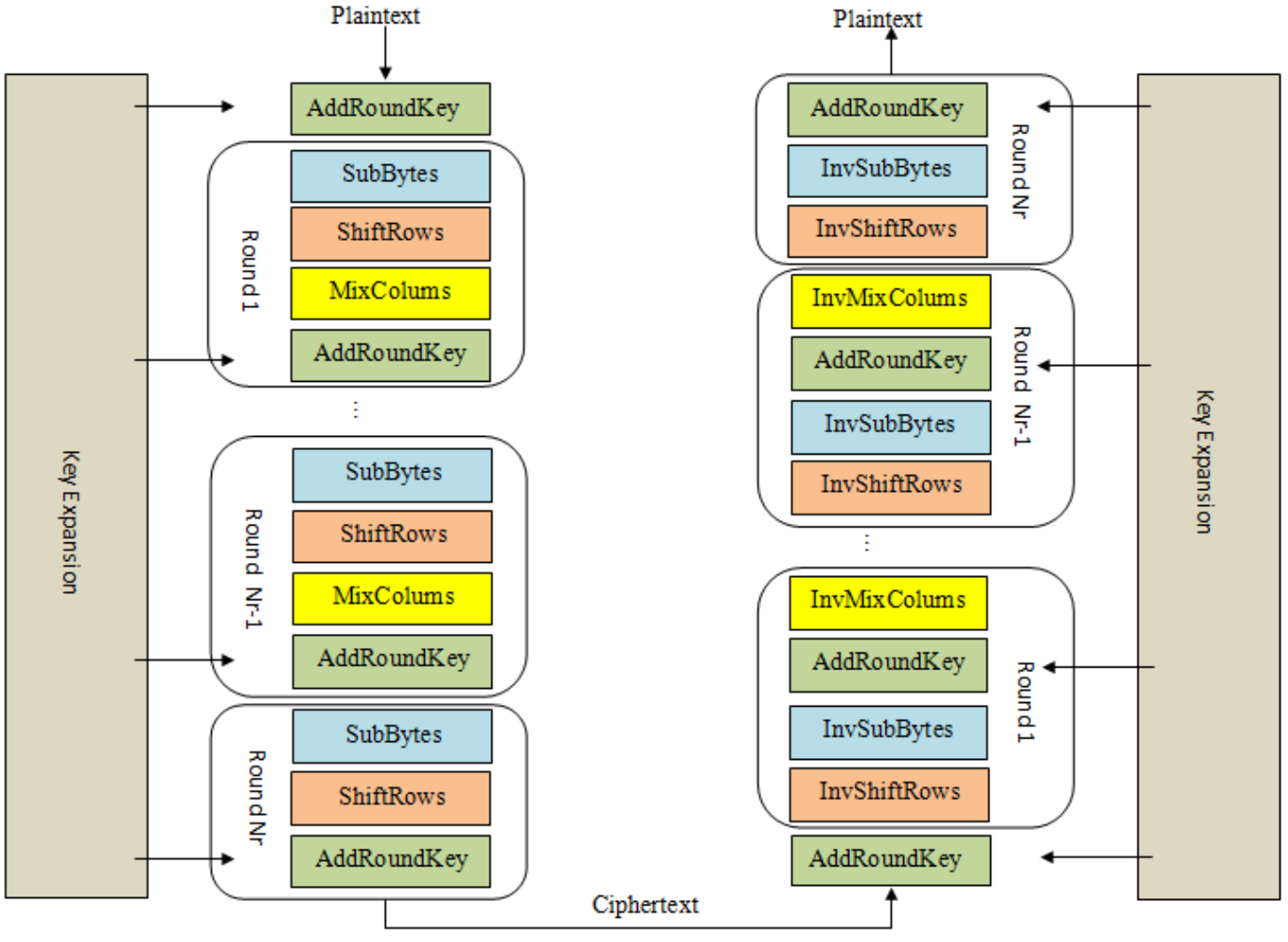
Key Size: 128, 192, 256 bits.

Block Size: 128 bits.

Candidates

- CAST-256 Entrust (CA)
- Crypton Future Systems (KR)
- E2 NTT (JP)
- Frog TecApro (CR)
- Magenta Deutsche Telekom (DE)
- **Mars IBM (USA)**
- **RC6 RSA (USA)**
- SAFER+ Cylink (USA)
- **Twofish Counterpane (USA)**
- DEAL Outerbridge, Knudsen (USA–DK)
- DFC ENS-CNRS (FR)
- HPC Schroeppel (USA)
- LOKI97 Brown et al. (AU)
- **Rijndael Daemen and Rijmen (BE)**
- **Serpent Anderson, Biham, Knudsen (UK)**

Advanced Encryption Standard



I will Not Talk Too Much in Detail

- **Uniform** and **parallel** round transformation, composed of:
  - Byte substitution.
  - Shift rows.
  - Mix columns.
  - Round key addition.
- **Sequential and lightweight key schedule**.
- Mathematically quite **sophisticated**.
- **No arithmetic operations**.

All you need to know is **AES is a secure PRP**.

Before We End Up This Topic

- This course is called **Information Security** instead of **Cryptography**.
- You can skip some details about how PRP works, but you need to know how to use these PRPs, like 3DES and AES.
- I hope one day I can open a course called Applied Cryptography ...

How to Use Block Ciphers

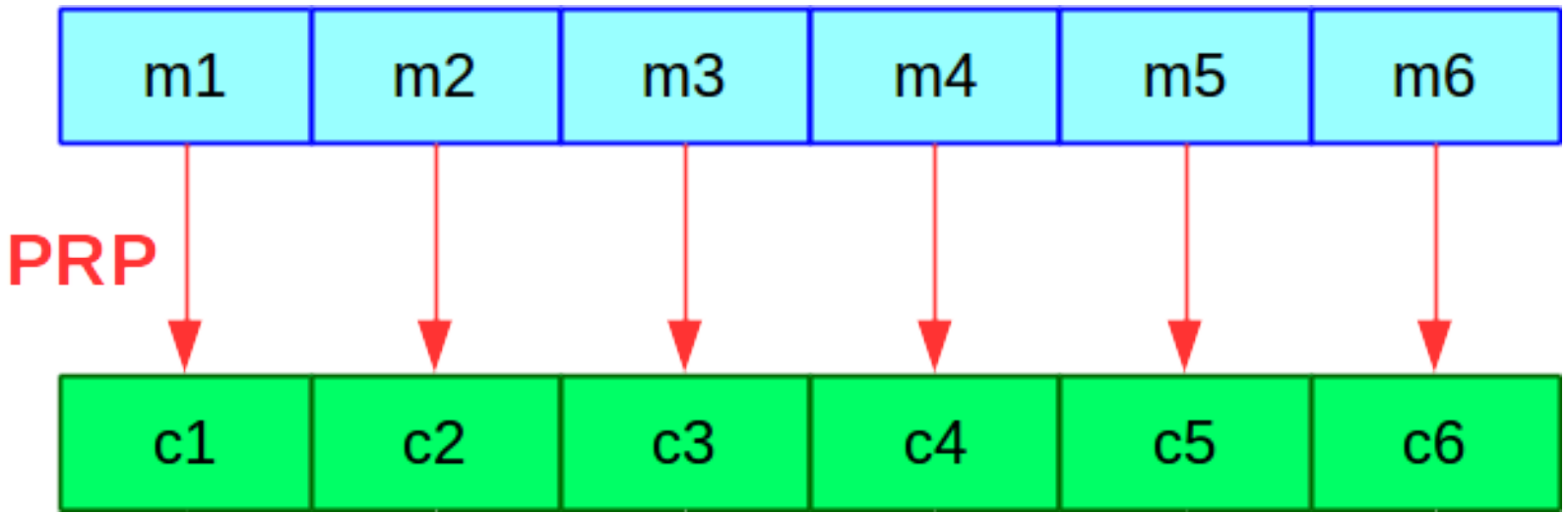
Now We Have a Block Cipher

1. 3DES
   - Block Size: 64 bits.
   - Key Size: 168 bits. (only 112 bits effective)
2. AES
   - Block Size: 128 bits.
   - Key Size: 128, 192, 256 bits.

However, a file size is often larger than a block size.

Trivial Solution: ECB

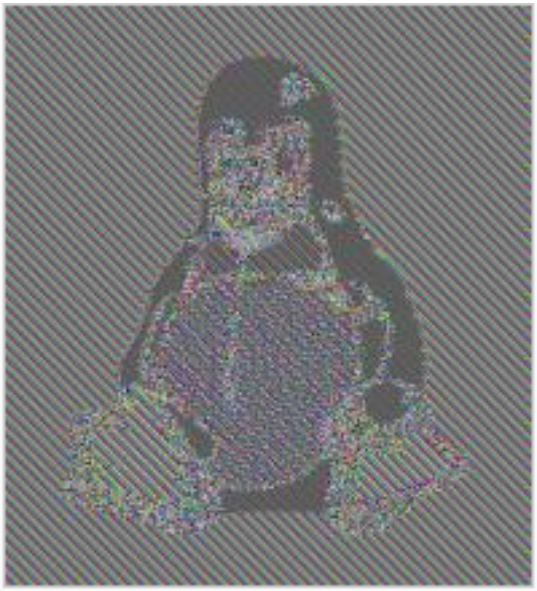
Electronic Code Book (ECB)



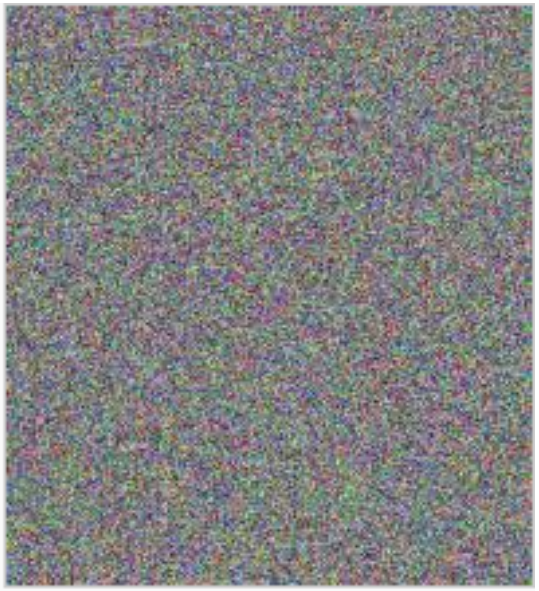
This mode has a big problem. Why?

AES with ECB

Original image



Encrypted using ECB mode



Modes other than ECB result in pseudo-randomness

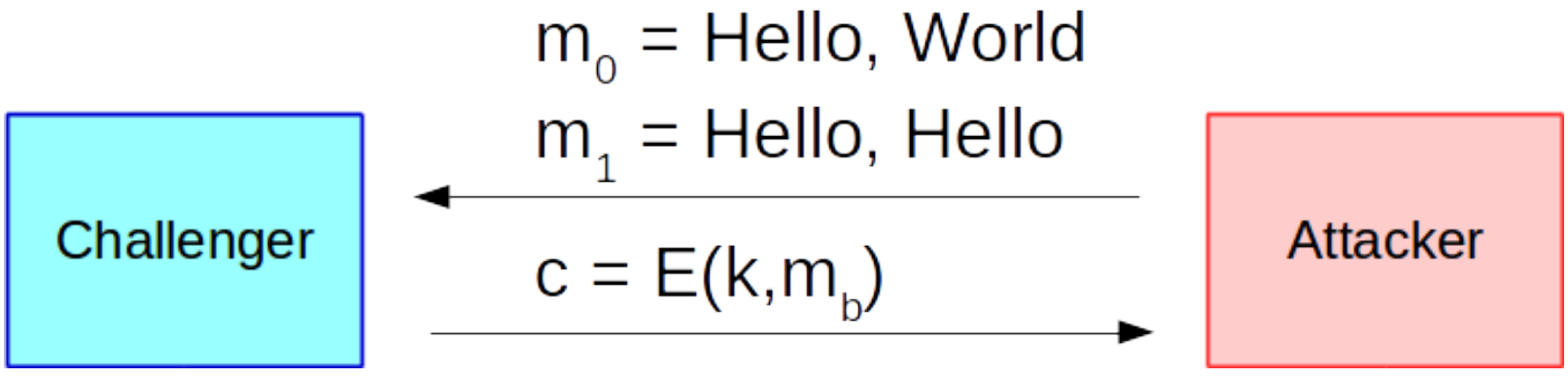
ECB is Not Semantically Secure

ECB is not semantically secure if the message has multiple blocks.

Can you show how to break ECB?

ECB is Not Semantically Secure

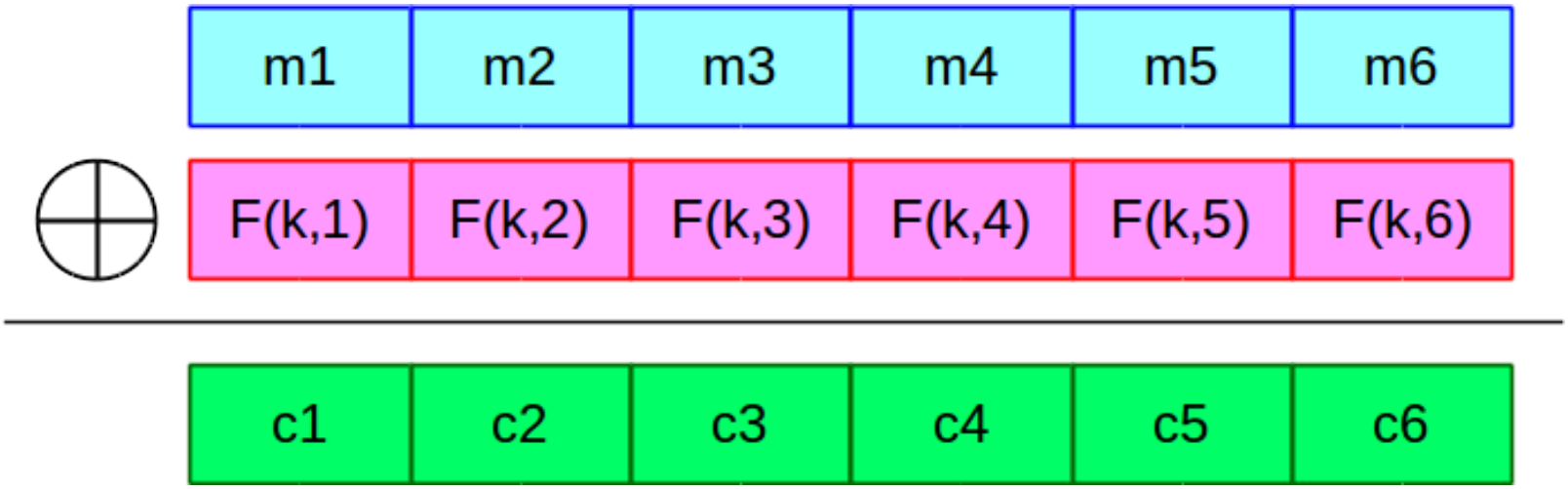
ECB is not semantically secure if the message has multiple blocks.



The probability that the attacker wins this game is?

Solution: Add Counters

Suppose there is a PRP function F.



Look, you can build a stream cipher from a block cipher (PRP).

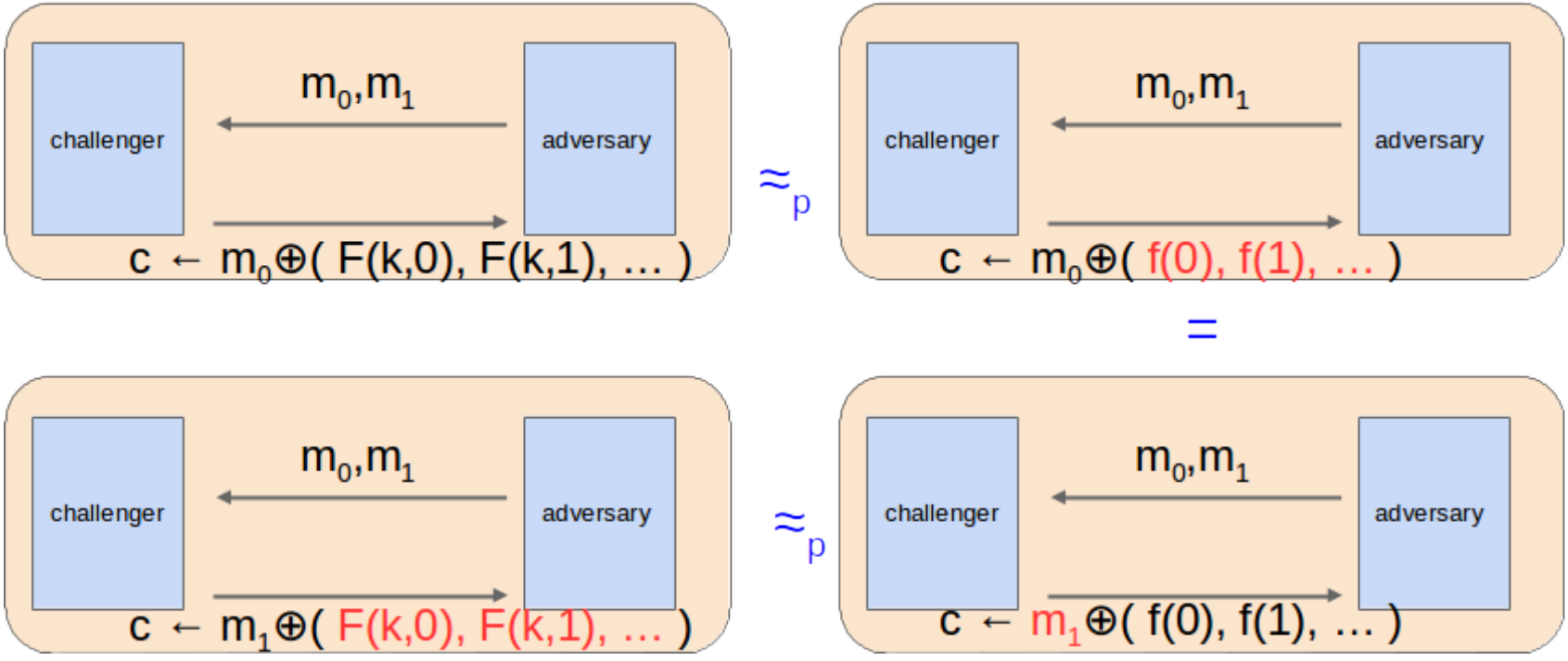
Deterministic Counter Mode Security

Theorem

If F is a secure PRF, then E_{DETCTR} is semantic secure. For any efficient adversary $\mathcal{A}$ attacking E_{DETCTR}, there exists an efficient PRF adversary $\mathcal{B}$ such that:

$$\mathsf{Adv}_{\mathsf{SS}}[\mathcal{A}, E_{\mathsf{DETCTR}}] = 2 \times \mathsf{Adv}_{\mathsf{PRF}}[\mathcal{B}, F]$$

Proof


challenger
m_0, m_1
adversary
$c \leftarrow m_0 \oplus (F(k,0), F(k,1), \ldots)$
$\approx_p$
challenger
m_0, m_1
adversary
$c \leftarrow m_0 \oplus (f(0), f(1), \ldots)$
=
challenger
m_0, m_1
adversary
$c \leftarrow m_1 \oplus (F(k,0), F(k,1), \ldots)$
$\approx_p$
challenger
m_0, m_1
adversary
$c \leftarrow m_1 \oplus (f(0), f(1), \ldots)$

Quiz

When using one key many times, counter mode does not work.

Why?

Quiz

When using one key many times, counter mode does not work.

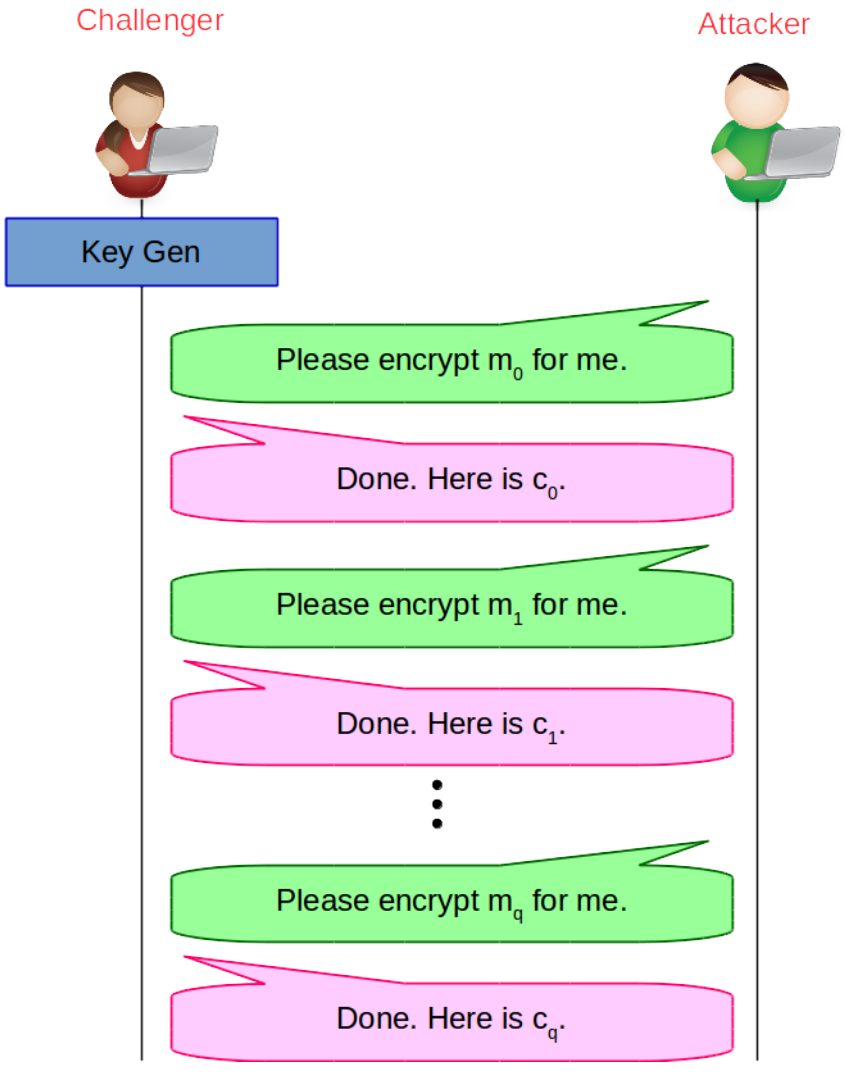
Why?

Because each counter start from 0 for many files.

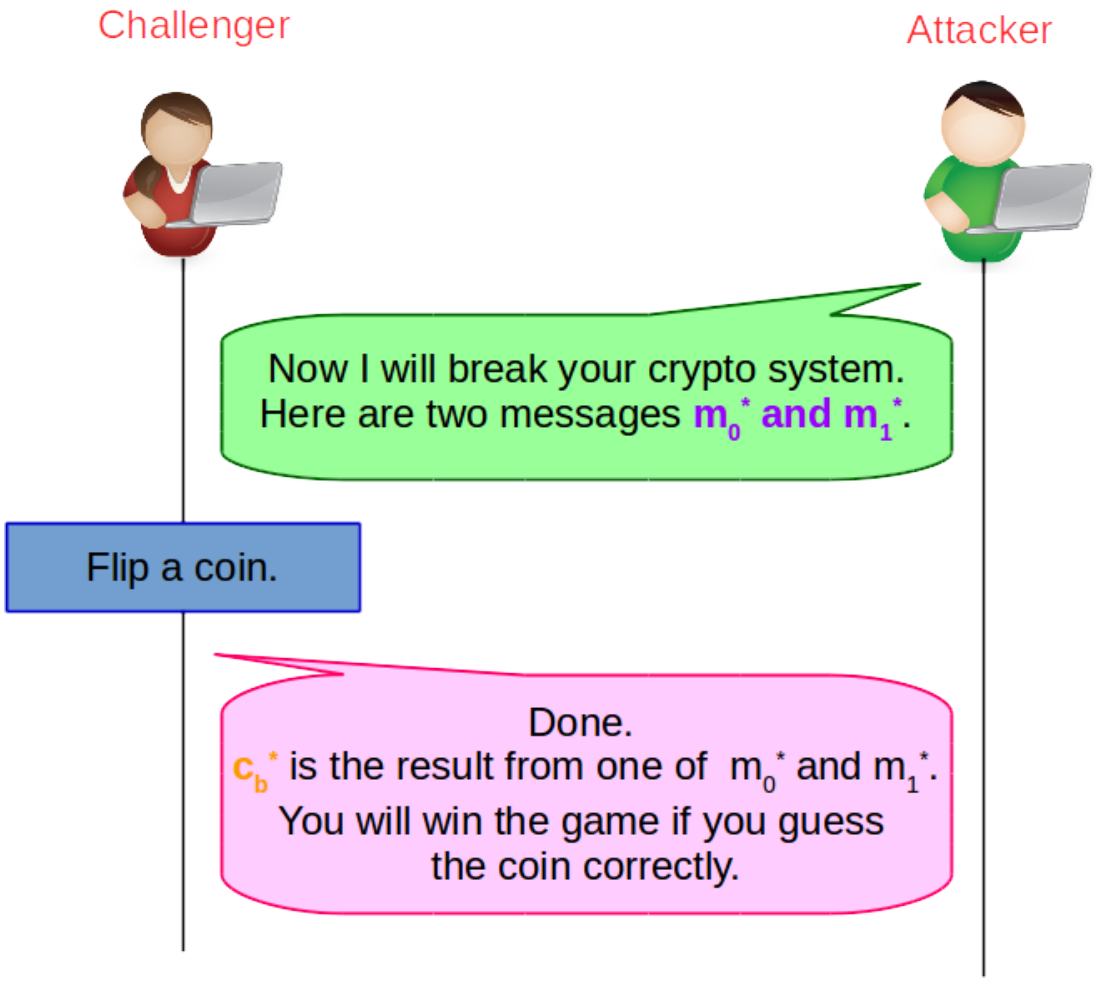
Chosen Plaintext Attack

- Adversary can obtain the encryption of arbitrary messages of his choice.
- Actually, it is semantic security for many-times key.

CPA Game Model 1/2



CPA Game Model 2/2



CPA-Security

- To achieve CPA-security, the encryption method must generates different outputs for a given message multiple times.
- This implies we need to **randomize** the encryption.

How to Use Block Ciphers: Many-Times Key

How to Randomize the Ciphertext?

Your idea?

How to Randomize the Ciphertext?

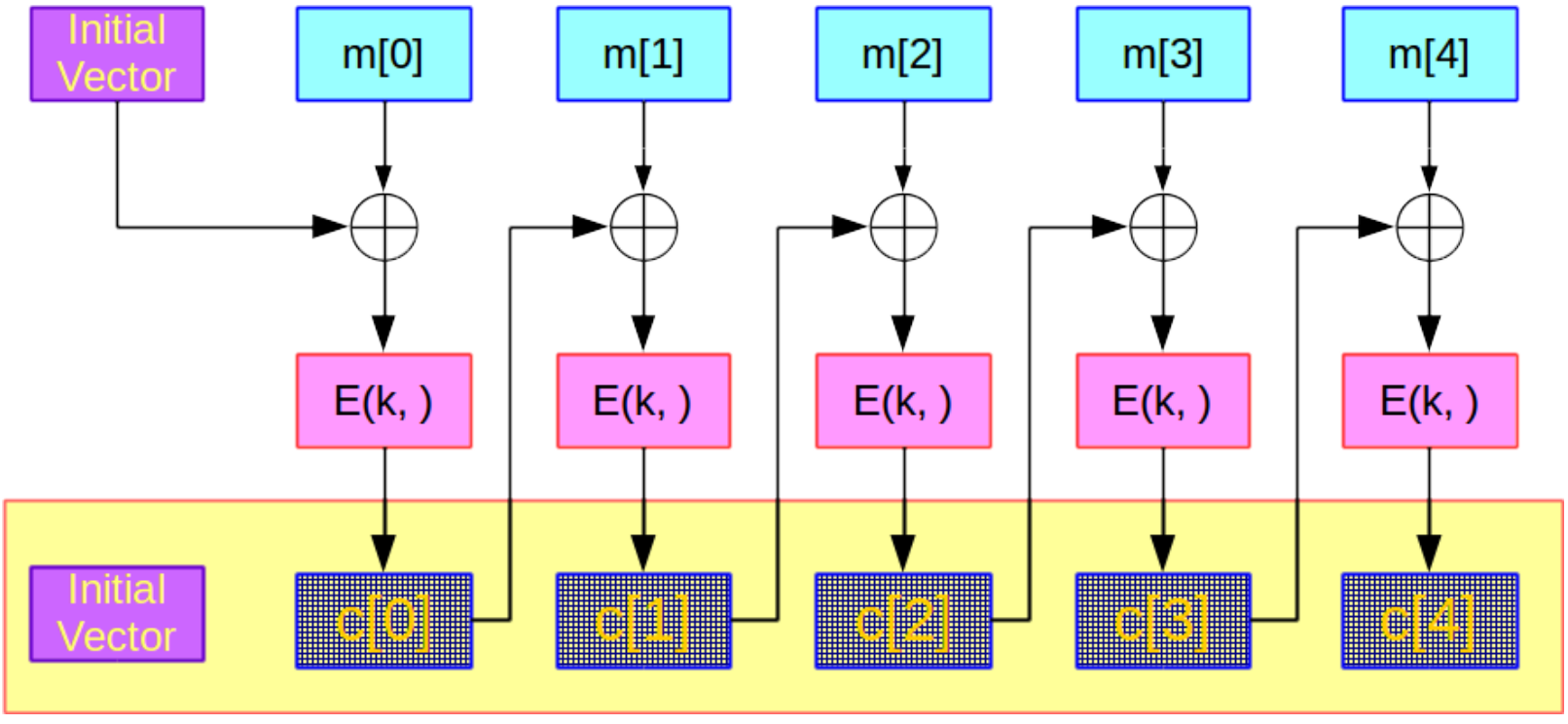
Your idea?

Add a random number in the content.

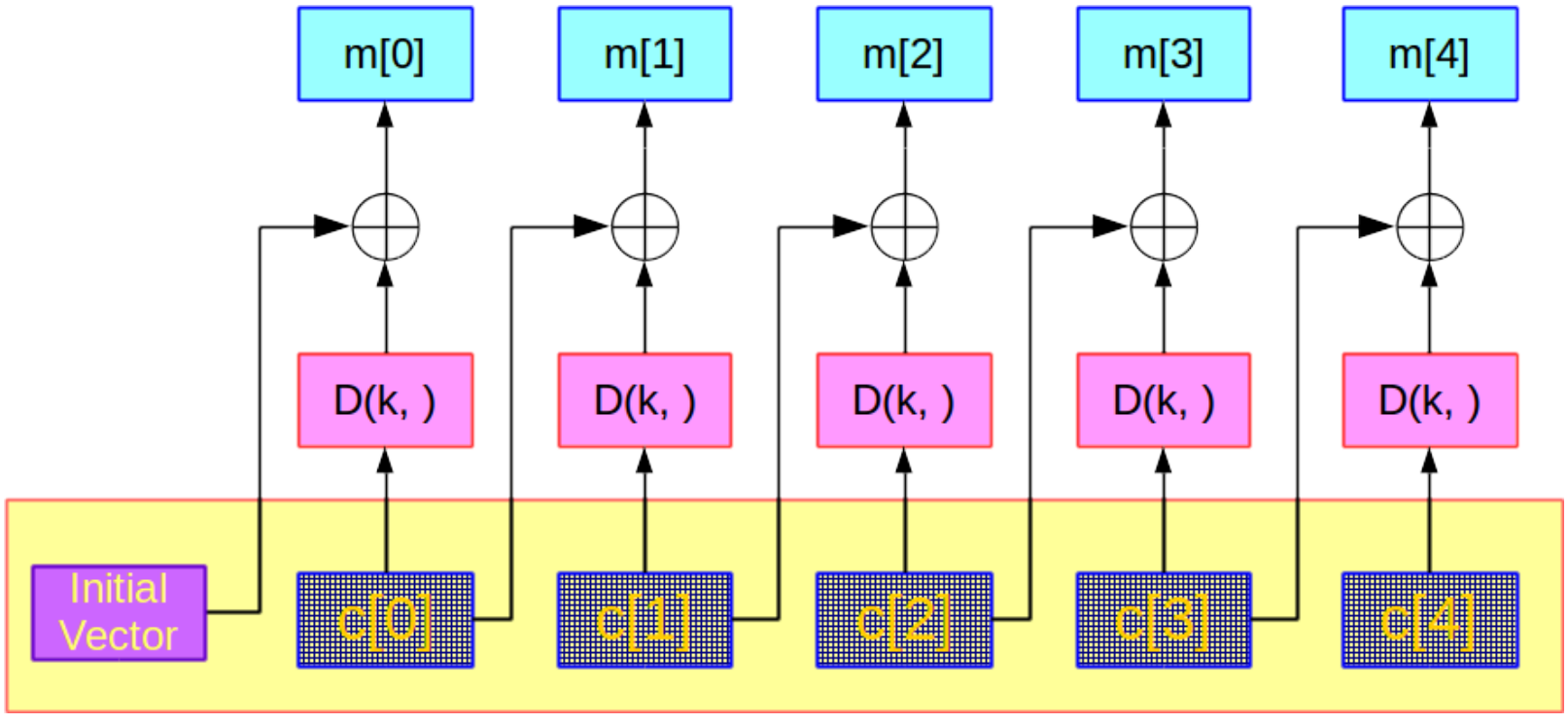
Other Operation Modes

1. CBC: Cipher Block Chaining.
2. CTR: Counter.

CBC Mode 1/2


Initial Vector
m[0]
m[1]
m[2]
m[3]
m[4]
E(k,)
E(k,)
E(k,)
E(k,)
E(k,)
Initial Vector
c[0]
c[1]
c[2]
c[3]
c[4]

CBC Mode 2/2



CBC Mode is Secure

Theorem

For any $L > 0$, if E is a secure PRP over (K, X), E_{CBC} is CPA-secure over (K, X_L, X_{L+1}).

$$\text{Adv}_{\text{CPA}}[\mathcal{A}, E_{\text{CBC}}] \leq 2 \times \text{Adv}_{\text{PRP}}[\mathcal{B}, E] + \frac{2q^2L^2}{|X|}.$$

- q: # messages encrypted with k.
- L: length of max message.

Example

Suppose we want $\mathrm{Adv}_{\mathrm{CBC}}$ to be less than $\frac{1}{2^{32}}$.

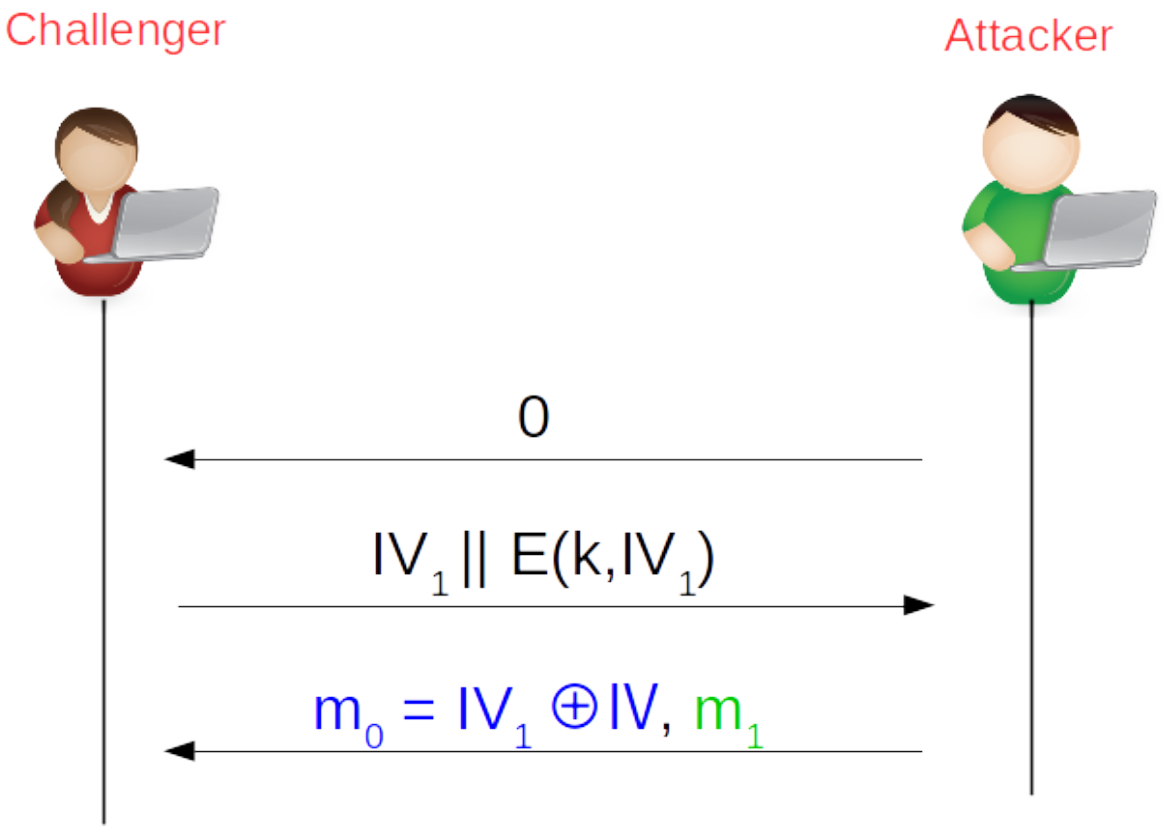
- 3-DES:
  - $|X| = 2^{64}$.
  - $ql < 2^{16}$.
- AES:
  - $|X| = 2^{128}$.
  - $ql < 2^{48}$.

Quiz

Suppose IV is **predictable**, what will happen?

Quiz

Suppose IV is **predictable**, what will happen?



OpenSSL API

```
void AES_cbc_encrypt    (
    const unsigned char *     in,
    unsigned char *     out,
    size_t      length,
    const AES_KEY *     key,
    unsigned char *     ivec,
    const int       enc
)
```

Quiz

How about the last block??

Quiz

How about the last block??

Padding issue. Pad all zeros in the last block.

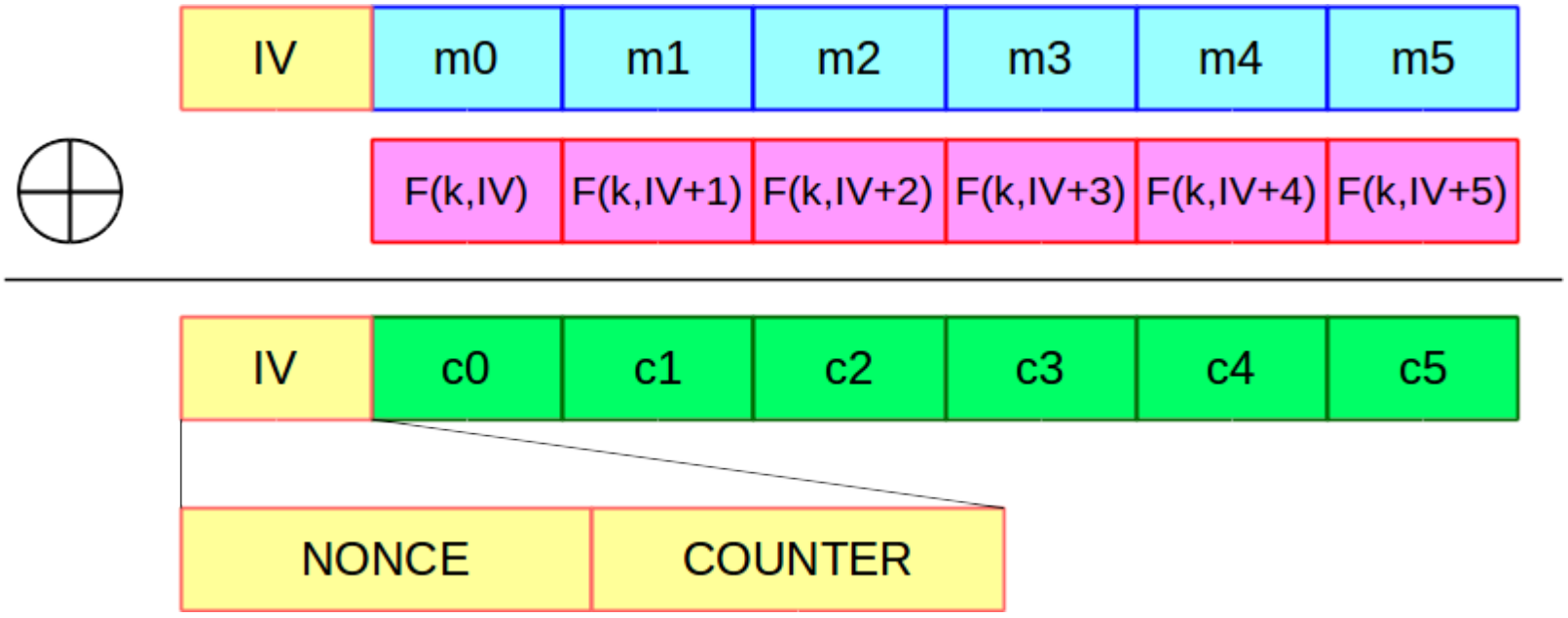
Quiz

How about the last block??

Padding issue. Pad all zeros in the last block.

How to distinguish 0 between real message and padding?

CTR Mode


IV
m0
m1
m2
m3
m4
m5
F(k,IV)
F(k,IV+1)
F(k,IV+2)
F(k,IV+3)
F(k,IV+4)
F(k,IV+5)
IV
c0
c1
c2
c3
c4
c5
NONCE
COUNTER

CTR Mode is Secure

Theorem

For any $L > 0$, if E is a secure PRP over (K, X), E_{CTR} is CPA-secure over (K, X_L, X_{L+1}).

$$\mathsf{Adv}_{\mathsf{CPA}}[\mathcal{A}, E_{\mathsf{CTR}}] \leq 2 \times \mathsf{Adv}_{\mathsf{PRP}}[\mathcal{B}, E] + \frac{2q^2 L}{|X|}.$$

- q: # messages encrypted with k.
- L: length of max message.

So, CTR mode is better than CBC.

Appendix: Reminder

Never Implement Crypto Cipher

- In this class, I have introduced some block ciphers.
- I know you are good at programming ···but please do not implement them yourselves.
  - If you want to practice or for fun, that is OK. But do not use them in the serious scenario.
  - **Why?**