Symmetric Encryption

CS 363 Computer Security

Father of Information Age: Claude Shannon (1916-2001)

- Information Theory
  - How to quantify information?
  - Lead to breakthrough in compression, machine learning, and information retrieval
- Error Detection and Control
  - How can we transmit information through noisy channel?
  - Enable wireless and mobile communication
- Cryptography
  - What does it mean by keeping information secure?
  - Gold standard for any crypto-system

Shannons strategy

- thwart cryptanalysis that is based on statistical analysis
- hacker has some knowledge of statistical characteristic of plaintext
- if statistics are reflected in ciphertext, then analyst may be able to deduce encryption key, or part of it
- in Shannons ideal cipher, statistics of ciphertext are independent of plaintext

Shannons building blocks

- confusion
  - make relation between statistics of ciphertext and the value of the encryption key as complex as possible
- diffusion
  - diffuse statistical property of plaintext digit across a range of ciphertext digits
  - i.e. each plaintext digits affects value of many ciphertext digits

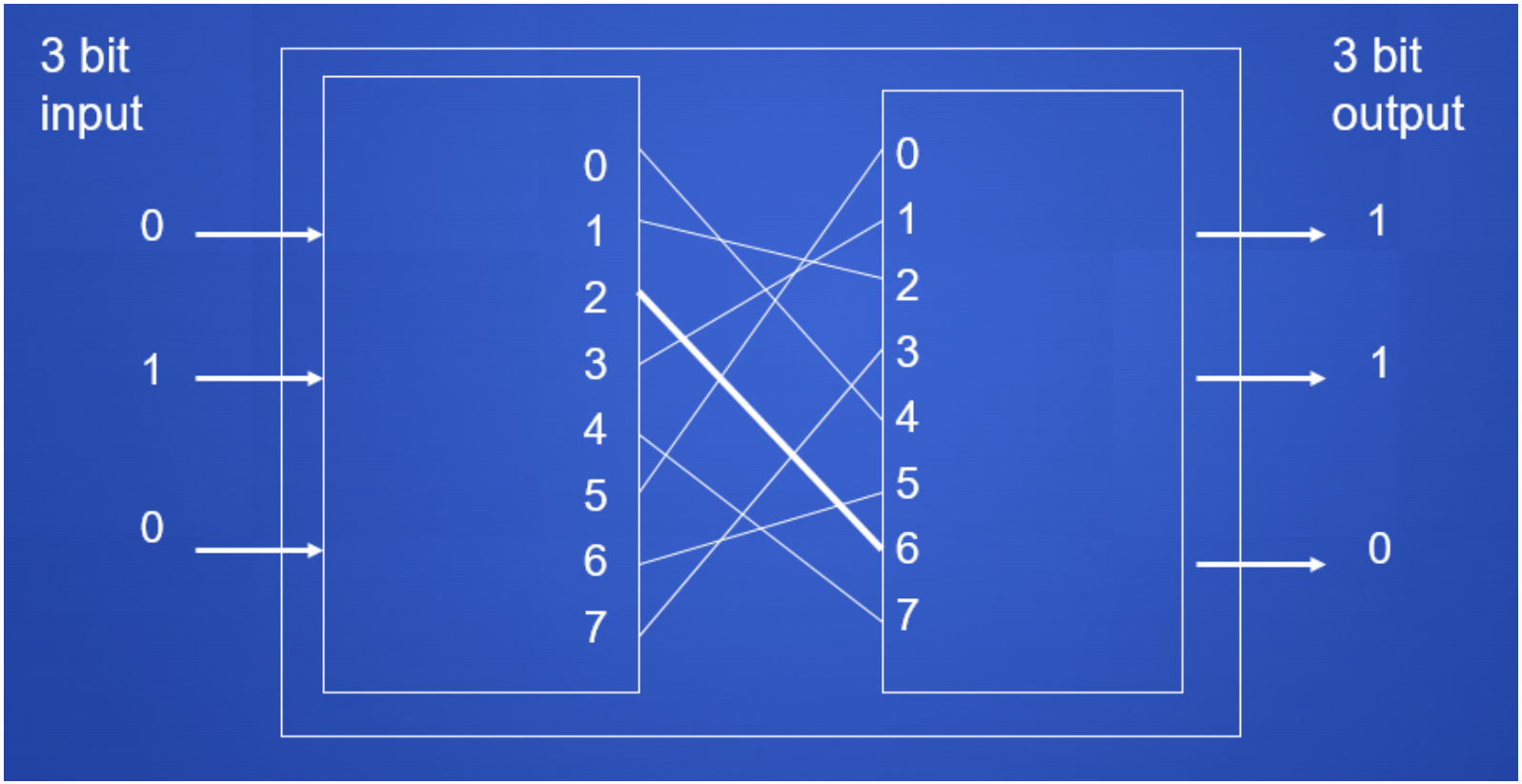
Basis of modern ciphers

- product cipher
  - perform two or more ciphers in sequence so that result (product) is cryptographically stronger than any component cipher
- alternate confusion & diffusion
- virtually all significant symmetric block ciphers currently in use are of this type

Shannons building blocks

- Shannon proposed product ciphers with two components
  - S-Boxes – substitution: providing confusion of input bits
  - P-Boxes – permutation: providing diffusion across S-box inputs
- n rounds of S-P boxes

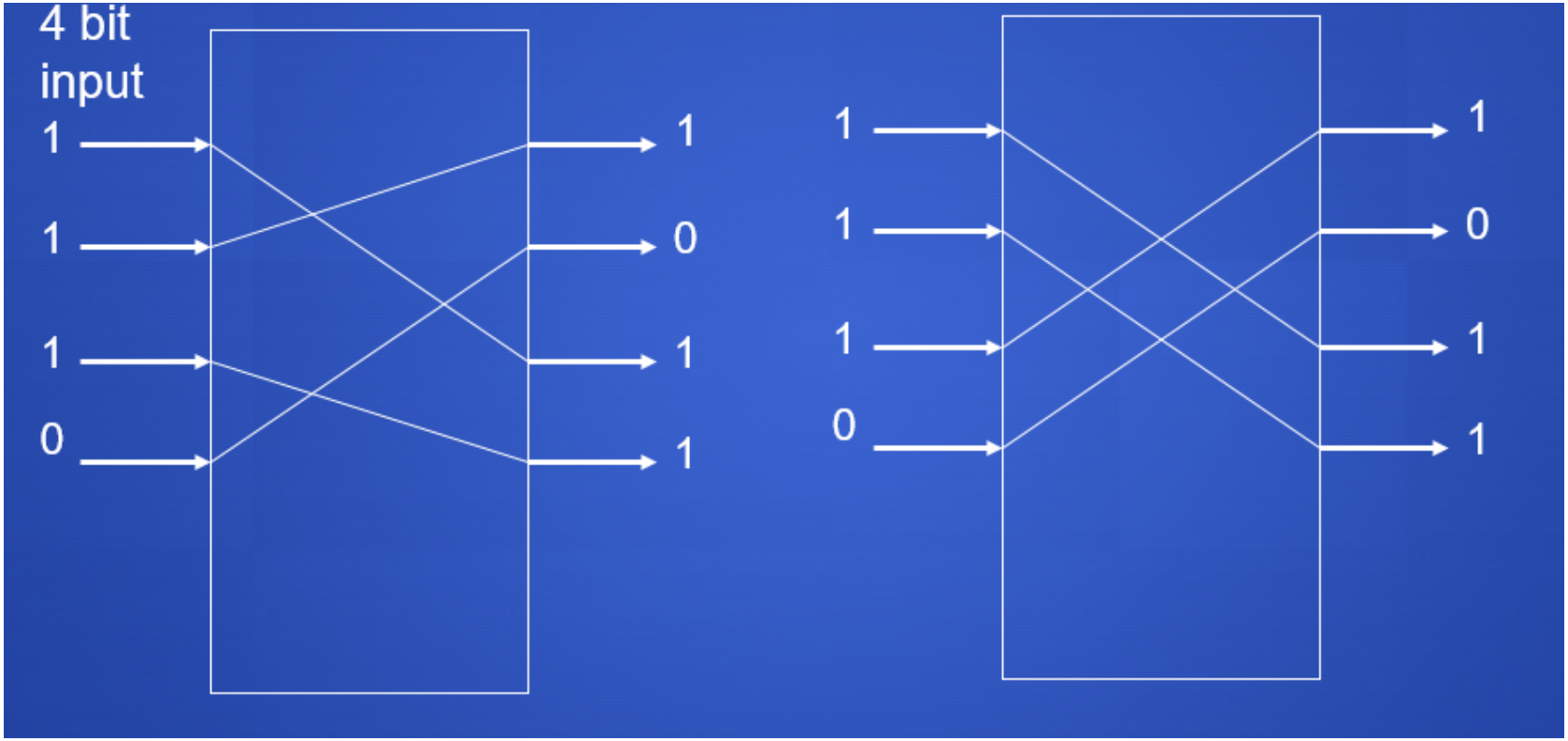
S-box (substitution)



Word-size of 3 bits $\rightarrow$ mapping of $2^3 = 8$ values

Note: mapping can be reversed

P-box (permutation)



S-P networks

- alternate S and P boxes
- BUT, in practice we must decrypt as well as encrypt
- so define the sequence of boxes so that precisely the same system will decrypt as well as encrypt
- just run it backwards

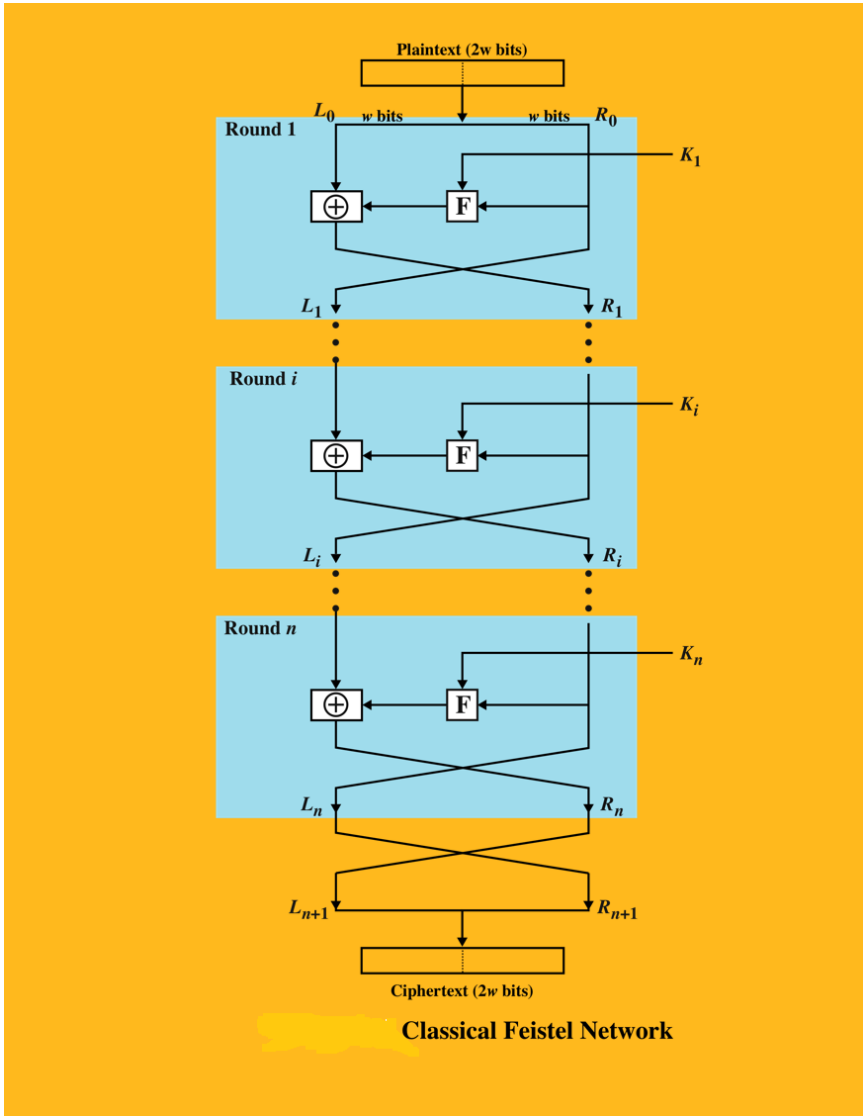
Block Cipher Structure

- symmetric block cipher consists of:
  - a sequence of rounds
  - with substitutions and permutations controlled by key
- parameters and design features:
  - block size, key size, number of rounds, subkey generation algorithm, round function, fast software encryption/decryption, ease of analysis

Data Encryption Standard (DES)

- adopted in 1977 by National Bureau of Standards: now NIST
- FIPS PUB 46
- minor variation of the Feistel network
  - 64 bit plaintext
  - 56 bit key
  - 16 rounds

Feistel Cipher Structure

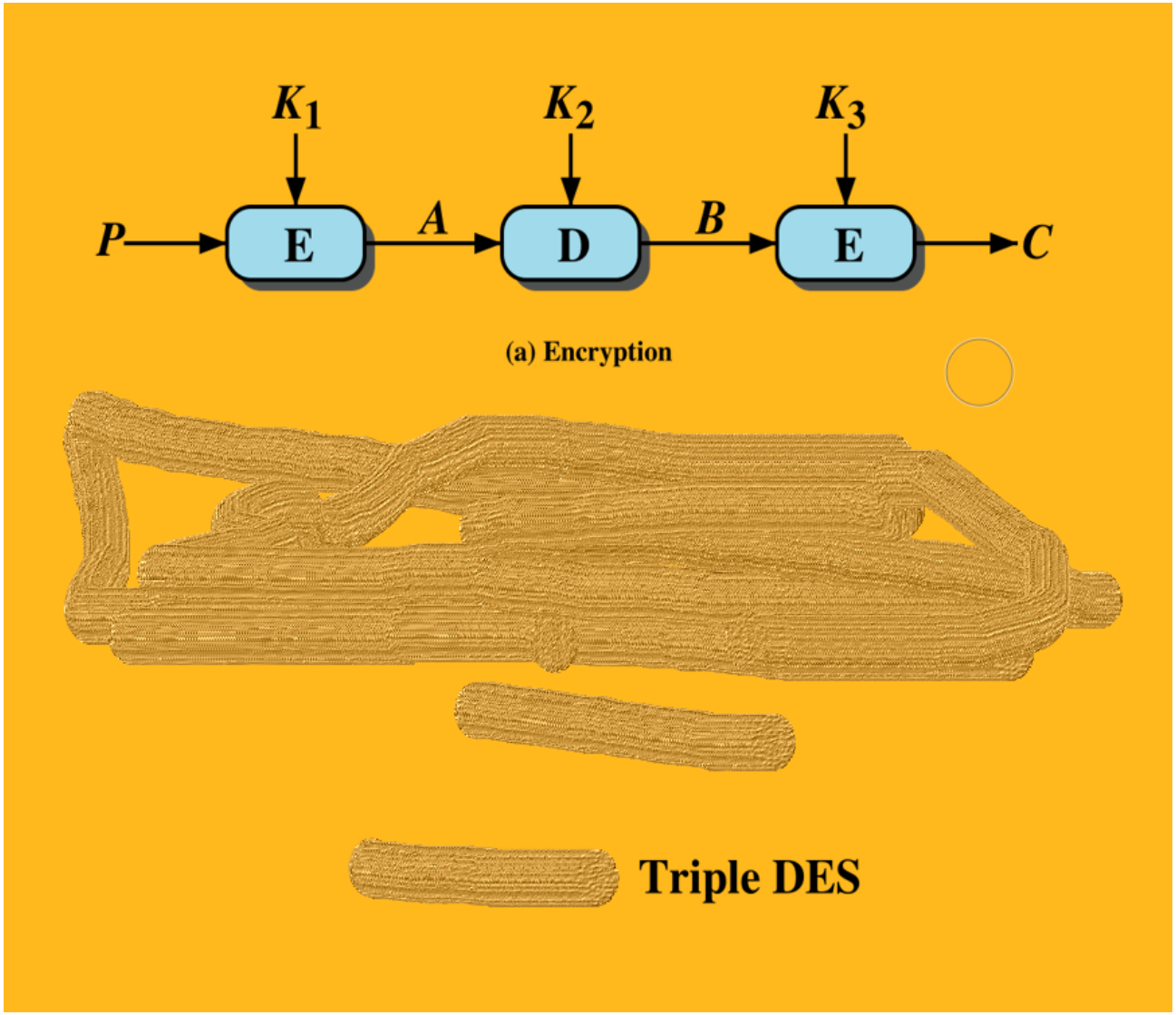


Classical Feistel Network

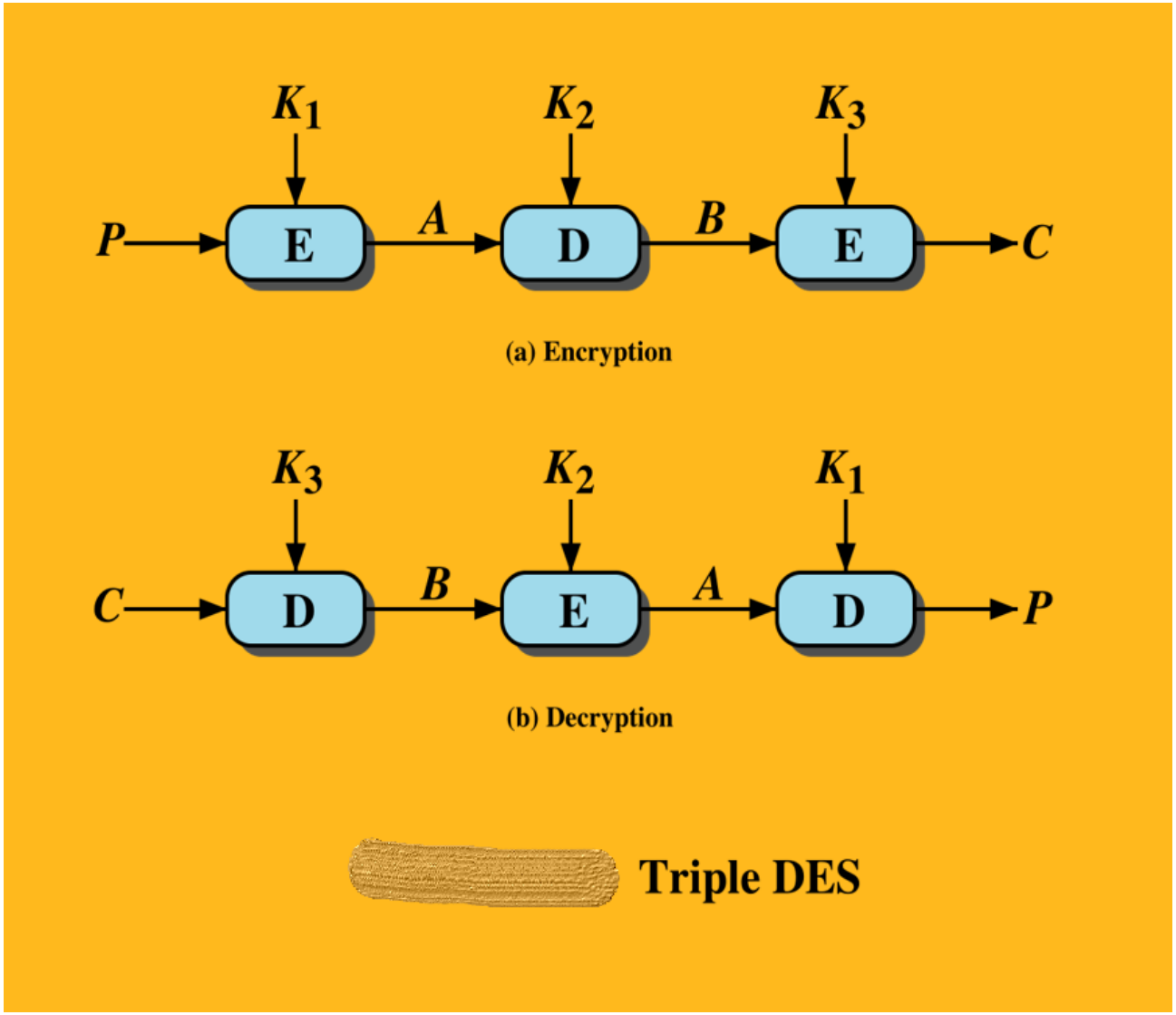
Security of DES

- Strong theoretically but vulnerable to brute-force attack
- DESCHALL Competition
  - RSA Security offered a $10,000$ dollars prize in 1997, for the first who crack the DES.
  - A group of computer scientists involved thousands of volunteers deciphered it!
  - It took only 96 days!
- How?
  - With the help of up to 14k computers a day and a total of 78k unique computers.
  - By offering a $4,000$ dollars prize to the computer owner who finds the right key.

Triple DES (3DES)



Triple DES (3DES)



Triple DES (3DES)

- first used in financial applications
- in DES FIPS PUB 46-3 standard of 1999
- uses three keys and three DES executions:
  $C = E(k_3, D(K_2, E(K_1, P)))$
- decryption same with keys reversed
- use of decryption in second stage gives compatibility with original DES users
- effective 168-bit key length, slow, secure

Origins

- a replacement for DES was needed
  - Key size is too small
  - The variants are just patches
- can use Triple-DES - but slow, has small blocks
- US NIST issued call for ciphers in 1997
- 15 candidates accepted in Jun 98
- 5 were shortlisted in Aug 99

AES Competition Requirements

- private key symmetric block cipher
- 128-bit data, 128/192/256-bit keys
- stronger & faster than Triple-DES
- provide full specification & design details
- both C & Java implementations
- NIST have released all submissions & unclassified analyses

AES Shortlist

- after testing and evaluation, shortlist in Aug-99:
  - MARS (IBM) - complex, fast, high security margin
  - RC6 (USA) - v. simple, v. fast, low security margin
  - Rijndael (Belgium) - clean, fast, good security margin
  - Serpent (Euro) - slow, clean, v. high security margin
  - Twofish (USA) - complex, v. fast, high security margin
- then subject to further analysis & comment
- saw contrast between algorithms with
  - few complex rounds versus many simple rounds
  - Refined versions of existing ciphers versus new proposals

The AES Cipher - Rijndael

- Rijndael was selected as the AES in Oct-2000
- issued as FIPS PUB 197 standard in Nov-2001
- designed by Joan Rijmen and Vincent Daemen in Belgium
- has 128/192/256 bit keys, 128 bit data
- an iterative rather than Feistel cipher
  - processes data as block of 4 columns of 4 bytes
  - operates on entire data block in every round
- designed to be:
  - resistant against known attacks
  - speed and code compactness on many CPUs
  - design simplicity
  - few complex rounds versus many simple rounds
  - Refined versions of existing ciphers versus new proposals

The AES Cipher - Rijndael

- data block viewed as 4-by-4 table of bytes
- Such a table is called the current state
- key is expanded to array of words
- has 10 rounds in which state the following transformations (called 'layers'):
  - BS- byte substitution (1 S-box used on every byte)
  - SR- shift rows (permute bytes between groups/columns)
  - MC- mix columns (uses matrix multiplication in GF(256))
  - ARK- add round key (XOR state with round key)
- First and last round are a little different

AES Encryption and Decryption

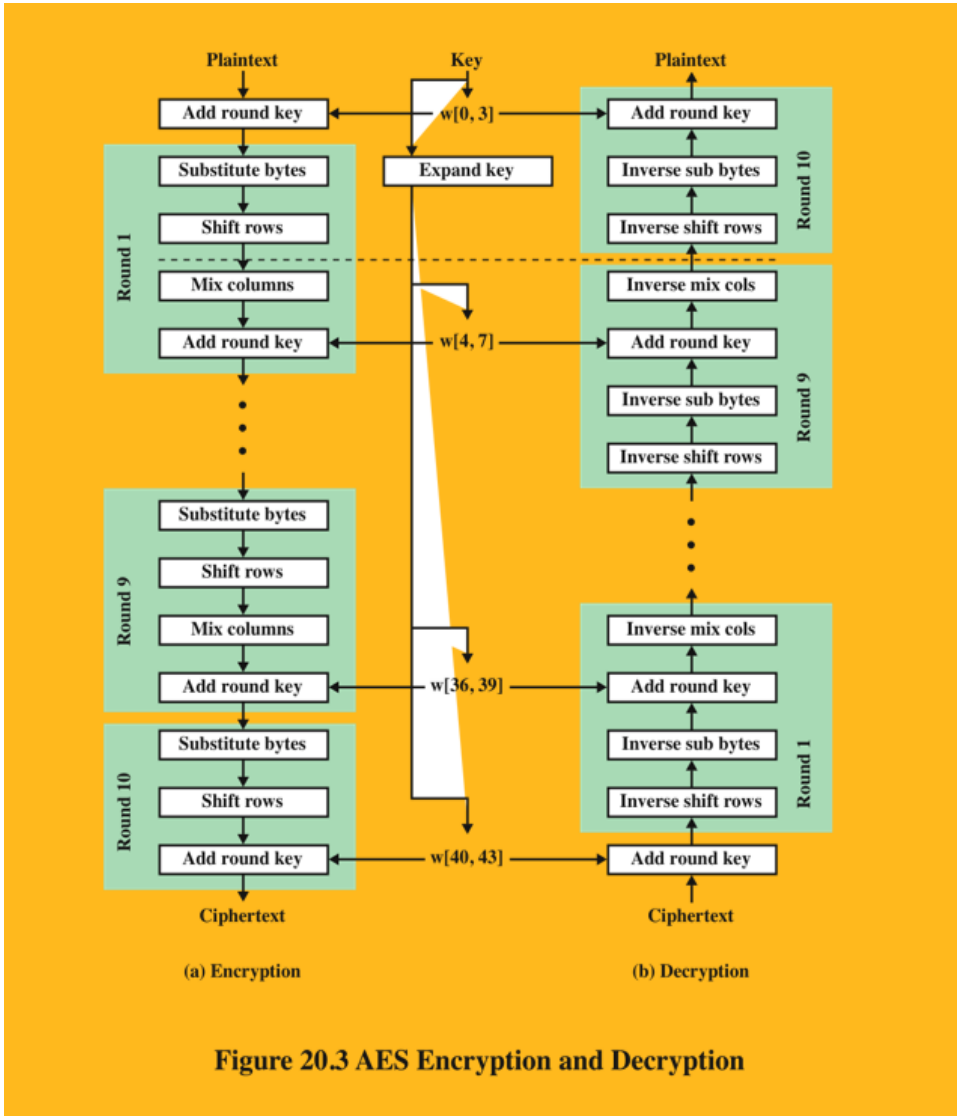


Figure 20.3 AES Encryption and Decryption

AES Decryption

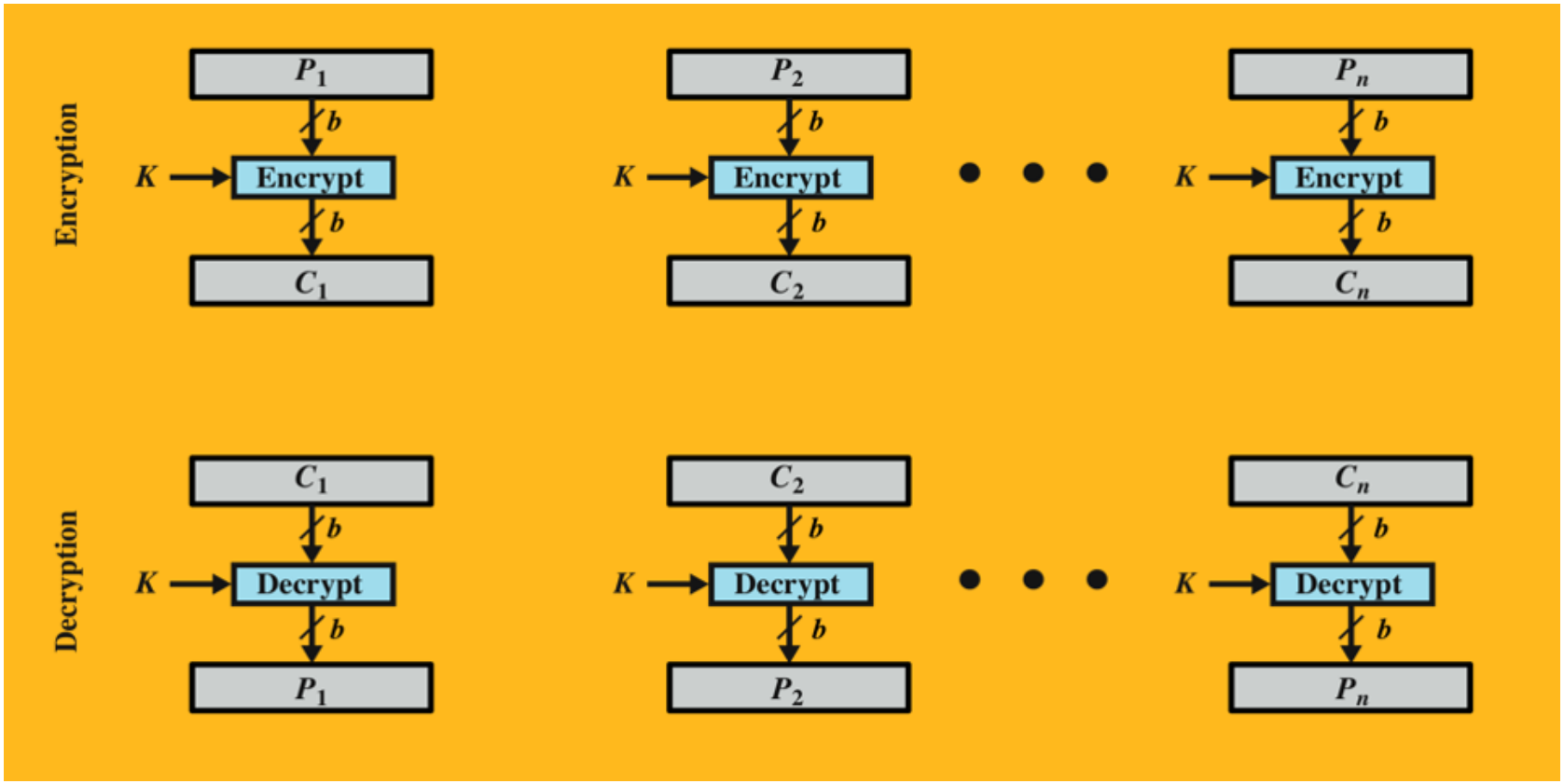
- AES decryption is not identical to encryption since steps done in reverse
- but can define an equivalent inverse cipher with steps as for encryption
  - but using inverses of each step
  - with a different key schedule
- works since result is unchanged when
  - swap byte substitution & shift rows
  - swap mix columns & add (tweaked) round key

Implementation Aspects

Can efficiently implement on 8-bit CPU

- byte substitution works on bytes using a table of 256 entries
- shift rows is simple byte shift
- add round key works on byte XORs
- mix columns requires matrix multiply which works on byte values, can be simplified to use table lookups & byte XORs

Mode of Operations



Mode of Operations

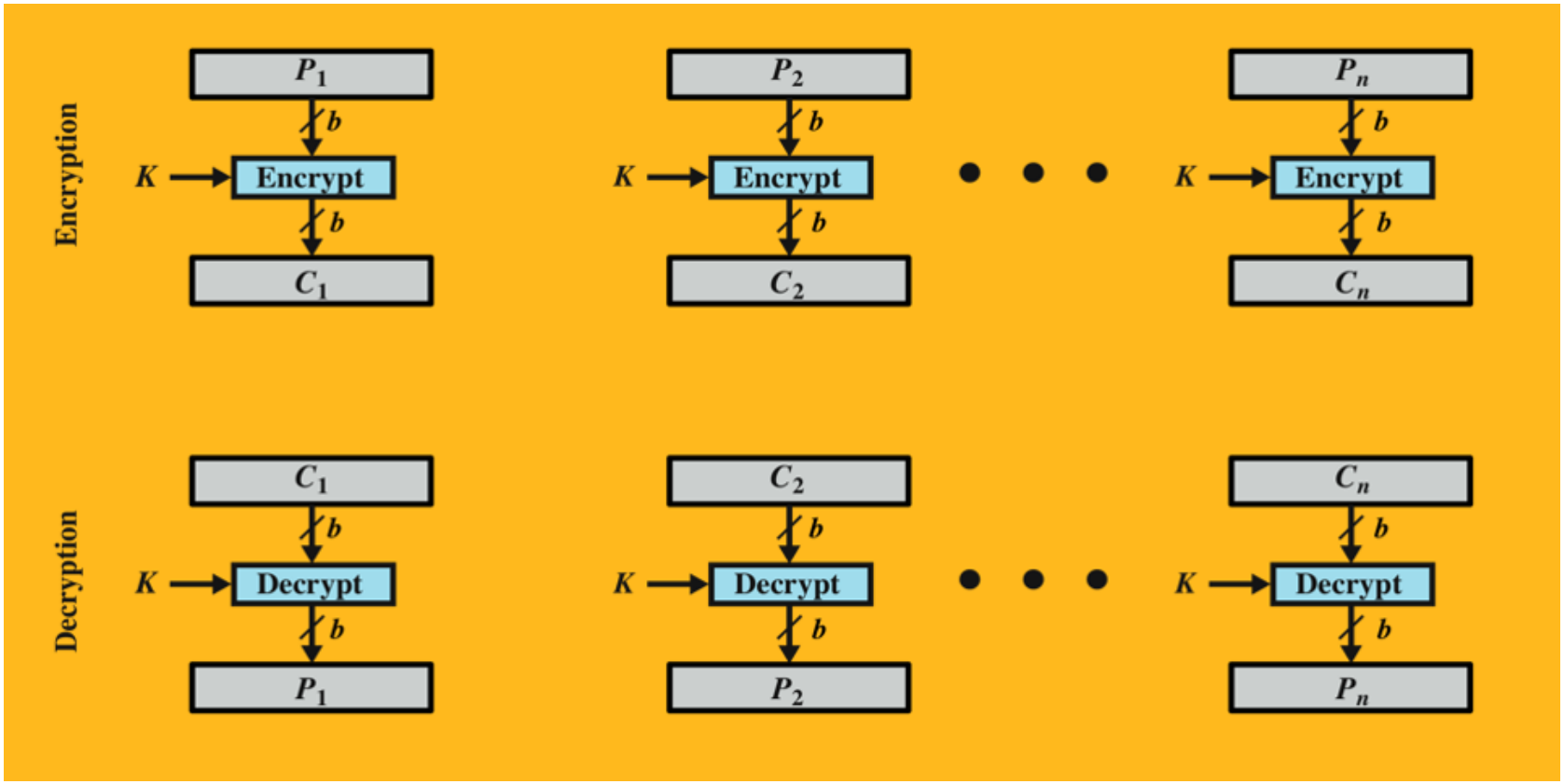
Mode	Description	Typical Application
Electronic Codebook (ECB)	Each block of 64 plaintext bits is encoded independently using the same key.	•Secure transmission of single values (e.g., an encryption key)
Cipher Block Chaining (CBC)	The input to the encryption algorithm is the XOR of the next 64 bits of plaintext and the preceding 64 bits of ciphertext.	•General-purpose block-oriented transmission •Authentication
Cipher Feedback (CFB)	Input is processed s bits at a time. Preceding ciphertext is used as input to the encryption algorithm to produce pseudorandom output, which is XORed with plaintext to produce next unit of ciphertext.	•General-purpose stream-oriented transmission •Authentication
Output Feedback (OFB)	Similar to CFB, except that the input to the encryption algorithm is the preceding DES output.	•Stream-oriented transmission over noisy channel (e.g., satellite communication)
Counter (CTR)	Each block of plaintext is XORed with an encrypted counter. The counter is incremented for each subsequent block.	•General-purpose block-oriented transmission •Useful for high-speed requirements

Implementation Aspects

Can efficiently implement on 8-bit CPU

- byte substitution works on bytes using a table of 256 entries
- shift rows is simple byte shift
- add round key works on byte XORs
- mix columns requires matrix multiply which works on byte values, can be simplified to use table lookups & byte XORs

Mode of Operations



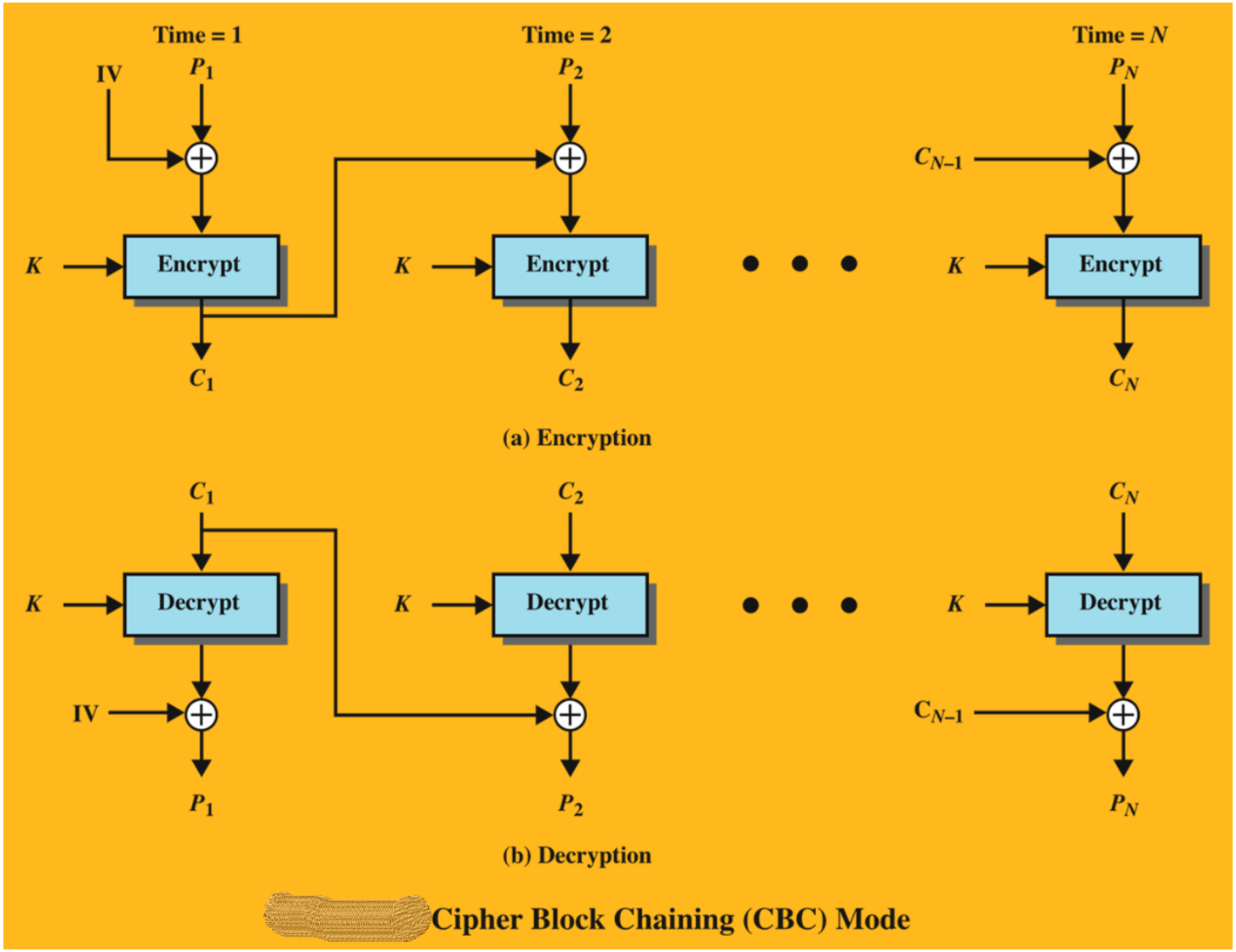
Mode of Operations

Mode	Description	Typical Application
Electronic Codebook (ECB)	Each block of 64 plaintext bits is encoded independently using the same key.	•Secure transmission of single values (e.g., an encryption key)
Cipher Block Chaining (CBC)	The input to the encryption algorithm is the XOR of the next 64 bits of plaintext and the preceding 64 bits of ciphertext.	•General-purpose block-oriented transmission •Authentication
Cipher Feedback (CFB)	Input is processed s bits at a time. Preceding ciphertext is used as input to the encryption algorithm to produce pseudorandom output, which is XORed with plaintext to produce next unit of ciphertext.	•General-purpose stream-oriented transmission •Authentication
Output Feedback (OFB)	Similar to CFB, except that the input to the encryption algorithm is the preceding DES output.	•Stream-oriented transmission over noisy channel (e.g., satellite communication)
Counter (CTR)	Each block of plaintext is XORed with an encrypted counter. The counter is incremented for each subsequent block.	•General-purpose block-oriented transmission •Useful for high-speed requirements

Electronic Codebook (ECB)

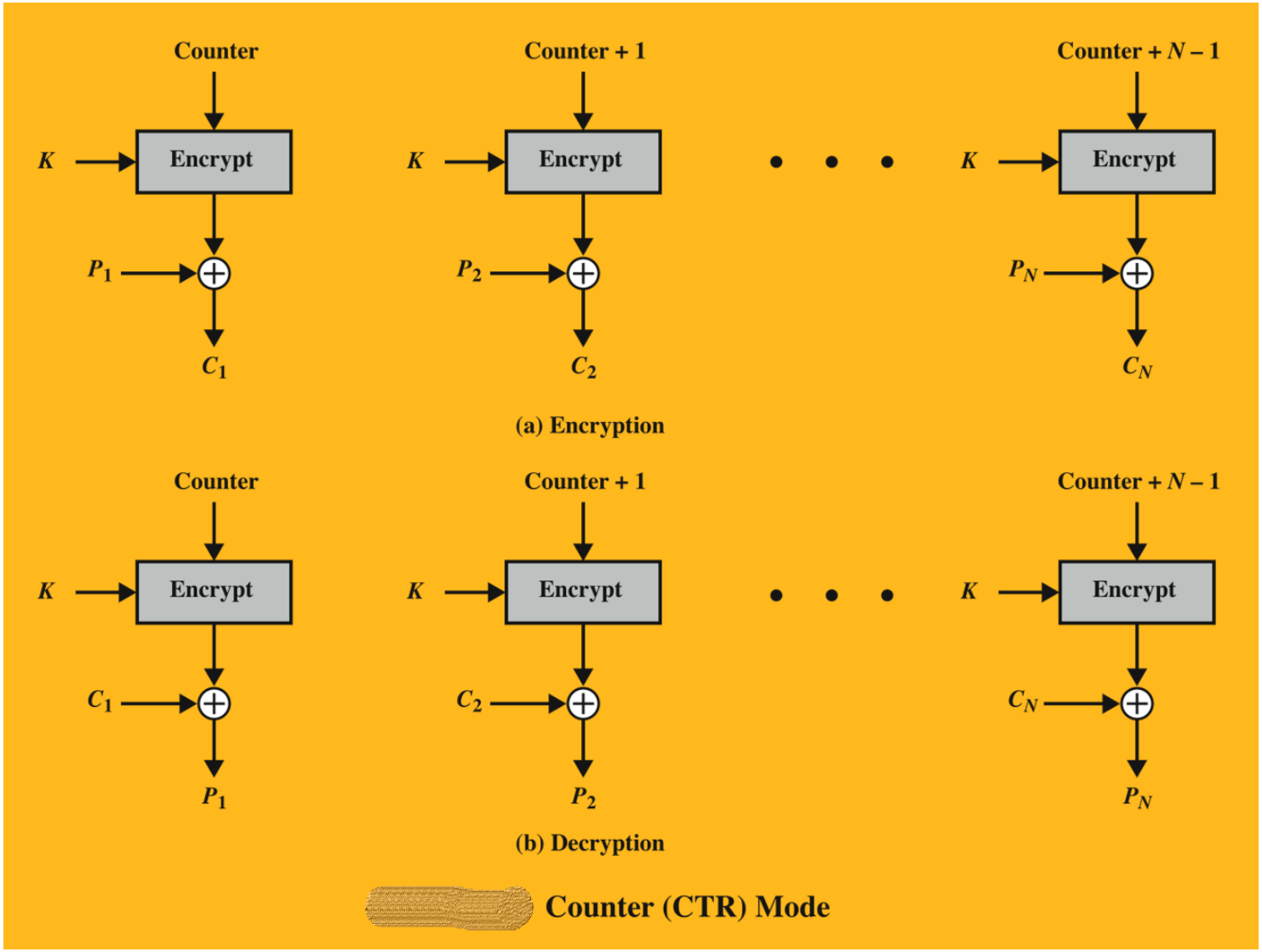
- simplest mode
- plaintext is handled b bits at a time and each block is encrypted using the same key
- "codebook" because have unique ciphertext value for each plaintext block
  - not secure for long messages since repeated plaintext is seen in repeated ciphertext
- to overcome security deficiencies you need a technique where the same plaintext block, if repeated, produces different ciphertext blocks

Cipher Block Chaining (CBC)



Cipher Block Chaining (CBC) Mode

Counter (CTR)


Counter
Counter + 1
Counter + N – 1
K
Encrypt
P_1
C_1
P_2
C_2
P_N
C_N
(a) Encryption
C_1
C_2
C_N
P_1
P_2
P_N
(b) Decryption
Counter (CTR) Mode