CS 547: Foundation of Computer Security

S. Tripathy
IIT Patna

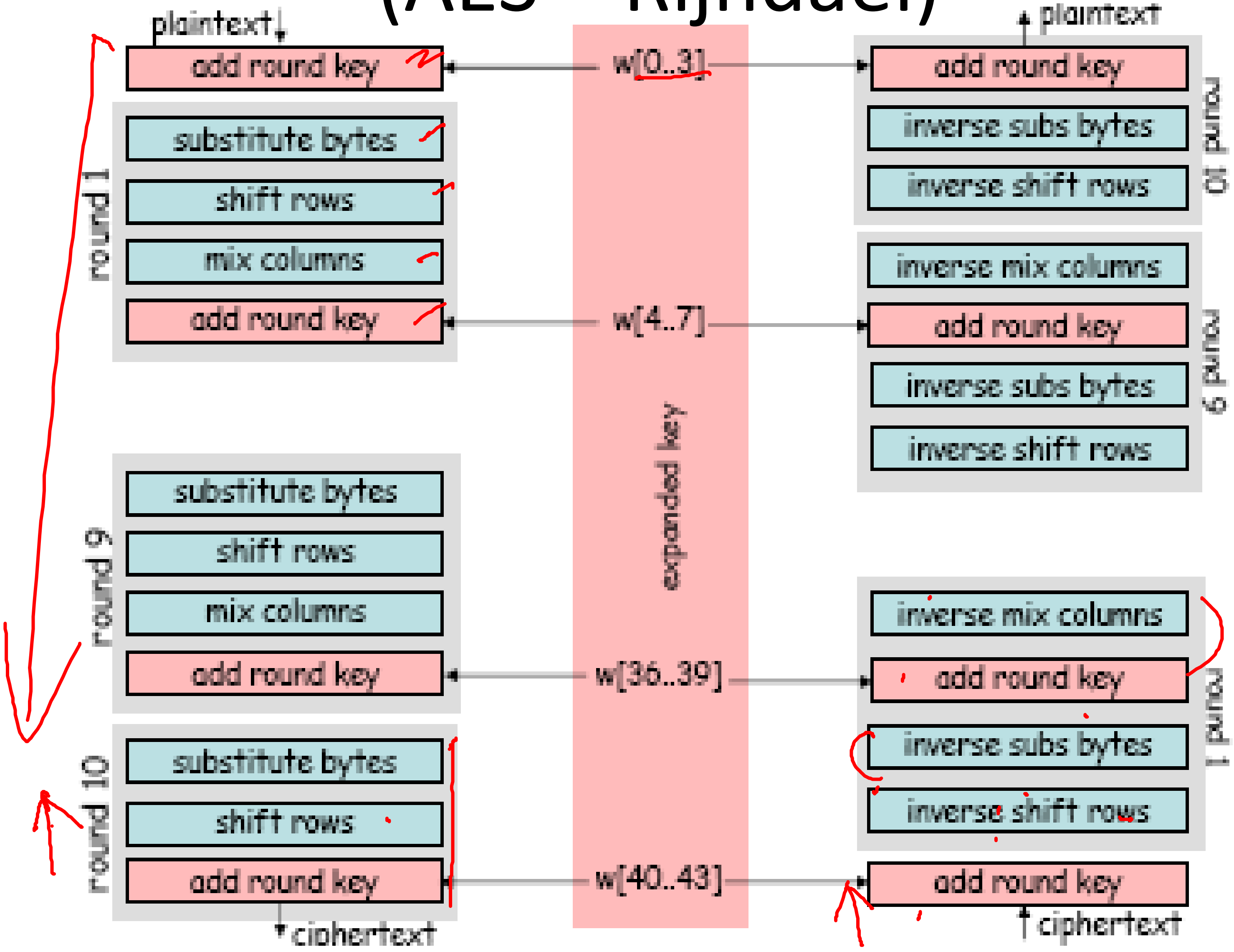
Previous Class

- Crypto Basics
- Block cipher
  - AES

Present class

- Crypto Basics
  - Block cipher
    - Modes of operations
  - Message Authentication

Symmetric key Block cipher (AES – Rijndael)



plaintext

round 1

add round key

substitute bytes

shift rows

mix columns

add round key

round 9

substitute bytes

shift rows

mix columns

add round key

round 10

substitute bytes

shift rows

add round key

ciphertext

expanded key

w[0..3]

w[4..7]

w[36..39]

w[40..43]

plaintext

round 10

add round key

inverse subs bytes

inverse shift rows

round 9

inverse mix columns

add round key

inverse subs bytes

inverse shift rows

round 1

inverse mix columns

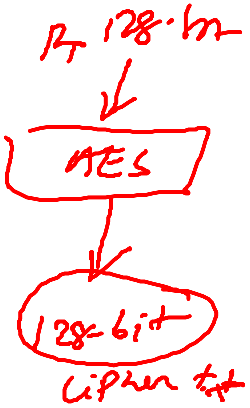
add round key

inverse subs bytes

inverse shift rows

add round key

ciphertext

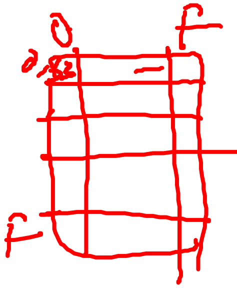


P, 128-bit

AES

128-bit

cipher txt



Practical Security Issues

- typically data unit is larger than a single 64-bit or 128-bit block
- electronic codebook (ECB) mode modes of opn
  - the simplest approach to multiple-block encryption ECB
  - each block is encrypted using the same key
  - exploit regularities in the plaintext ✓
- modes of operation
  - alternative techniques to increase the security for large sequences ✓
    - CBC, CFB, OFB, CTR etc.
  - overcomes the weaknesses of ECB

P1 Msg P2 P3 P4

Size 128 | 128 | 128 | 1B

K AES AES

C1 C2

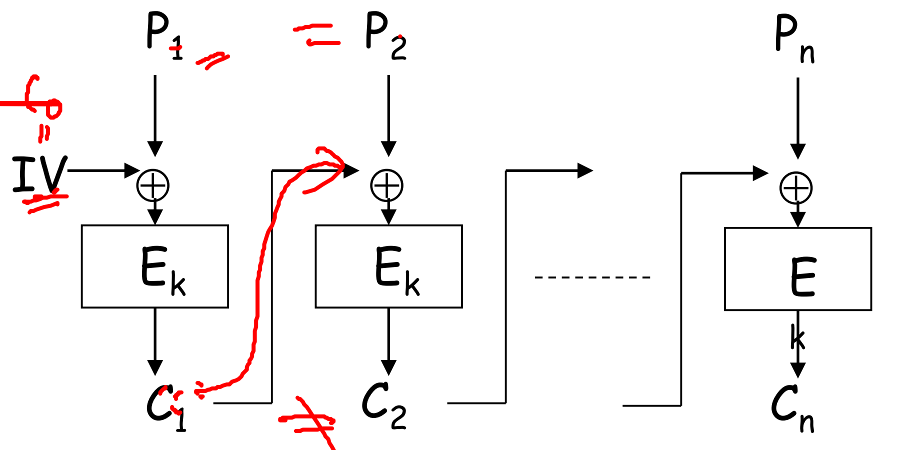
500B 1978

A Ex(500)

B Ex(B) 1978

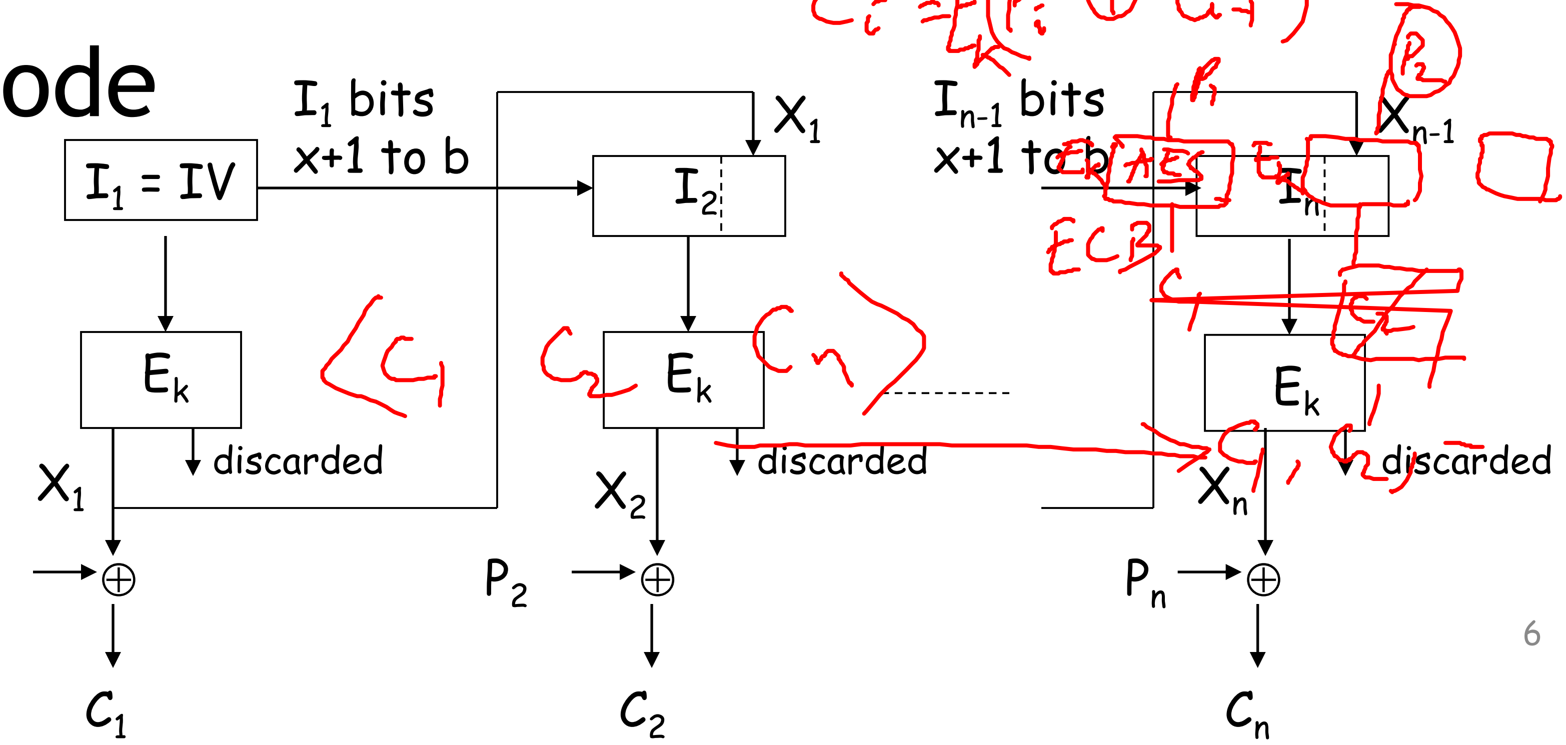
CBC Mode

Cipher Block chaining

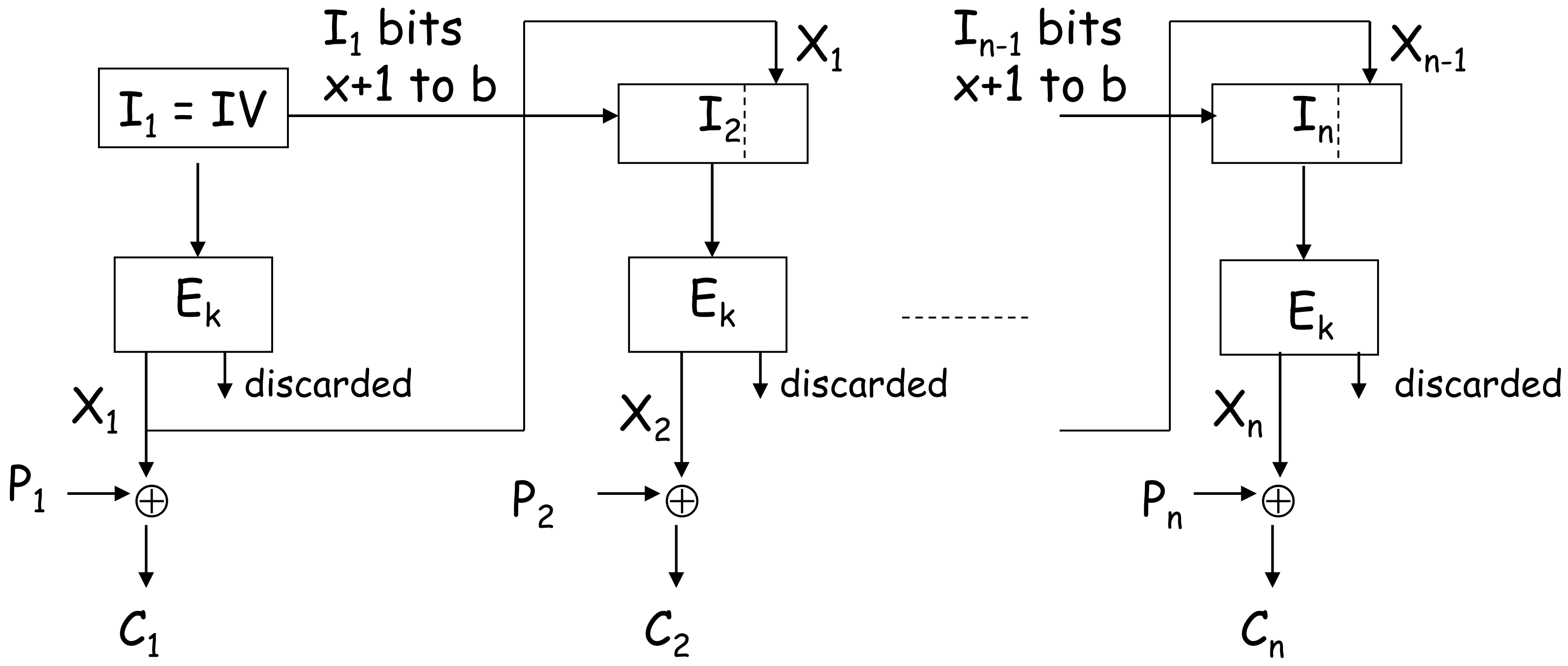


$C_i = E_k(P_i \oplus C_{i-1})$

OFB Mode

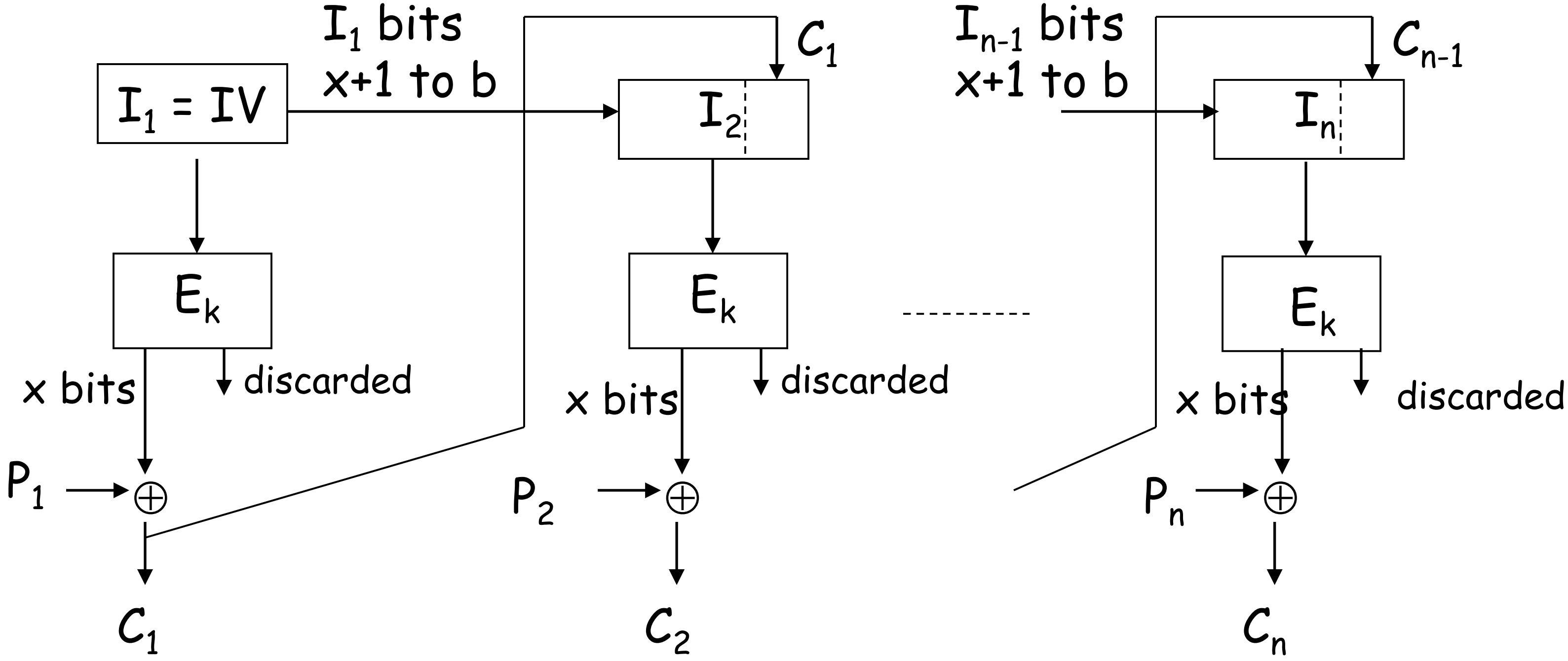


OFB Mode

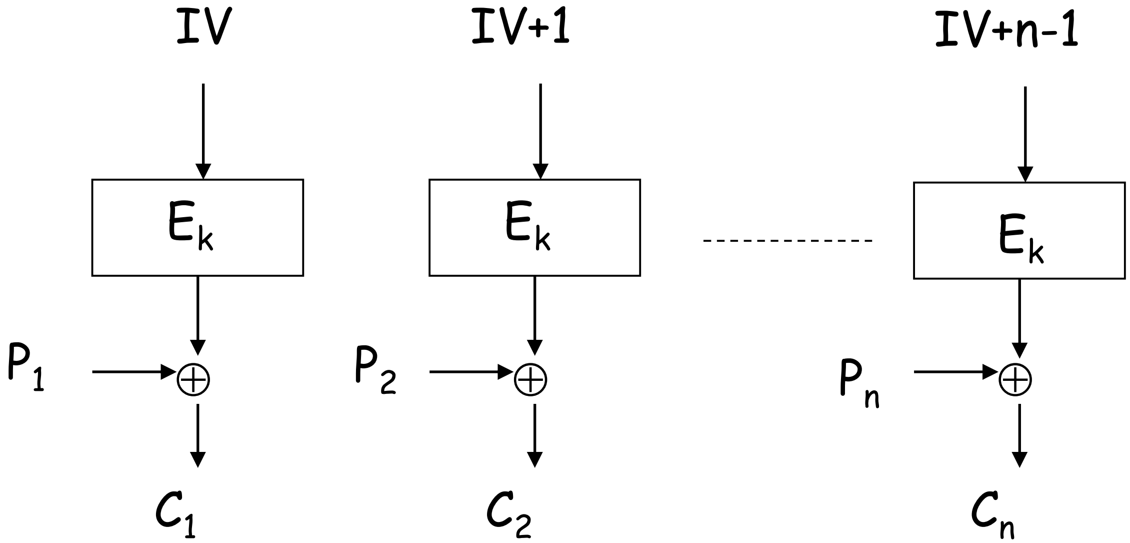


X_j = leftmost x bits of the b bit output from the cipher
P_j is x bits
$I_j = I_{j-1}$ bits x+1 to b || X_{j-1}

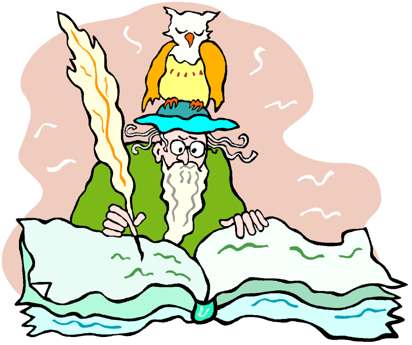
CFB Mode



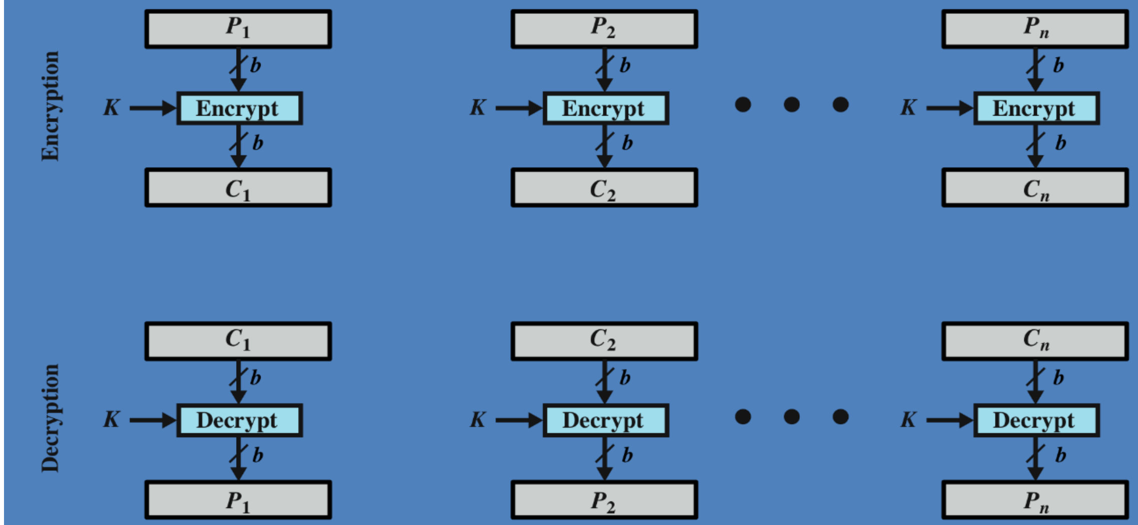
CTR Mode



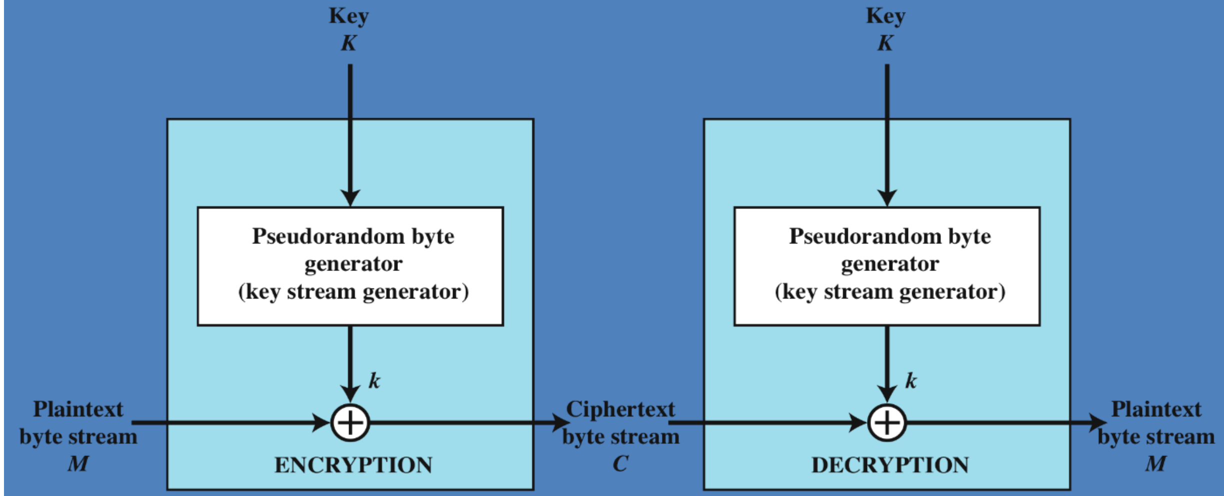
Block Cipher Encryption



Stream Encryption



(a) Block cipher encryption (electronic codebook mode)


Key
K
Pseudorandom byte generator (key stream generator)
k
Plaintext byte stream M
ENCRYPTION
Ciphertext byte stream C
Key
K
Pseudorandom byte generator (key stream generator)
k
DECRYPTION
Plaintext byte stream M

(b) Stream encryption

Block & Stream Ciphers

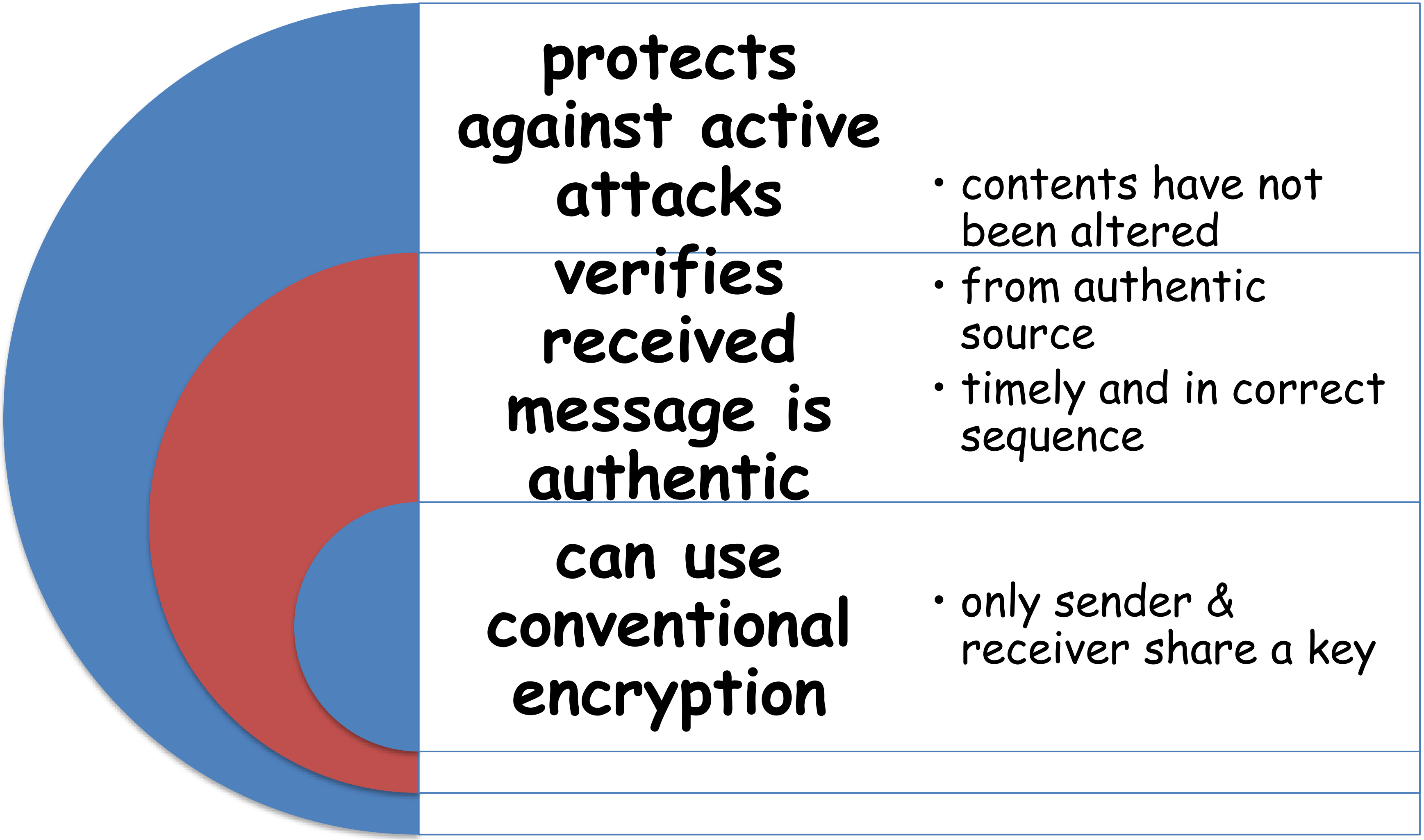
Block Cipher

- processes the input one block of elements at a time
- produces an output block for each input block
- can reuse keys
- more common

Stream Cipher

- processes the input elements continuously
- produces output one element at a time
- primary advantage is that they are almost always faster and use far less code
- encrypts plaintext one byte at a time
- pseudorandom stream is one that is unpredictable without knowledge of the input key

Message Authentication



protects against active attacks

- contents have not been altered

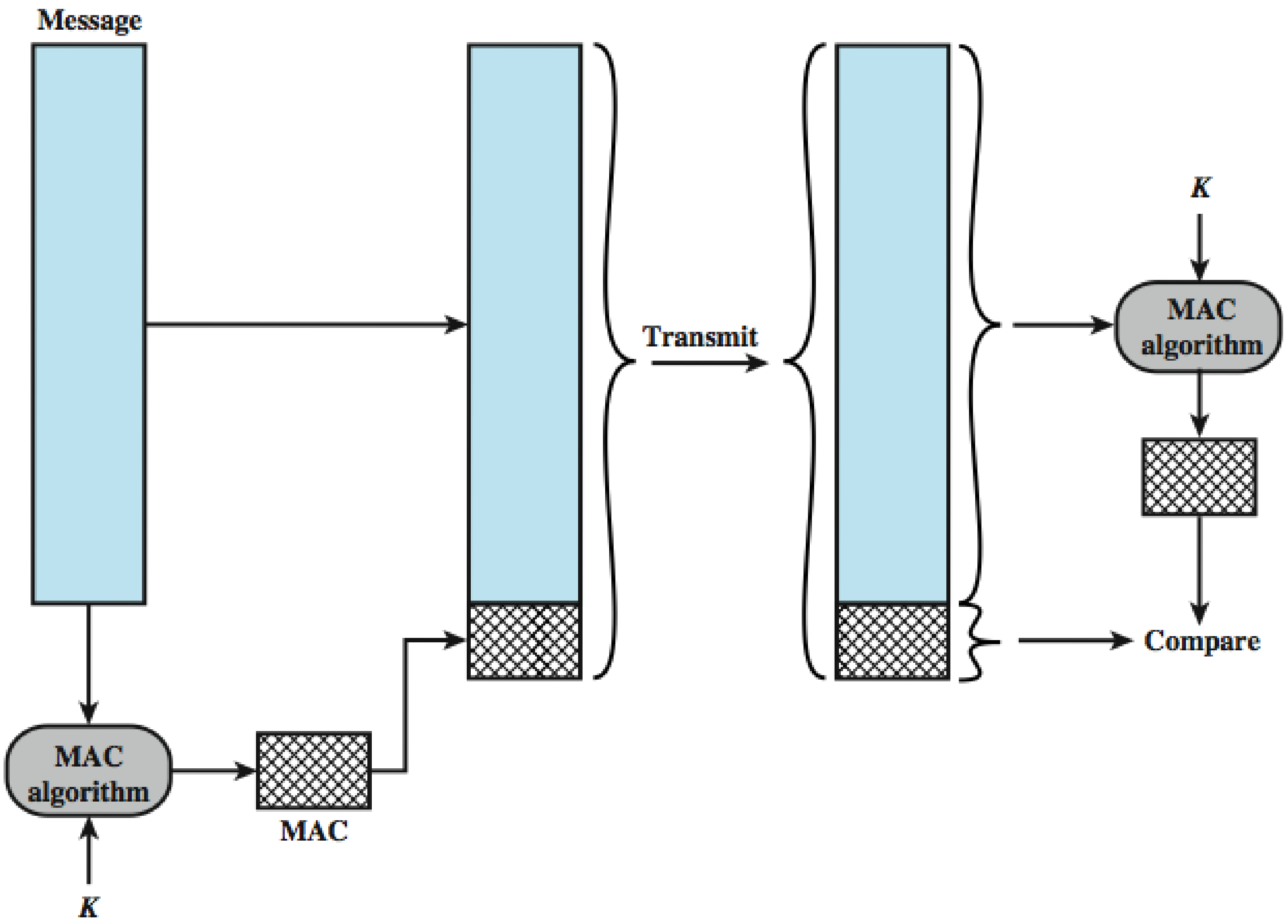
verifies received message is authentic

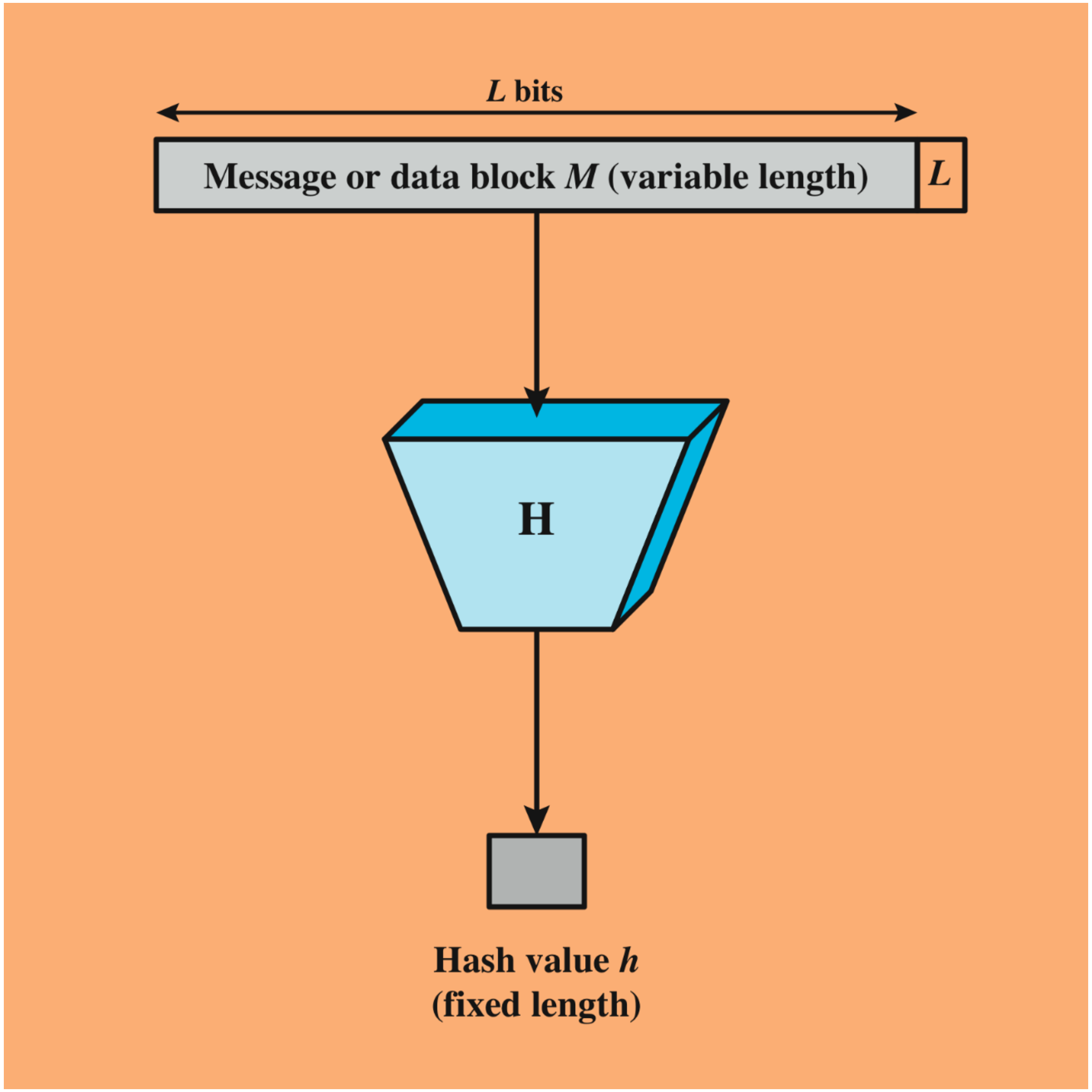
- from authentic source
- timely and in correct sequence

can use conventional encryption

- only sender & receiver share a key

Message Authentication Codes





Secure Hash Functions