

1

LECTURE CONTENT

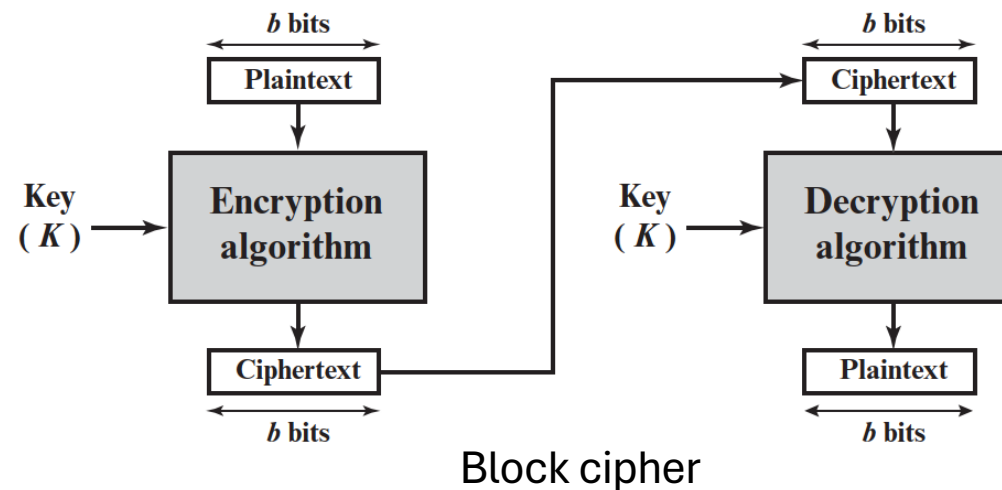
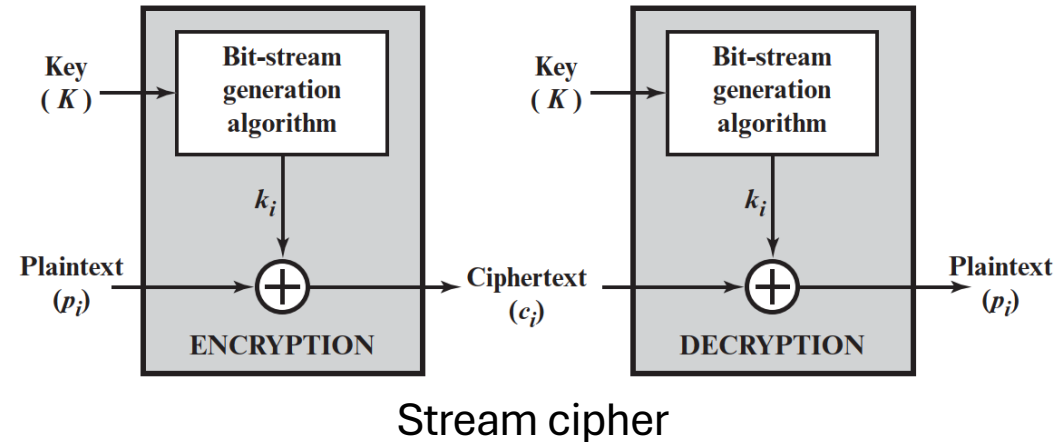
- Feistel Cipher
- Data Encryption Standard (DES)
- Multiple Encryption DES (3DES)
- Advanced Encryption Standard (AES)
- Laboratory_01: Python Encryption AES
- Laboratory_02: DES encryption using OpenSSL
- Laboratory_03: AES encryption using OpenSSL

Learning objectives

- Block ciphers encrypt message in units called blocks
- Modern Cryptography Algorithm

STREAM CIPHER V.S. BLOCK CIPHER

- ❑ A stream cipher is one that encrypts a digital data stream one bit or one byte at a time.
- ❑ A block cipher is one in which a block of plaintext is treated as a whole and used to produce a ciphertext block of equal length.



101011010101000010110101010101000010010101000010101101010100010110

MOTIVATION OF BLOCK CIPHER

- Can we use long blocks with a reversible/simple/arbitrary substitution cipher?

- Block size = $n = 4$ bits
 - Key size = $n \times 2^n$ bits
 - Number of possible transformations = $2^n!$
- With a large block size is not practical from an implementation and performance point of view
 - $n = 64$ bits
 - No. of transformations = $2^{64}!$
- Problem: Key size = 2^{70} bits $\approx 10^{20}$ bytes!!!!

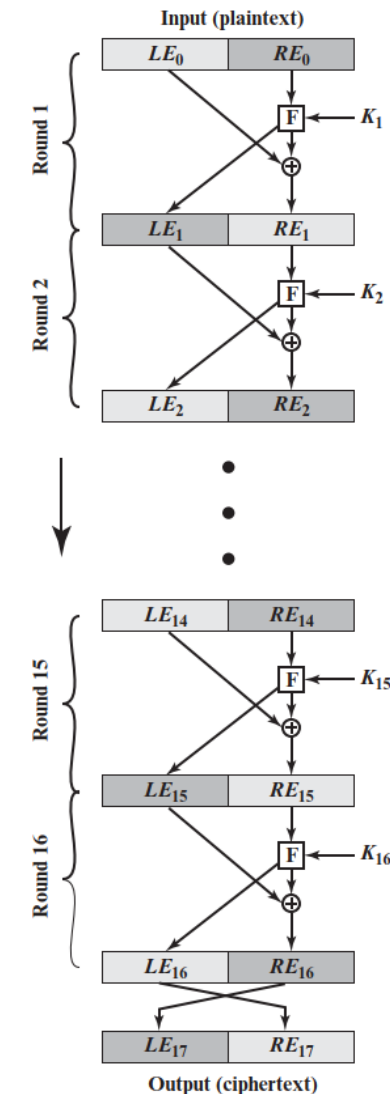
Plaintext	Ciphertext
0000	1110
0001	0100
0010	1101
0011	0001
0100	0010
0101	1111
0110	1011
0111	1000
1000	0011
1001	1010
1010	0110
1011	1100
1100	0101
1101	1001
1110	0000
1111	0111

FEISTEL CIPHER

- Feistel proposed to approximate the ideal block cipher by utilizing the concept of a product cipher.
- A product cipher is the execution of two or more simple ciphers in sequence, e.g. rotor machine.
- Feistel proposed the use of alternating substitutions and permutations:
 - **Substitution:** Each plaintext element or group of elements is uniquely replaced by a corresponding ciphertext element or group of elements.
 - **Permutation:** A sequence of plaintext elements is replaced by a permutation of that sequence.
- The purpose is to implement Claude Shannon's proposal to thwart cryptanalysis with *diffusion* and *confusion*.
 - **Confusion** - makes relationship between ciphertext and key as complex as possible
 - **Diffusion** – dissipates statistical structure of plaintext over bulk of ciphertext

FEISTEL CIPHER STRUCTURE

- ❑ **Block size:**
 - ❑ Larger block size → greater security
 - ❑ Larger block size → reduced encryption/decryption speed
 - ❑ Typical sizes → 64/128 bits
- ❑ **Key:**
 - ❑ Key is regenerated in each round
- ❑ **Number of rounds:**
 - ❑ Single round is not enough
 - ❑ Multiple rounds offer increasing security
 - ❑ Typical value is 16 rounds
- ❑ **Subkey generation algorithm**
 - ❑ Increasing complexity
- ❑ **Round function F**
 - ❑ Further increasing complexity



101011010101000010110101010101000100101010001101011010100010110

FEISTEL CIPHER STRUCTURE

- Formula of encryption :

$$LE_i = RE_{i-1}$$

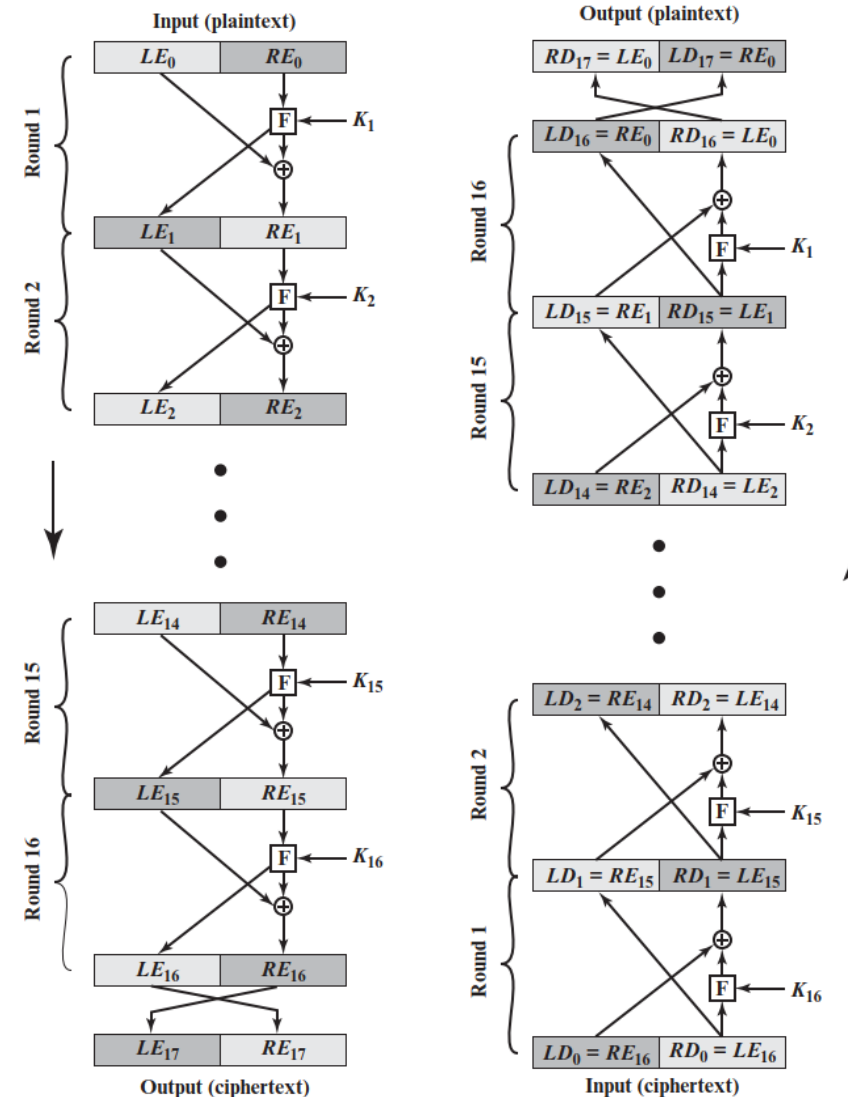
$$RE_i = LE_{i-1} \oplus F(RE_{i-1}, K_i)$$

- Formula of decryption :

$$LD_i = RD_{i-1}$$

$$RD_i = LD_{i-1} \oplus F(RD_{i-1}, K_{17-i})$$

- Encryption and decryption can share the same implementation!



1010110101010000101101011101010101010001001010100001101011010100010110

- A property of the Feistel Cipher Structure is Avalanche Effect
- A change of **one** input bit or key bit should result in changing approximately **half** of output bits!
- Making attempts to guess the key by using different Plaintext – Ciphertext pairs should be impossible

DATA ENCRYPTION STANDARD (DES)

- DES is based on the Feistel Cipher Structure
- One of the most widely used block cipher in world
- Adopted in 1977 by NIST
- Encrypts 64-bit data using 56-bit key
- DES has become widely used, especially in financial applications

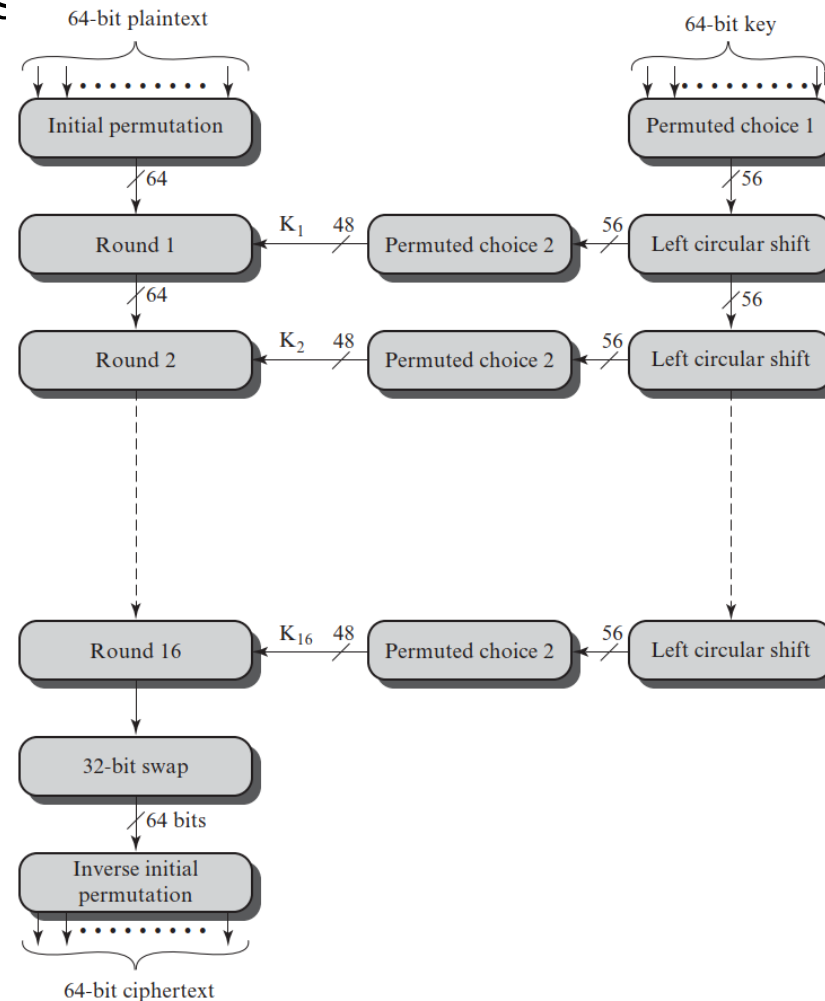
DES ENCRYPTION

Break message into 8-byte (64-bit) blocks

- Each block broken into 32-bit halves
- Initial permutation
- 16 rounds of scrambling
- Final (reverse) permutation

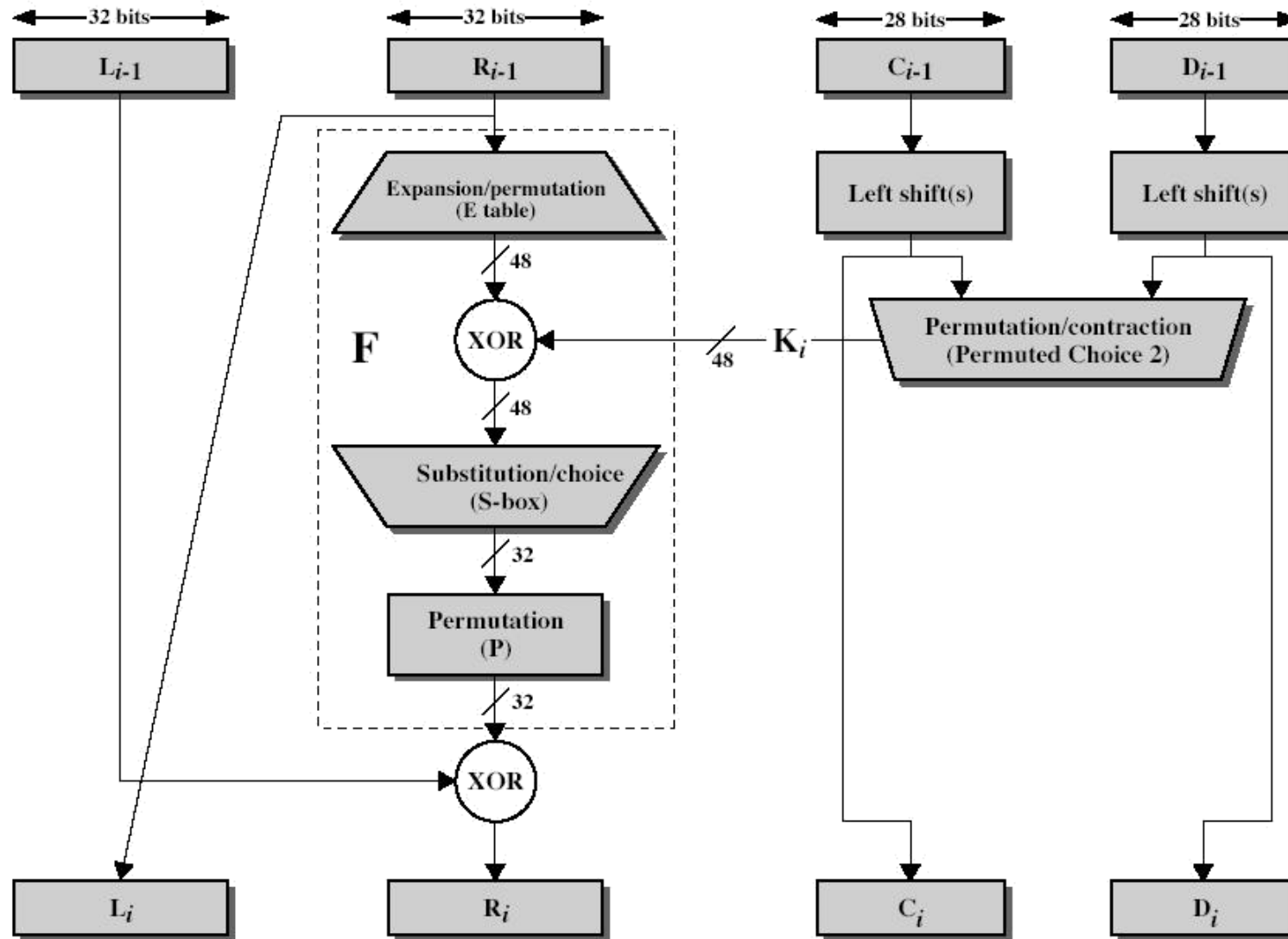
Encryption algorithm structure:

- Initial and final permutation
- Round
 - Scrambling F function
- Key schedule



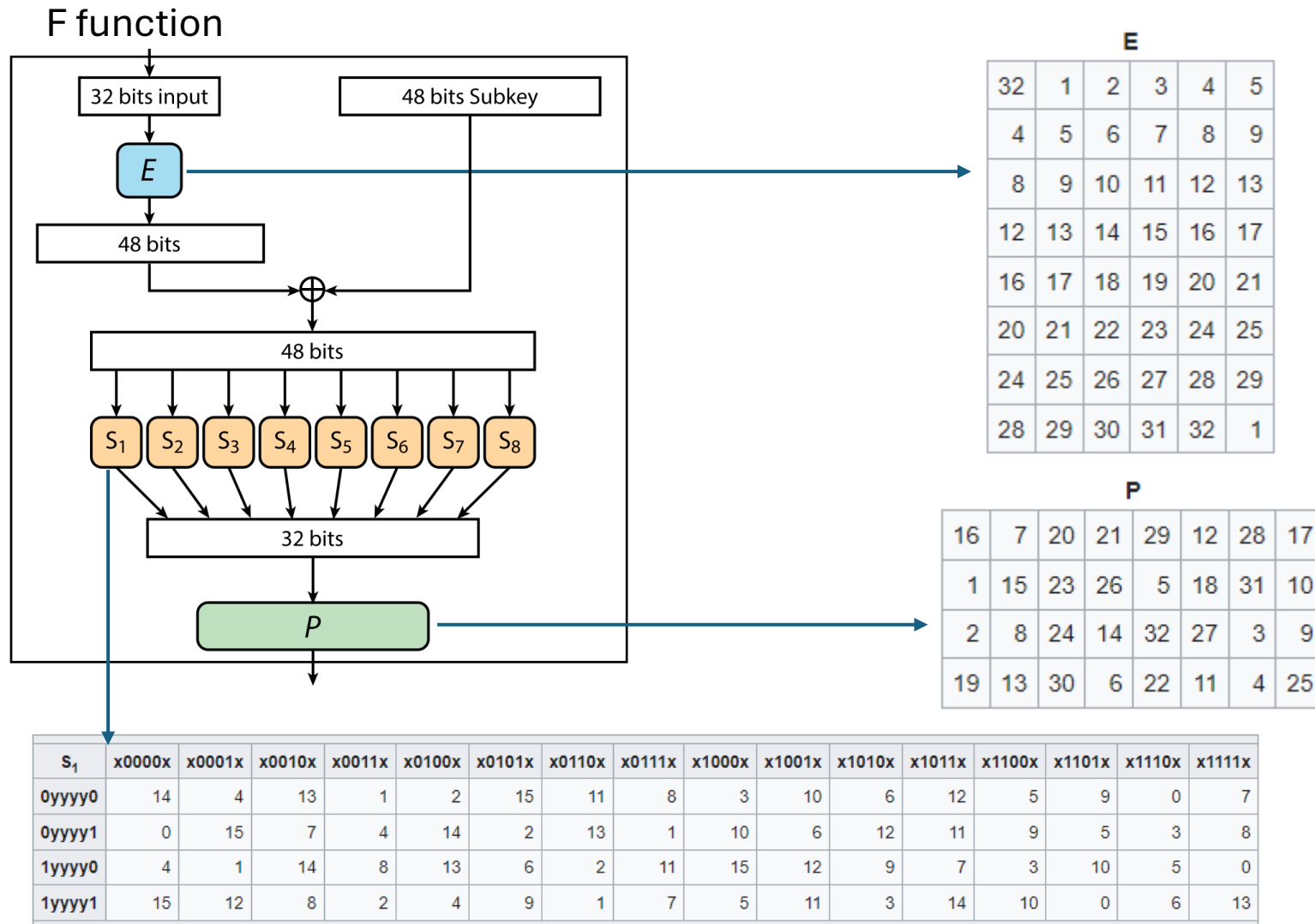
101011010100001011010101010100010010101000101101010100010110

SINGLE ROUND OF DES ALGORITHM



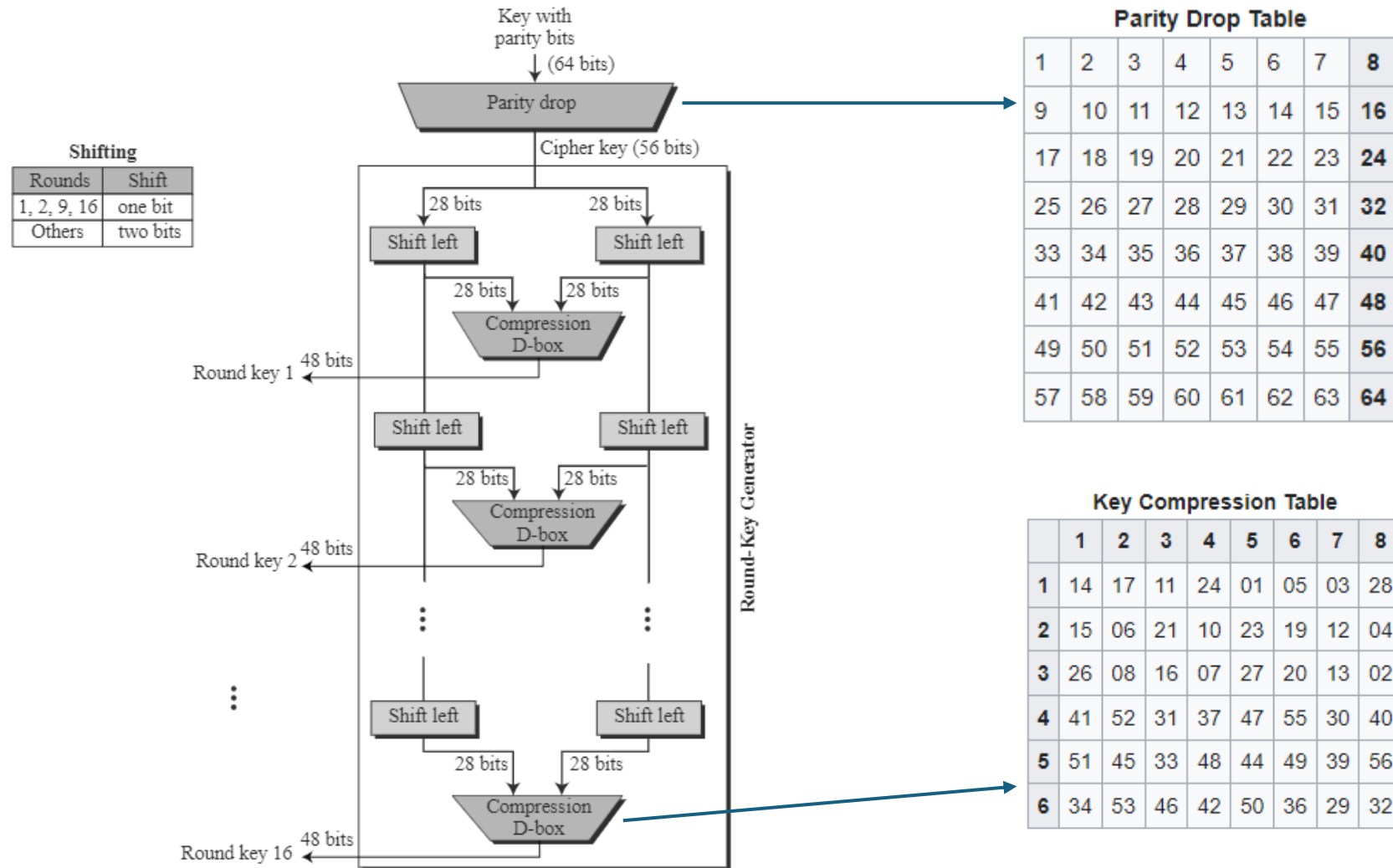
101011010101000101101010101010001001010100010101101010100010110

SINGLE ROUND OF DES ALGORITHM



10101101010100010110101110101010101000100101010001101011010100010110

DES KEY SCHEDULE



10101101010000101101010101010001001010100010101010100010110

STRENGTH OF DES

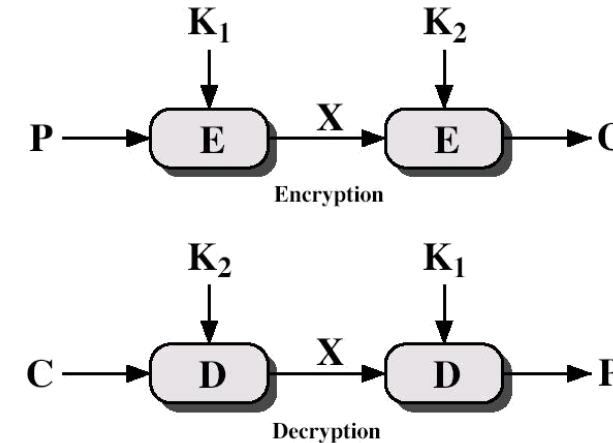
- **Time to break DES**
 - Number of keys: $2^{56} = 7.2 \times 10^{16}$ keys
 - On the *average* you need to search through 2^{55} keys (half of all possible keys must be tried to achieve success.)
 - In the worst case you need to search all 2^{56} keys
 - If you can do one encryption/decryption in 1 clock cycle @ 500 MHz
 - Time taken to check ONE key = $1/(500 \times 10^6)$ s
 - Time taken to check 2^{55} keys = $2^{55}/(500 \times 10^6)$ s = 72,057,594.04 s /3600 = 20016 hours /24 = 834 days
- The **hertz** (symbol: **Hz**) is defined as the number of [cycles per second](#) (MHz = 10^6 Hz)
- **Nowadays technology**
 - A single PC can break DES in about a year
 - If 100 PCs work in parallel, it only takes 3-4 days.

- It is necessary to design a replacement for DES, leading to two solutions:
 - Triple-DES (3DES)
 - Advanced Encryption Standard (AES)

WHY TRIPLE-DES?

- Why not Double-DES?
 - Key length = 112 bits

$$C = E_{K_2} [E_{K_1} [P]]$$



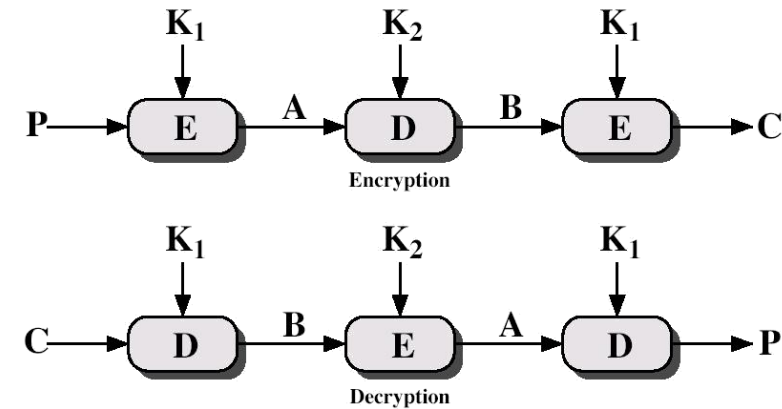
- Meet-in-the-middle attack
 - Since $X = E_{K_1} [P] = D_{K_2} [C]$
 - Attack by encrypting P with all keys and store
 - Then decrypt C with keys and match X value
 - It takes $O(2^{56})$ steps

1010110101010001011010101010100010010010101010100010110

TRIPLE-DES WITH TWO-KEYS

- Use 2 keys with E-D-E sequence
 - Key length = 112 bits

$$C = E_{K_1}[D_{K_2}[E_{K_1}[P]]]$$



- If $K_1=K_2$ then can work with single DES, no new hardware is required for single DES.
- No current known practical attacks for 2-key 3DES

101011010100001011010110101010100010010010101010100010110

ADVANCED ENCRYPTION STANDARD (AES)

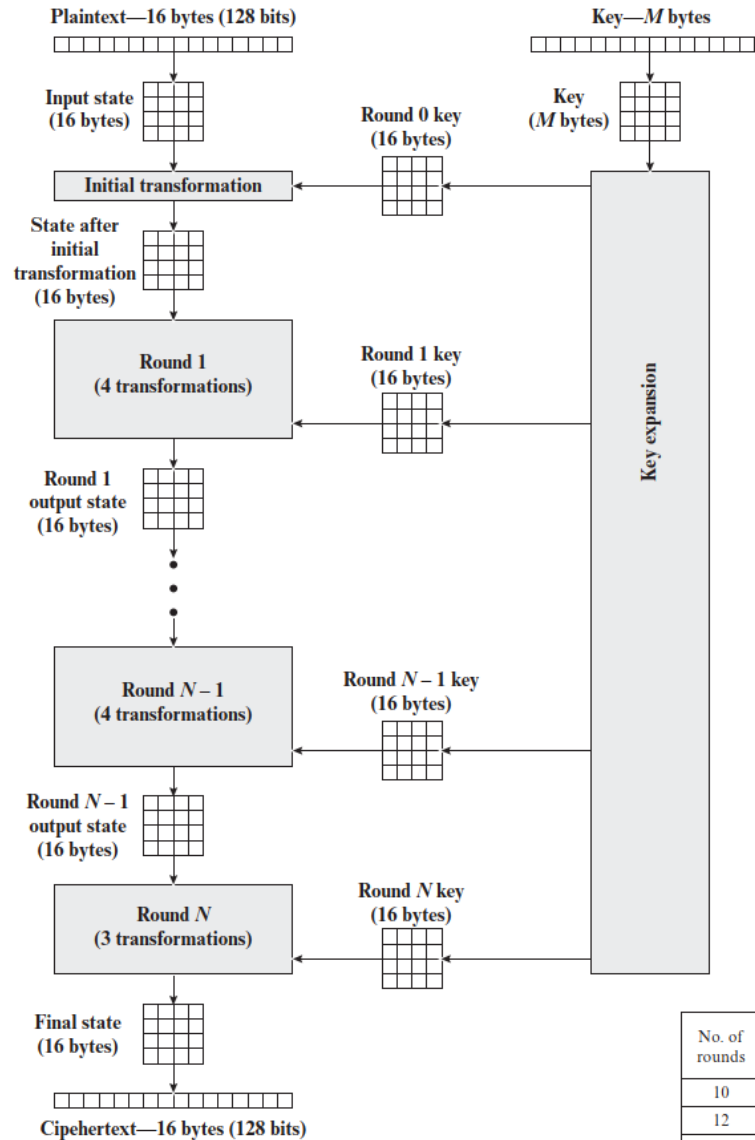
- It was clearly needed a replacement for DES
 - Theoretical attacks that can break it
 - Have demonstrated exhaustive key search attacks
- It can be used Triple-DES – but slow with small blocks
- US NIST: call for candidates for Advanced Encryption Standard (AES) in 1997
- 15 candidates accepted in Jun 98, and 5 were shortlisted 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
- Rijndael was selected as the AES in Oct-2000
- Issued as FIPS PUB 197 standard in Nov-2001

FEATURES OF AES

- Designed by Rijmen-Daemen in Belgium
- Block size: 128 bits
- Key sizes: 128/192/256 bits
- Variable rounds: 10/12/14 rounds
- Resistant against known attacks
- Speed and code compactness on many CPUs

10101101010100001010111010101010101000100100010101101010100010110

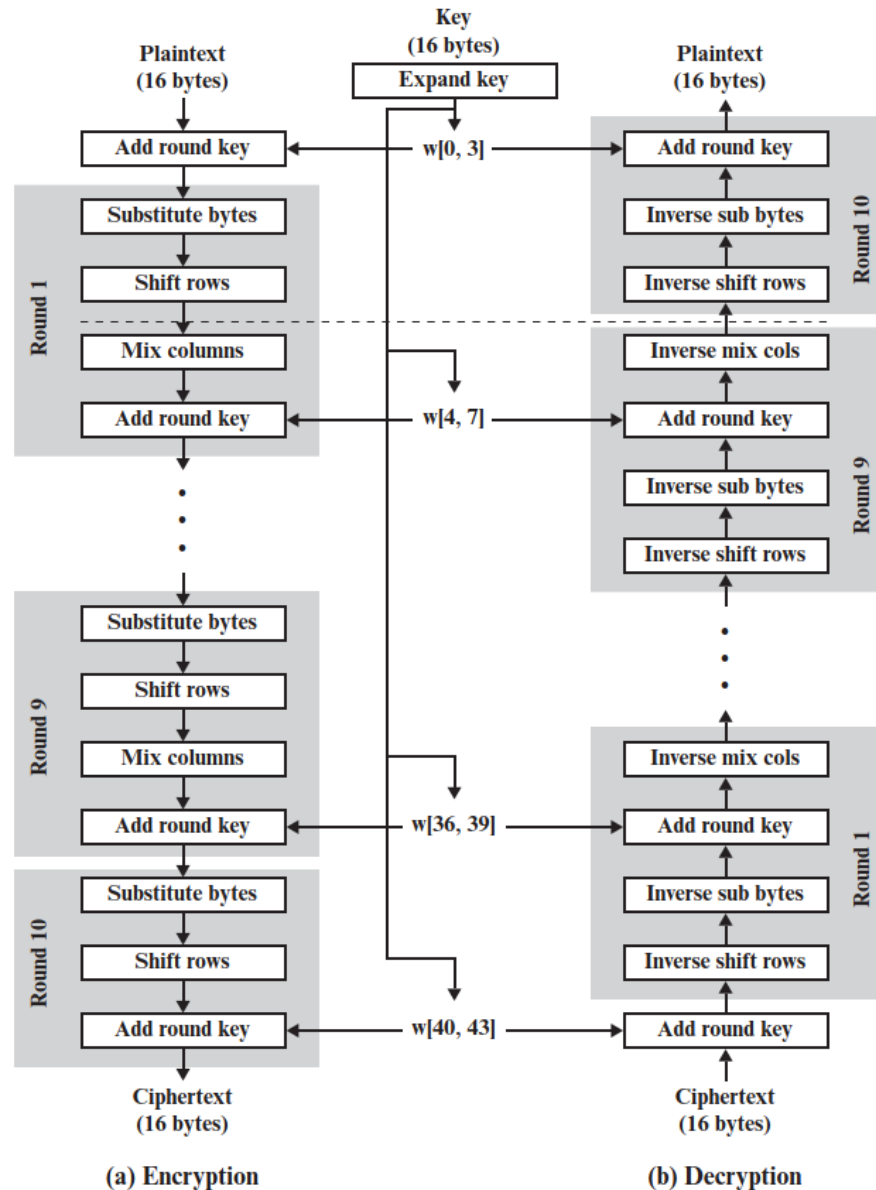
STRUCTURE OF AES



10101101010100001011010101010101000010010101010001101011010100010110

AES ENCRYPTION AND DECRYPTION

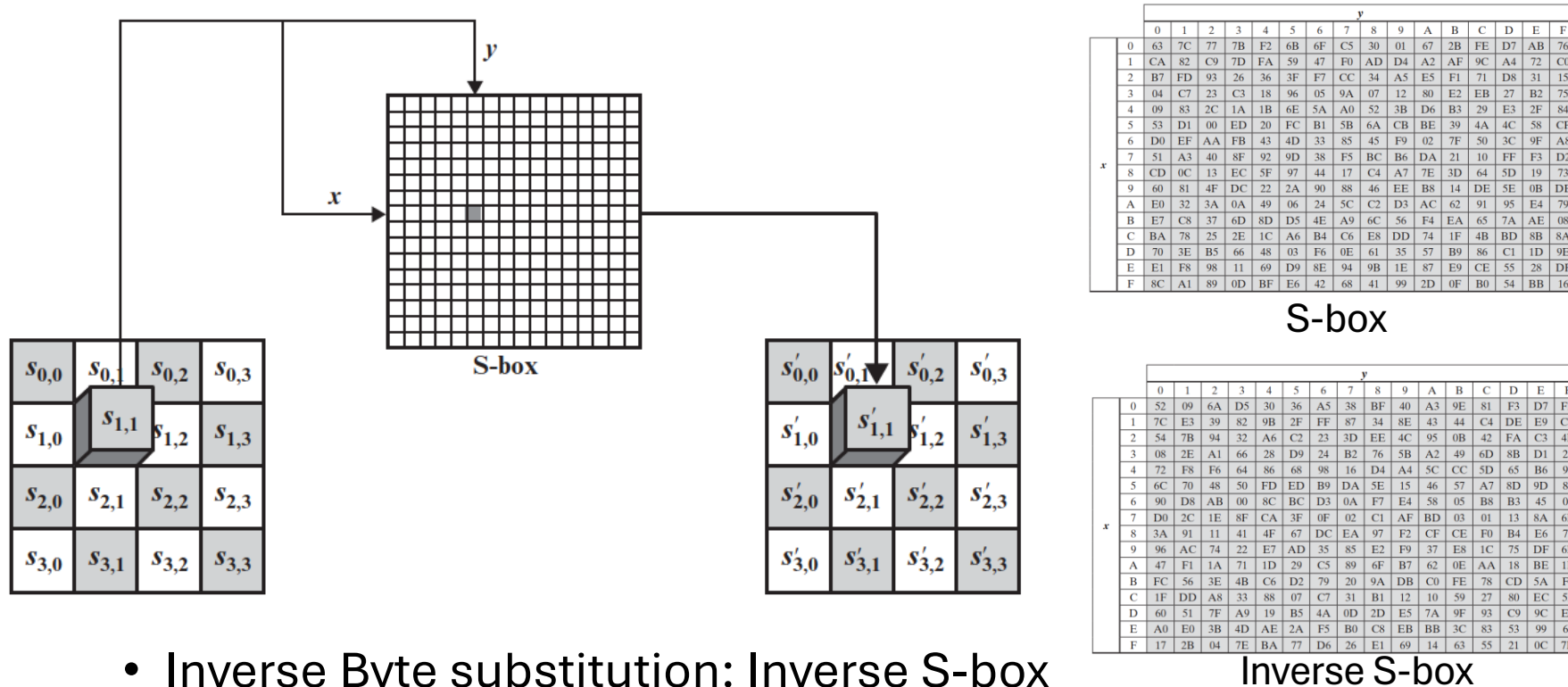
- In AES, each round is not Feistel network
- Each round has four operations:
 - Substitute
 - Shift rows
 - Mix columns
 - Add round key



10101101010000101101010101010000100100100010101101010100010110

AES ROUND (BYTE SUBSTITUTION)

- Byte substitution (1 S-box of 16x16 used on every byte)

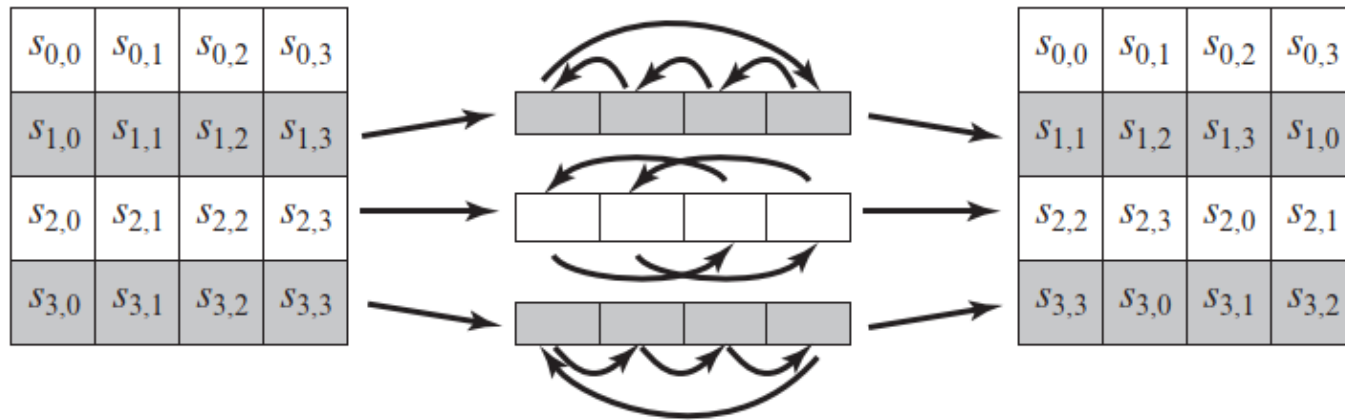


- Inverse Byte substitution: Inverse S-box
 - $IS\text{-}box(S\text{-}box(a)) = a$

1010110101000010110101101010100001001010101000010110

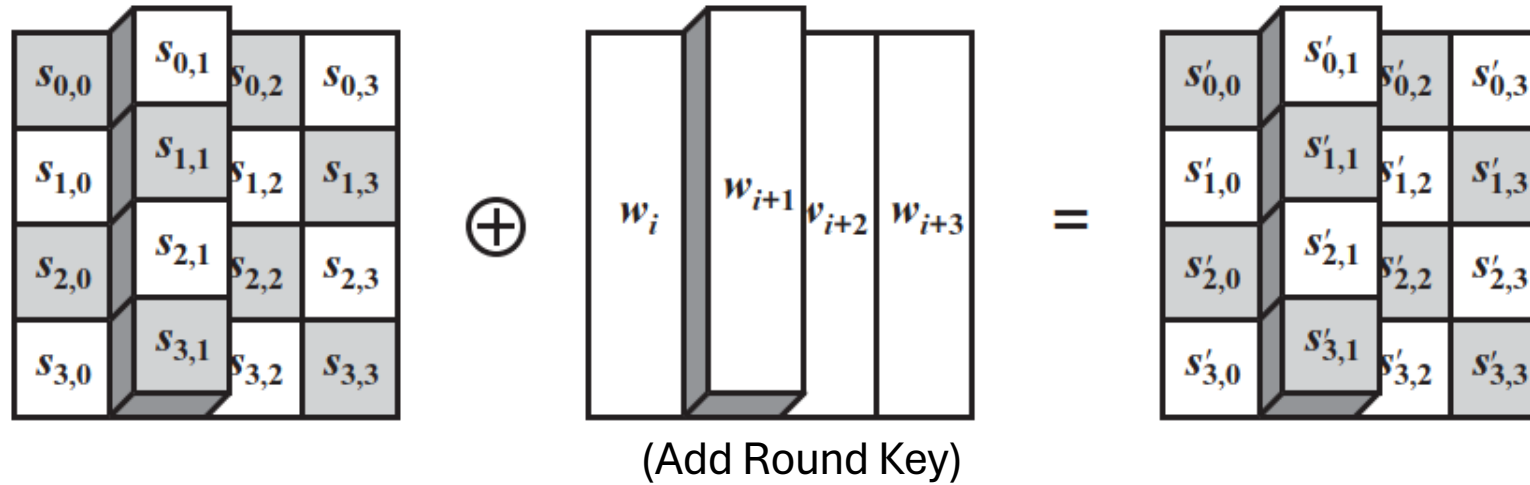
AES ROUND (SHIFT ROWS)

- Shift rows (permute bytes in each row)
 - Circular left shift



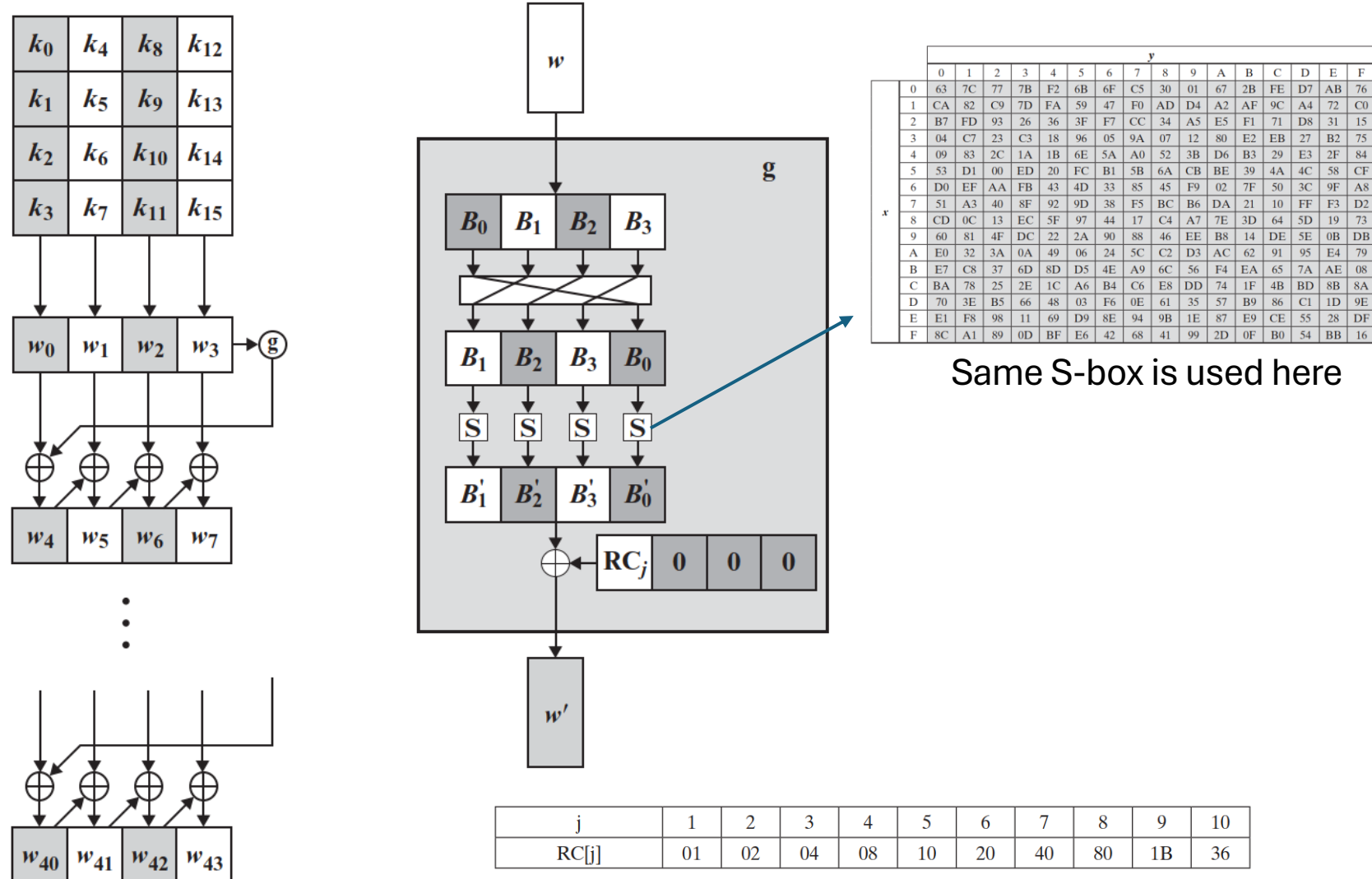
- Inverse shift rows: circular right shift

AES ROUND (ADD ROUND KEY)



101011010101000101101010101010001001010100010101101010100010110

AES KEY GENERATION



101011010100001011010101010100001001010100001010110101000010110

AVALANCHE EFFECT IN AES

Round		Number of Bits that Differ
	0123456789abcdeffedcba9876543210 0023456789abcdeffedcba9876543210	1
0	0e3634aece7225b6f26b174ed92b5588 0f3634aece7225b6f26b174ed92b5588	1
1	657470750fc7ff3fc0e8e8ca4dd02a9c c4a9ad090fc7ff3fc0e8e8ca4dd02a9c	20
2	5c7bb49a6b72349b05a2317ff46d1294 fe2ae569f7ee8bb8c1f5a2bb37ef53d5	58
3	7115262448dc747e5cdac7227da9bd9c ec093dfb7c45343d689017507d485e62	59
4	f867aee8b437a5210c24c1974cffeabc 43efdb697244df808e8d9364ee0ae6f5	61
5	721eb200ba06206dcdbd4bce704fa654e 7b28a5d5ed643287e006c099bb375302	68
6	0ad9d85689f9f77bc1c5f71185e5fb14 3bc2d8b6798d8ac4fe36a1d891ac181a	64
7	db18a8ffa16d30d5f88b08d777ba4eaa 9fb8b5452023c70280e5c4bb9e555a4b	67
8	f91b4fbfe934c9bf8f2f85812b084989 20264e1126b219aef7feb3f9b2d6de40	65
9	cca104a13e678500ff59025f3bafaa34 b56a0341b2290ba7dfd8ddcd8578205	61
10	ff0b844a0853bf7c6934ab4364148fb9 612b89398d0600cde116227ce72433f0	58

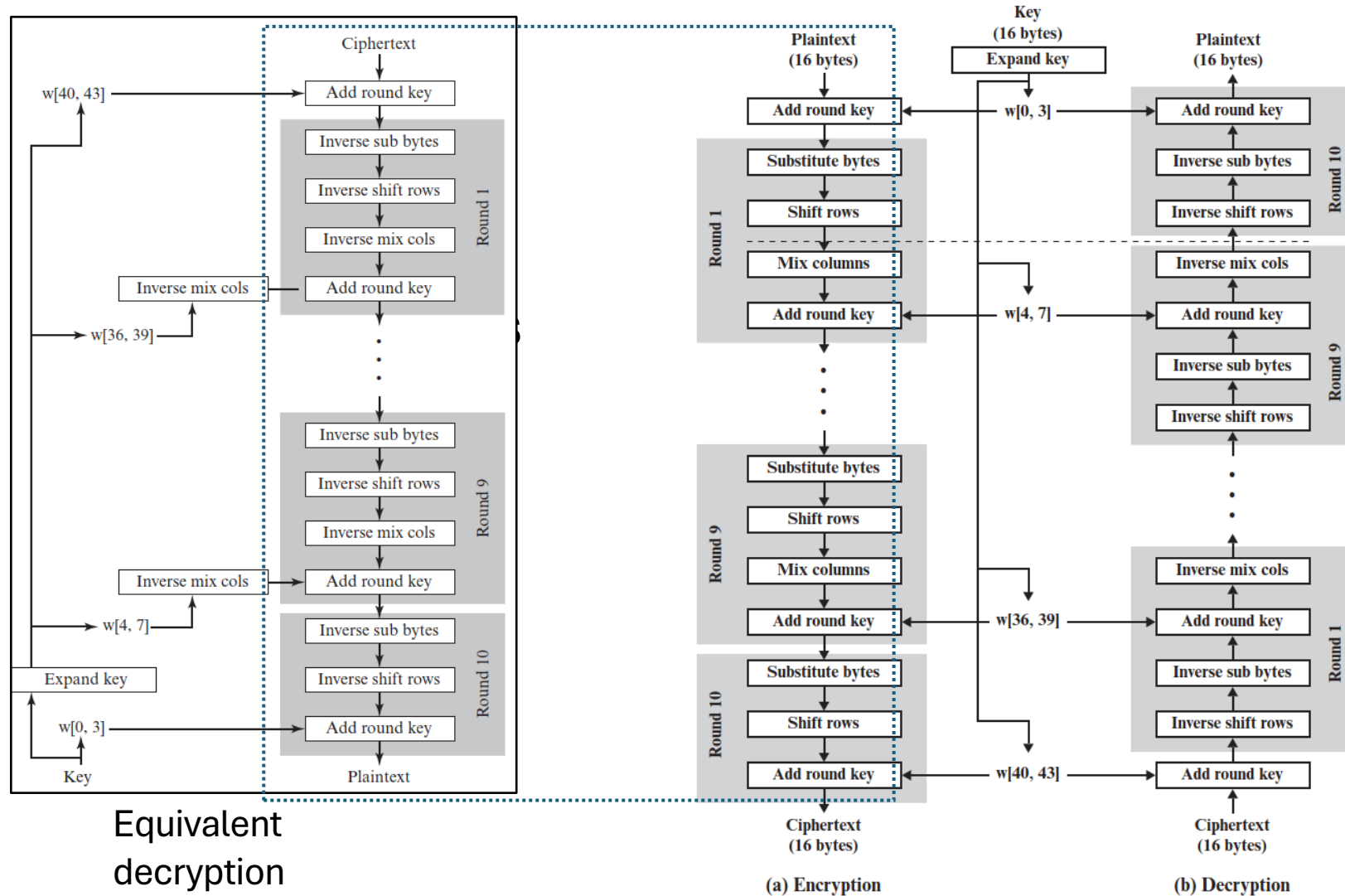
1-bit change in plaintext

Round		Number of Bits that Differ
	0123456789abcdeffedcba9876543210 0123456789abcdeffedcba9876543210	0
0	0e3634aece7225b6f26b174ed92b5588 0f3634aece7225b6f26b174ed92b5588	1
1	657470750fc7ff3fc0e8e8ca4dd02a9c c5a9ad090ec7ff3fc1e8e8ca4cd02a9c	22
2	5c7bb49a6b72349b05a2317ff46d1294 90905fa9563356d15f3760f3b8259985	58
3	7115262448dc747e5cdac7227da9bd9c 18aeb7aa794b3b66629448d575c7cebf	67
4	f867aee8b437a5210c24c1974cffeabc f81015f993c978a876ae017cb49e7eec	63
5	721eb200ba06206dcdbd4bce704fa654e 5955c91b4e769f3cb4a94768e98d5267	81
6	0ad9d85689f9f77bc1c5f71185e5fb14 dc60a24d137662181e45b8d3726b2920	70
7	db18a8ffa16d30d5f88b08d777ba4eaa fe8343b8f88bef66cab7e977d005a03c	74
8	f91b4fbfe934c9bf8f2f85812b084989 da7dad581d1725c5b72fa0f9d9d1366a	67
9	cca104a13e678500ff59025f3bafaa34 0ccb4c66bbfd912f4b511d72996345e0	59
10	ff0b844a0853bf7c6934ab4364148fb9 fc8923ee501a7d207ab670686839996b	53

1-bit change in key

10101101010000101101010101000010001000100010101010100010110

AES IMPROVEMENT FOR IMPLEMENTATION



Equivalent
decryption

(a) Encryption

(b) Decryption

1010110101010000101101010101010100010010101010001101011010100010110

BLOCK CIPHER OPERATION

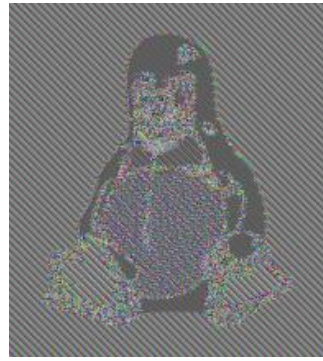
- We have discussed encryption for a single block, but the plaintext normally consists of multiblock
- There are five block cipher modes of operation:
 - Electronic Codebook (ECB)
 - Cipher Block Chaining (CBC)
 - Cipher Feedback (CFB)
 - Output Feedback (OFB)
 - Counter (CTR)

LIMITATIONS OF ECB

- Limitations
 - If the same block of plaintext appears more than once in the message, it always produces the same ciphertext.
 - Weakness due to encrypted message blocks being independent



Original



ECB



No ECB

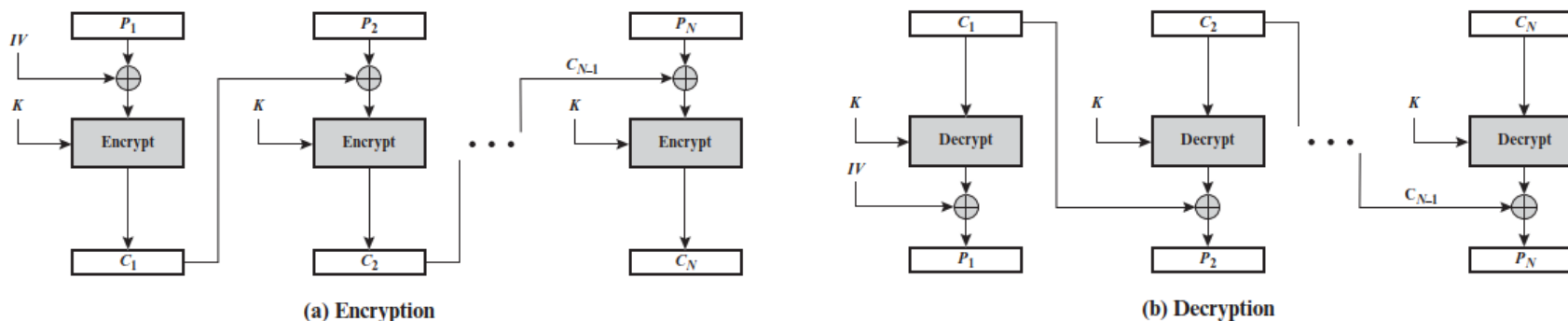
CIPHER BLOCK CHAINING (CBC)

- Message is broken into blocks
- But these are linked together in the encryption operation
- Each previous cipher blocks is chained with current plaintext block
- Use Initial Vector (IV) to start process

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

$$C_{-1} = IV$$

- CBC is used for bulk data encryption, authentication



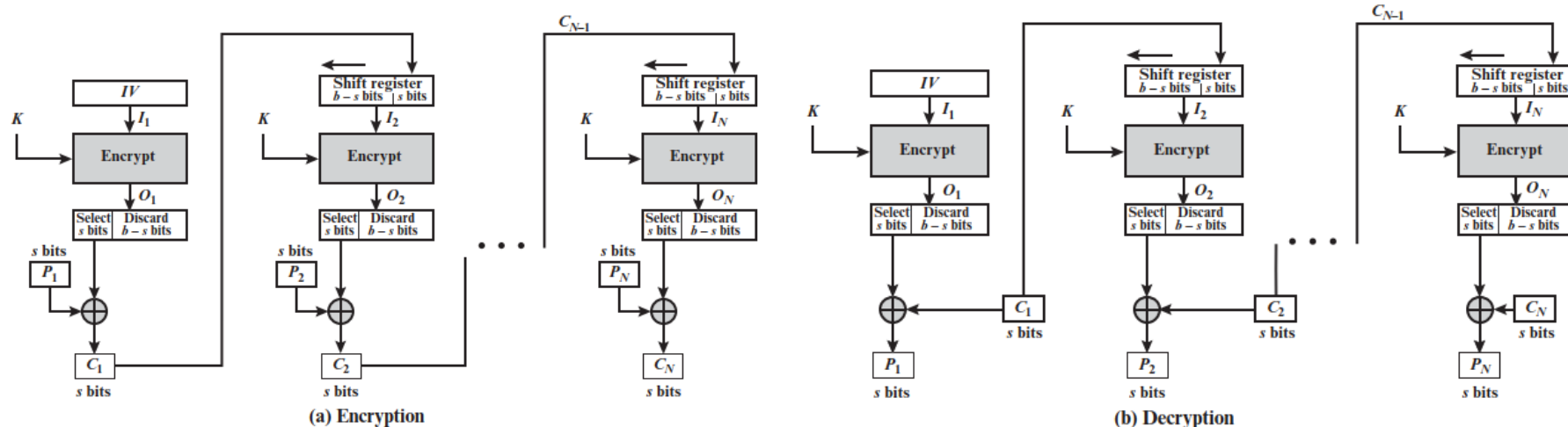
1010110101000010110101110101010101000100101010000110101101010100010110

CIPHER FEEDBACK (CFB)

- Message is treated as a stream of bits
- Result is feedback for next stage
- Standard allows any number of bit (1,8 or 64 or whatever) to be fed back, namely CFB-1, CFB-8, CFB-64, etc
- A common value is s=8 (CFB-8)

$$C_i = P_i \oplus S_s(E_K(C_{i-1})) \quad , \quad S_s(x) \text{ are the "s" bits of } x$$

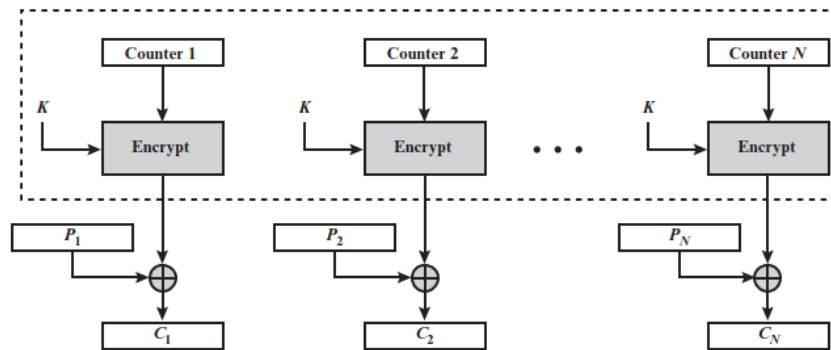
$$C_{-1} = IV$$



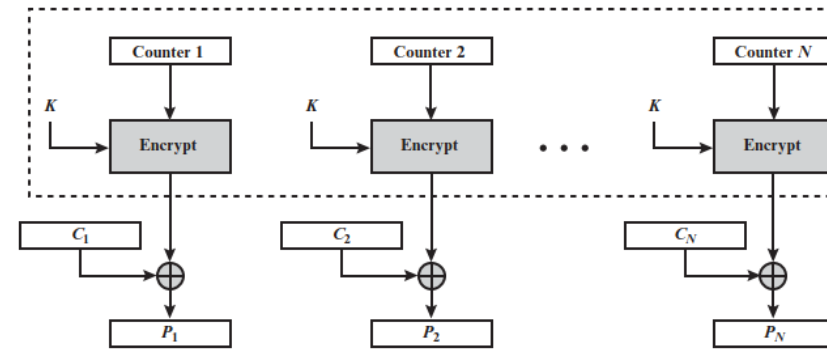
COUNTER (CTR)

- A “new” mode, though proposed early on
- Similar to output feedback but encrypts counter value rather than any feedback value
- Must have a different key & counter value for every plaintext block (never reused)

$$C_i = P_i \oplus O_i, \quad O_i = E_K(\text{Counter} + i - 1)$$



(a) Encryption



(b) Decryption

10101101010000101101010101010001001001000110101101010100010110

- Laboratory_01: Python Encryption AES
- Laboratory_02: DES encryption using OpenSSL
- Laboratory_03: AES encryption using OpenSSL