HUST

TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI

HANOI UNIVERSITY OF SCIENCE AND TECHNOLOGY

ONE LOVE. ONE FUTURE.

TRƯỜNG ĐẠI HỌC
BÁCH KHOA HÀ NỘI
HANOI UNIVERSITY
OF SCIENCE AND TECHNOLOGY

LÝ THUYẾT MẬT MÃ

Cryptography Theory

ET3310

PGS. TS. Đỗ Trọng Tuấn
Trường Điện - Điện tử * Đại học Bách Khoa Hà Nội

ONE LOVE. ONE FUTURE.

Stream Cipher

1. Introduction
2. Stream Cipher Structure
3. RC4 Stream Cipher

1 Introduction to Stream Cipher

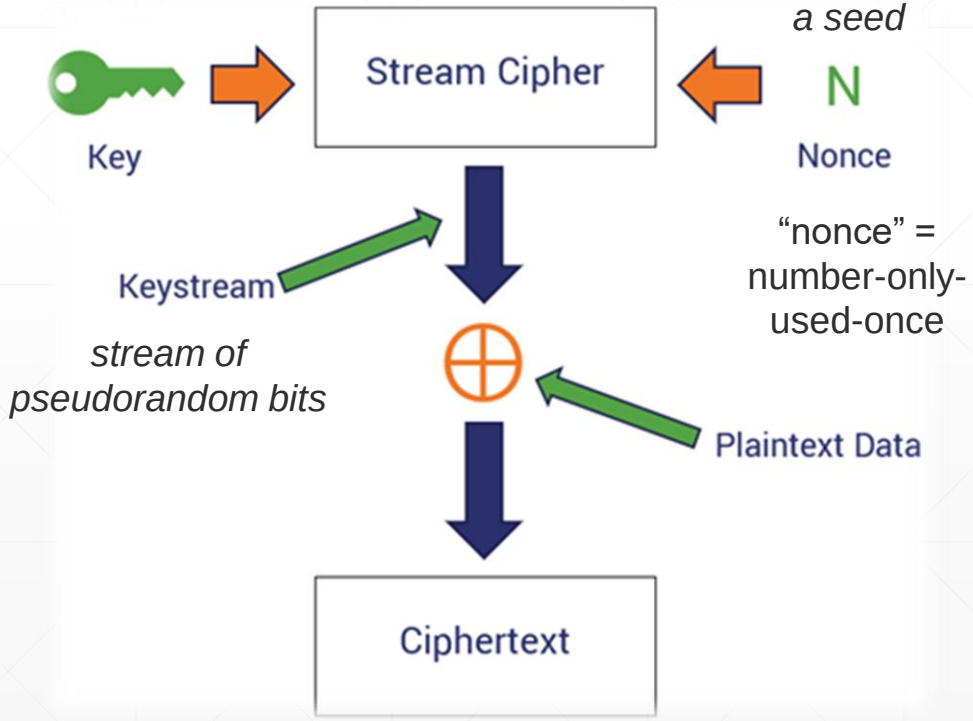
- In stream cipher, one byte is encrypted at a time while in block cipher N bits are encrypted at a time.
- *Benefit : usually simpler & faster*

the water/data flow

XOR Operations in Cryptography

Bit1 ⊕ Bit2 = Output.

Input Bit1	Input Bit2	Output
0	0	0
0	1	1
1	0	1
1	1	0



encrypts data one bit at a time

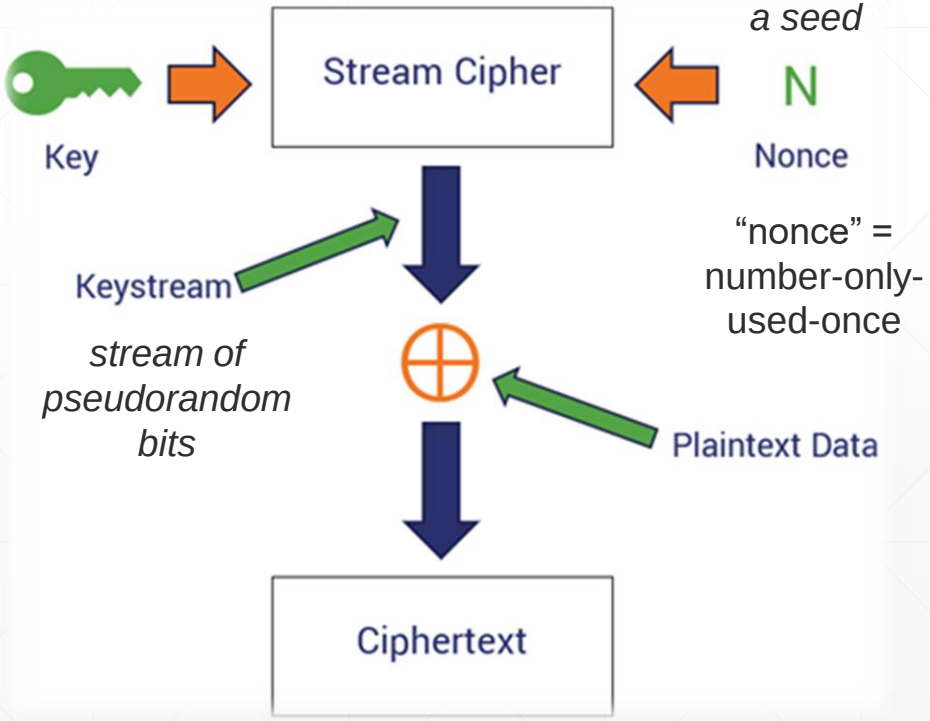
1 Introduction to Stream Cipher

- In stream cipher, one byte is encrypted at a time while in block cipher N bits are encrypted at a time.
- *Benefit : usually simpler & faster*

the water/data flow

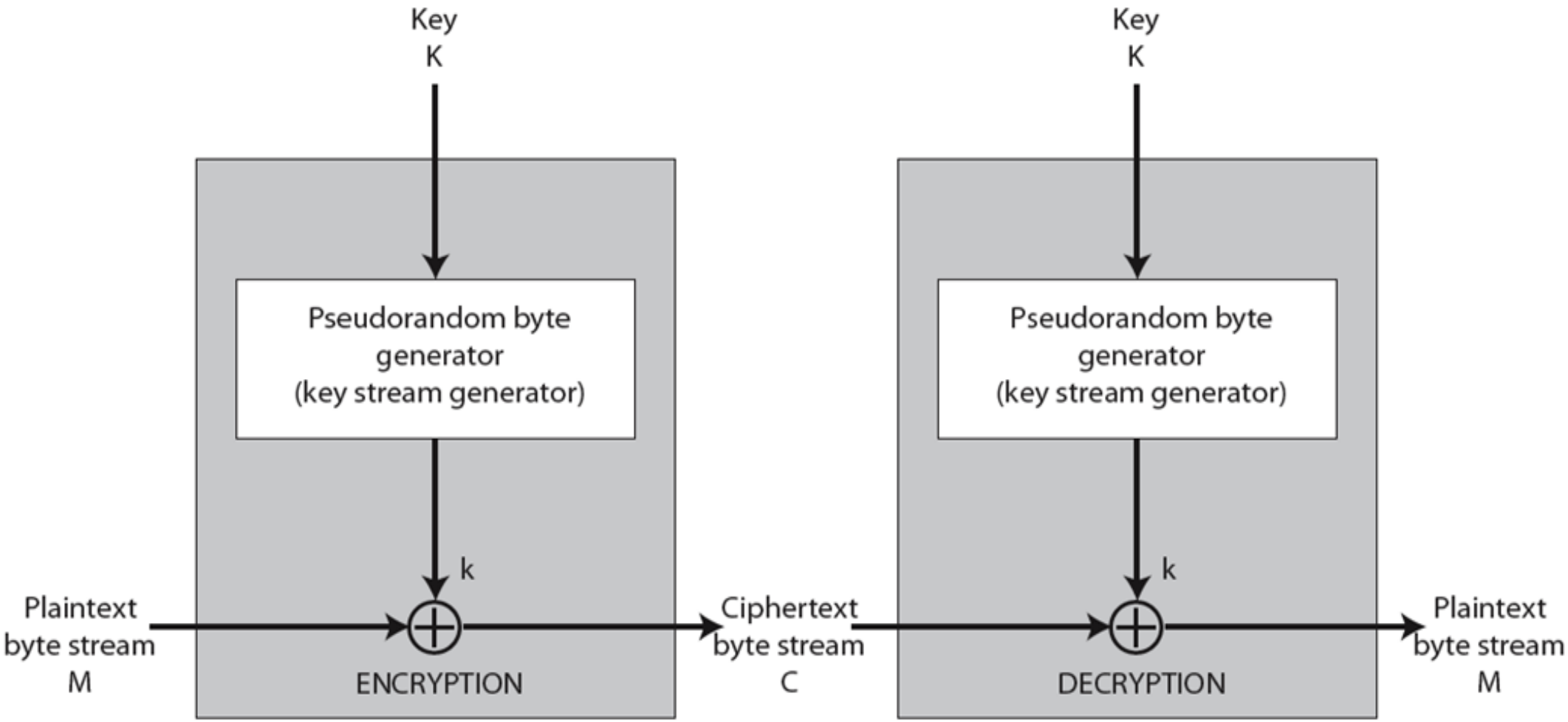
Two types of stream ciphers

1. ***Synchronous stream ciphers*** (aka key auto-key, or **KAK**) — These types of ciphers generate keystreams independently of any previous plaintext or ciphertexts.
2. ***Self-synchronizing stream ciphers*** (aka asynchronous stream ciphers, ciphertext autokey or **CTAK**) — These ciphers, on the other hand, rely on previous ciphertext bits to generate keystreams.



encrypts data one bit at a time

2 Stream Cipher Structure



3 RC4 Stream Cipher

- RC4 is an example of a modern symmetric-key stream cipher. It was developed in 1987 by Ron Rivest.
- For RC4, stream combinations are done on byte-length strings of plaintext. 256 bytes of memory are required for the state array.

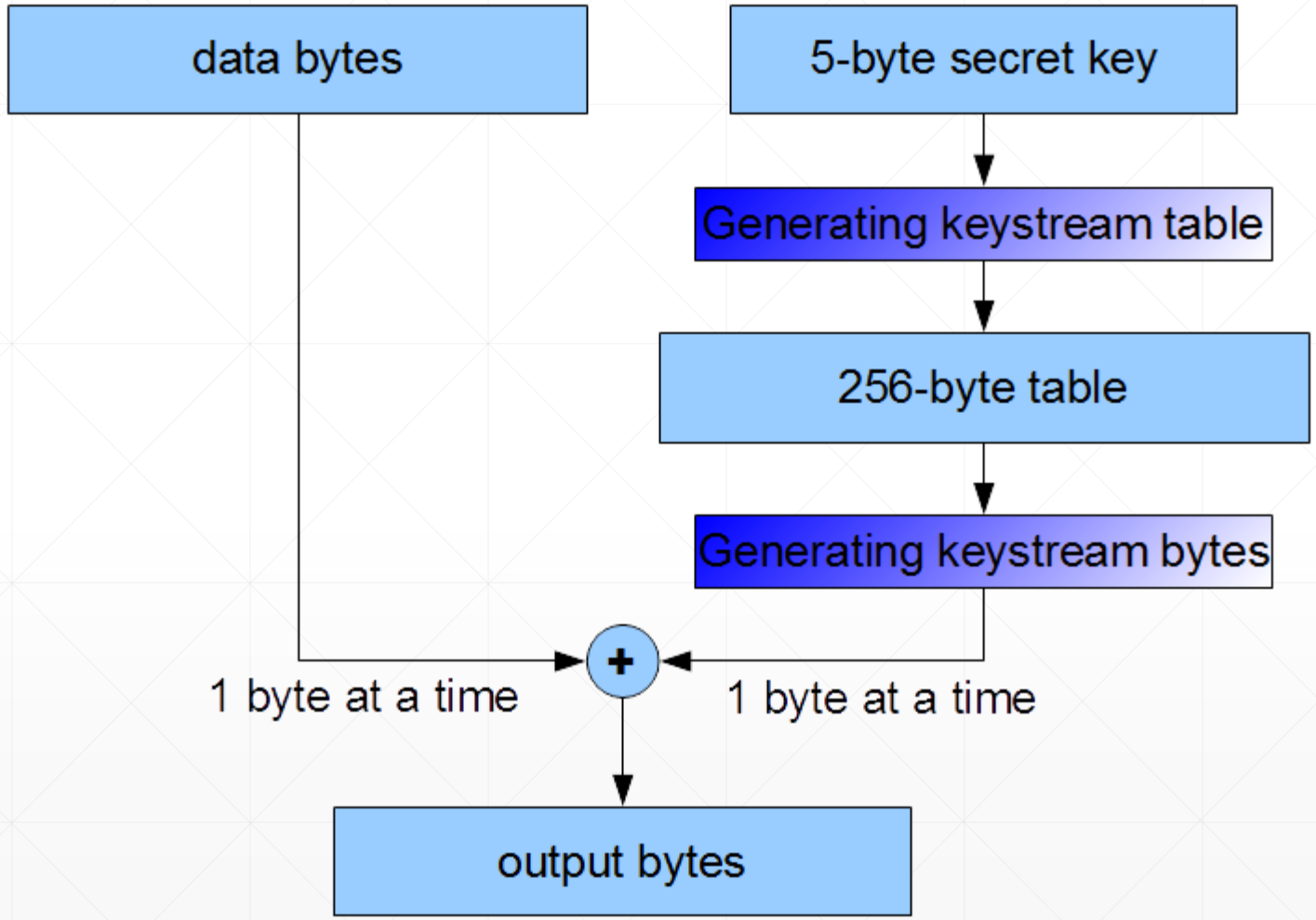
3 RC4 Stream Cipher

- Keystream Initialization

```
for i from 0 to 255
    T[i] := i
endfor
x_temp := 0
for i from 0 to 255
    x_temp := (x_temp + T[i] + K[i mod k_len]) mod 256
    swap(T[i], T[x_temp])
endfor
```

- Keystream Generation

```
p1 := 0
p2 := 0
while GeneratingOutput
    p1 := (p1 + 1) mod 256
    p2 := (p2 + T[p1]) mod 256
    swap(T[p1], T[p2])
    send(T[(T[p1] + T[p2]) mod 256])
endwhile
```



http://www.crypto-it.net/eng/symmetric/rc4.html

3 RC4 Stream Cipher

1. Key-Scheduling Algorithm

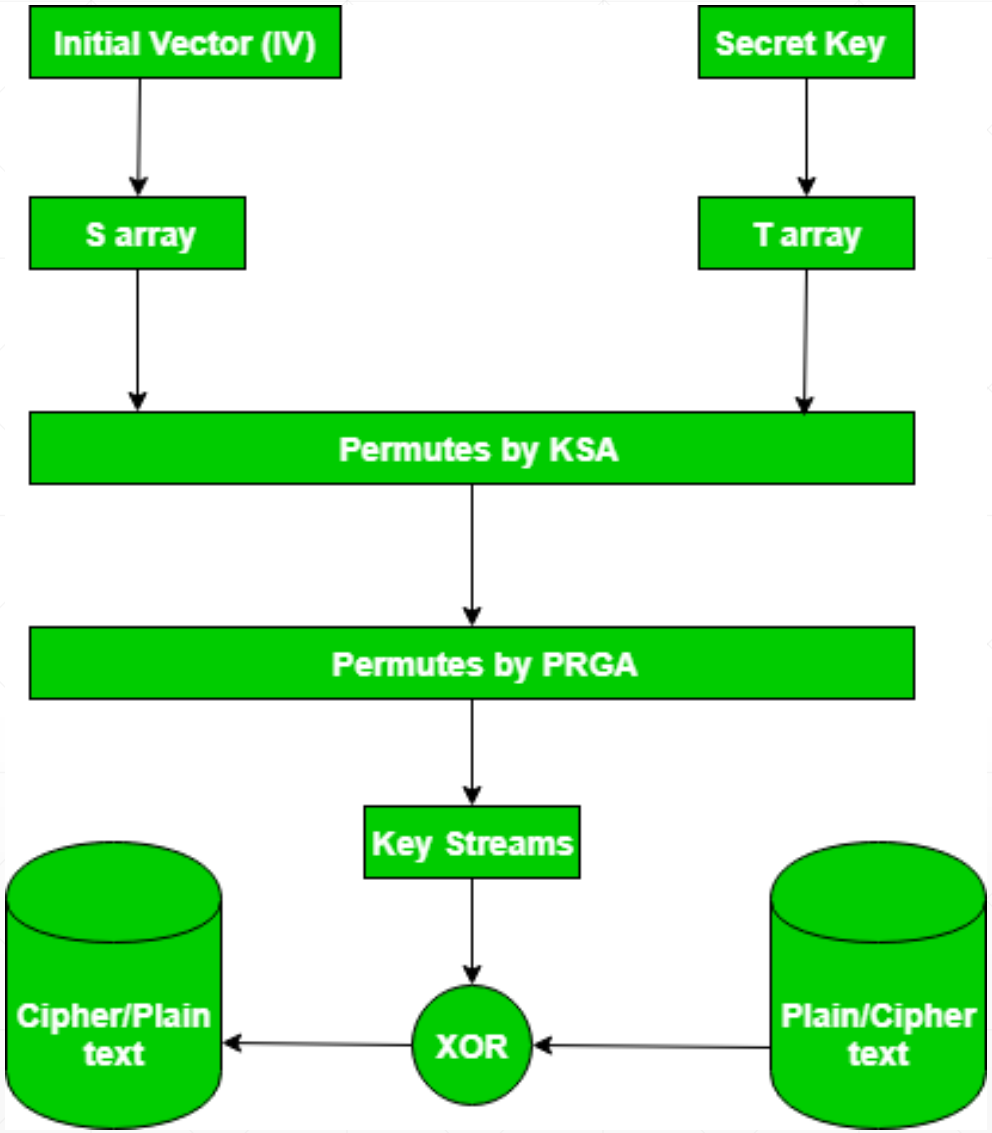
2. Pseudo random generation algorithm (Stream Generation):

3. Encrypt using X-Or()

Example:

```
RC4 Encryption
10011000 ? 01010000 = 11001000

RC4 Decryption
11001000 ? 01010000 = 10011000
```



https://www.geeksforgeeks.org/rc4-encryption-algorithm/

HUST

hust.edu.vn fb.com/dhbkhn

THANK YOU !