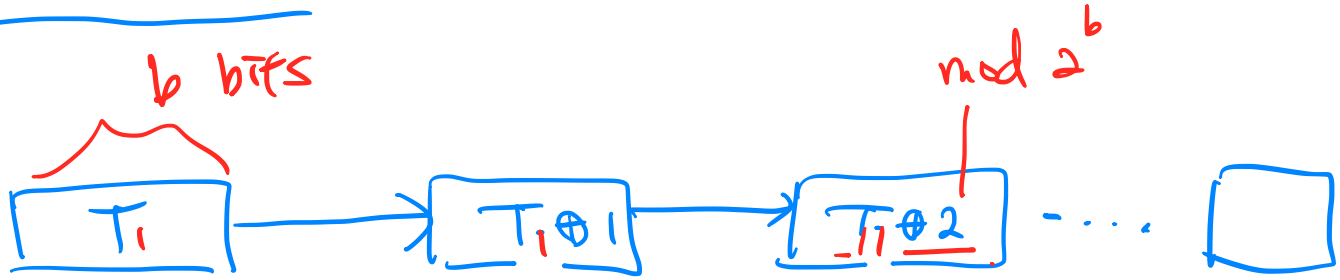
Counter mode



A counter equal to the plaintext block size is used.

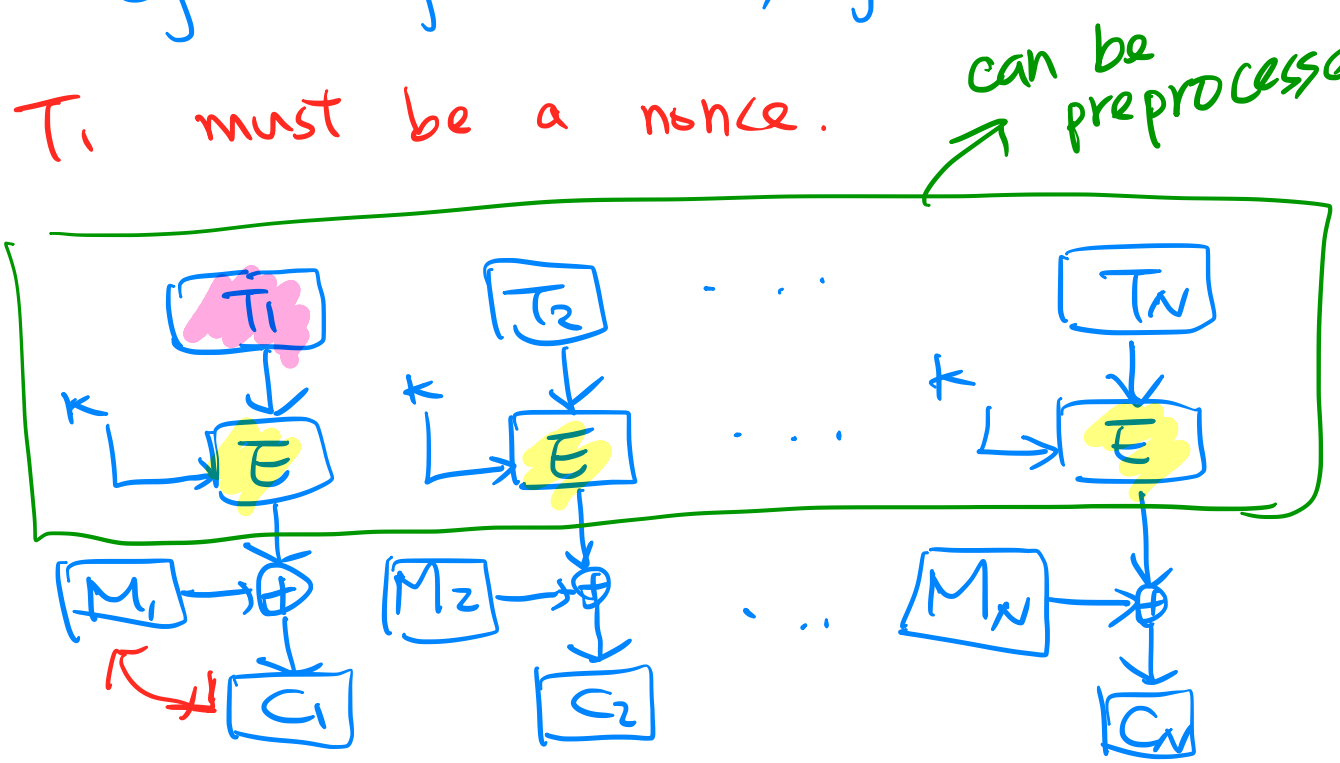
T_j : b bits.

$T_{j+1} = T_j + 1 \pmod{2^b}$.

$C_j = M_j \oplus E(k, T_j)$

T_1 must be a nonce.

can be preprocessed.



preprocessing : the execution of the underlying encryption algorithm does not depend on input of the plaintext / ciphertext.

Introduction to Cryptography and Information Security
UEE4611, Spring Semester 2020

Ching-Yi Lai
Institute of Communications Engineering
National Chiao Tung University

Chapter 8: Block Cipher Operation

- Principles of Pseudorandom Number Generation
- Pseudorandom Number Generators
- Pseudorandom Number Generation Using a Block Cipher
- Stream Ciphers
- RC4
- True Random Number Generators

Pseudorandom number generators (PRNGs).
(deterministic random bit generators)

Two criterions.

1. uniform distribution.
   The frequency of occurence of ones and zeros should be approximately equal.

2. Independence
   no subsequence in the sequance can be inferred from the others.

Examples: (Tests)

1. Frequency test: whether 1s or 0s appear approximately the same time.

2. Run test: a run is an uninterrupted sequence of identical bits

   ex $\underbrace{11111}_{5}$, $\underbrace{0000}_{4}$

Linear Congruential Generators

m : the modulus $m > 0$.

a : the multiplier $0 < a < m$

c : the increment $0 \le c < m$.

X_0 : the starting value or seed $0 \le X_0 < m$.

$$X_{n+1} = (aX_n + c) \bmod m.$$

The values of a, c, are critical.

Ex. $a = c = 1$. $\{x_n\} = \{x_0, x_0+1, x_0+2, \cdots\}$

$a = 7$. $c = 0$, $m = 32$.

$\{x_n\} = \{7, 17, 23, 1, 7, 17, \cdots\}$

m: very large . $\sim 2^{31}$ (32 bits)

T_1 : full-period generating. $0, \ldots, m-1$ before repeating.

T_2 : generated sequence appear random.

T_3 : efficiently implemented.

If m is prime & $c=0$, for certain values of a, the period of the generating function is $m-1$ with only the value 0 missing.

$\mathbb{Z}_p \setminus \{0\}$. cyclic group.

$\{a^0, a^1, \ldots, a^{m-1}\}$.

Ex. $m = 2^{31}-1$ (a prime).

$a = 7^5 = 16807$.

Cryptanalysis:

① If a, c, m are known