Network Information Security

Lecture six: mode of operation

Rachel yuan
2019.10

1

Try to compare DES and AES

2

Factors	AES	DES
Cipher type		
Key length		
Block size		
Possible keys		
Security		
S-Box		
Template		
Reversibility		
Number of Rounds		
Implementation		
Developed		
Confusion in each round		
Diffusion in each round		

3

How to encrypt long messages using block cipher?

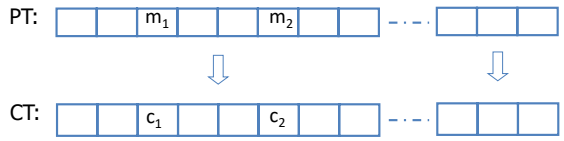
4

A mode of operation describes how to repeatedly apply a cipher's single-block operation to securely transform amounts of data larger than a block

5

A straightforward method

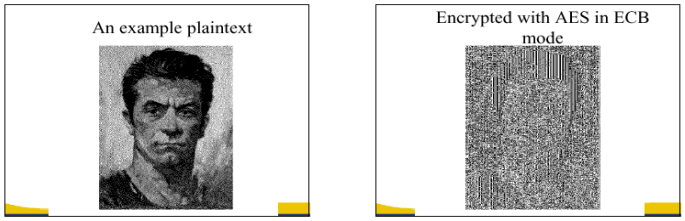
- Electronic Code Book (ECB):



- Problem:
  - if m1=m2 then c1=c2

6

In pictures

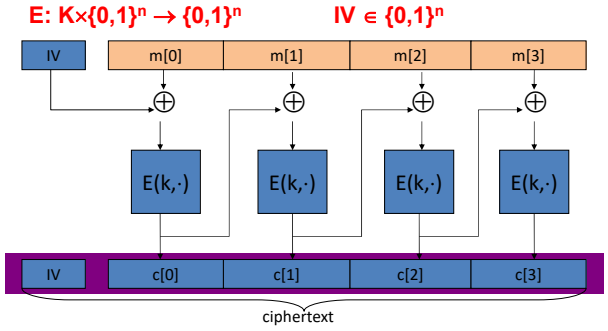


(courtesy B. Preneel)

7

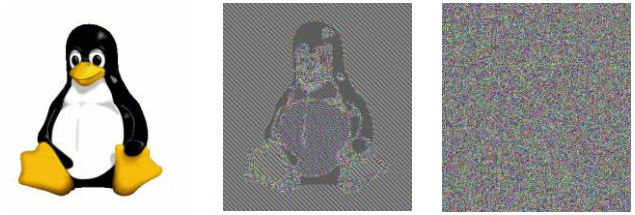
Construction 1: CBC with random IV

Let (E,D) be a block cipher. $E_{CBC}(k,m)$: choose **random** IV∈X and do:



CBC: cipher block chaining

8



9

CBC properties

- Parallel processing possible?
- Do errors propagate?

10

$c_i = E(m_i \oplus c_{i-1}, k)$, for i = 1, 2,…

$c_0 = E(m_0 \oplus IV, k)$

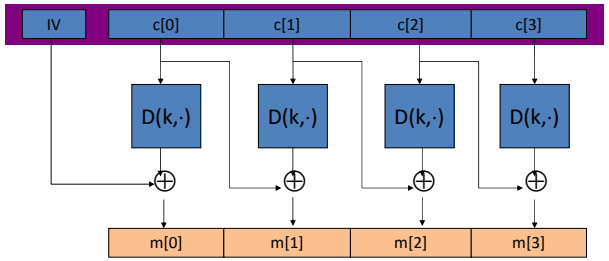
$m_i = D(c_i, k) \oplus c_{i-1}$, for i = 1, 2,…

$m_0 = D(c_0, k) \oplus IV$

11

Decryption circuit

In symbols: $c[0] = E(k, IV \oplus m[0])$ ⇒ $m[0] = D(k, c[0]) \oplus IV$

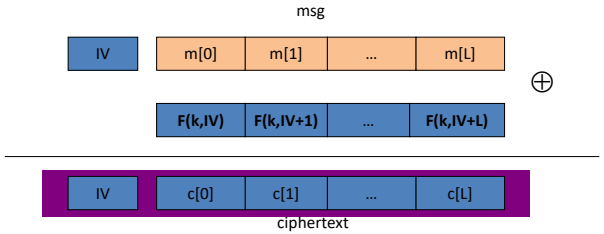


12

Construction 2: rand ctr-mode

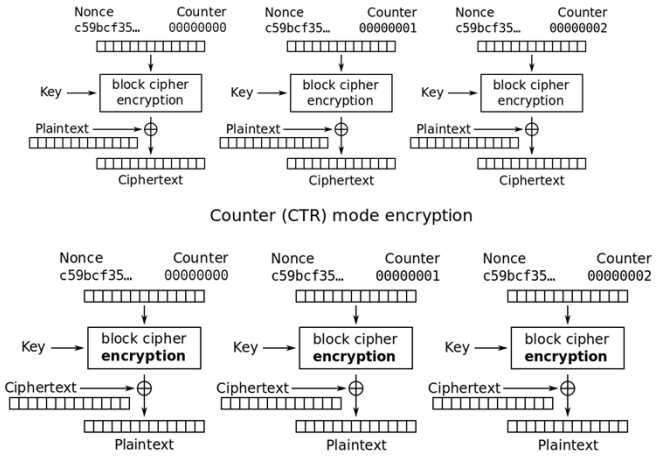
Let F: K × {0,1}^{n} ⟶ {0,1}^{n} be a secure block cipher.

E(k,m): choose a random IV ∈ {0,1}^{n} and do:



note: parallelizable (unlike CBC)

13



14

$c_i = m_i \oplus E(IV + i, k)$, for i = 0, 1, 2, …

$m_i = c_i \oplus E(IV + i, k)$, for i = 0, 1, 2, …

15

Along with CBC, CTR mode is one of two block cipher modes recommended by Niels Ferguson and Bruce Schneier.

16