# Information Security

**MCA- III, Department of Computer Science**

# Vigenere Cipher

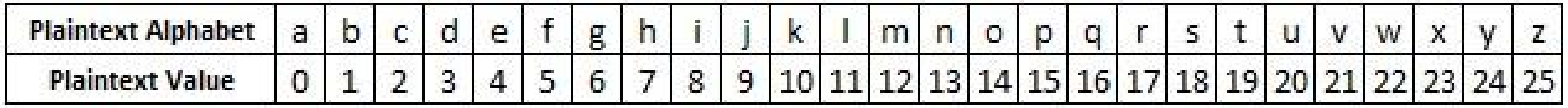
- Let letters A-Z are taken to be number 0-25.
- Let $P = \{P_1, P_2, P_3, . . , P_n | P_i \in \{A, . . , Z\}\}$ and $K = \{K_1, K_2, K_3, \ldots, K_m | K_i \in \{A, . . , Z\}\}$ are the plaintext and key respectively. The Vigenere Cipher can be defined algebraically
- Encryption $C_i = E_k(P_i) = (P_i + K_{(i \, mod \, m)}) \, mod \, 26$
- Decryption $P_i = D_k(C_i) = (C_i - K_{(i \, mod \, m)}) \, mod \, 26$

# Vigenere Cipher Example:

Plaintext: ATTACKATDAWN = {0, 19, 19,0,2,10,0,19, 3,0,22,13}

Key: LEMON = {11, 4, 12, 13, 14}

| Plaintext (P) | A | T | T | A | C | K | A | T | D | A | W | N |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 0 | 19 | 19 | 0 | 2 | 10 | 0 | 19 | 3 | 0 | 22 | 13 |
| Key(K) | 11 | 4 | 12 | 13 | 14 | 11 | 4 | 12 | 13 | 14 | 11 | 4 |
| $(P_i + K_{(i \bmod m)}) \bmod 26$ | 11 | 23 | 5 | 13 | 16 | 21 | 4 | 5 | 16 | 14 | 7 | 17 |
| Cyphertext (C) | L | X | F | O | P | V | E | F | R | N | H | R |



| Plaintext Alphabet | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Plaintext Value | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

# Vigenere Cipher

- Plaintext:

  ATTACKATDAWN

- Key:

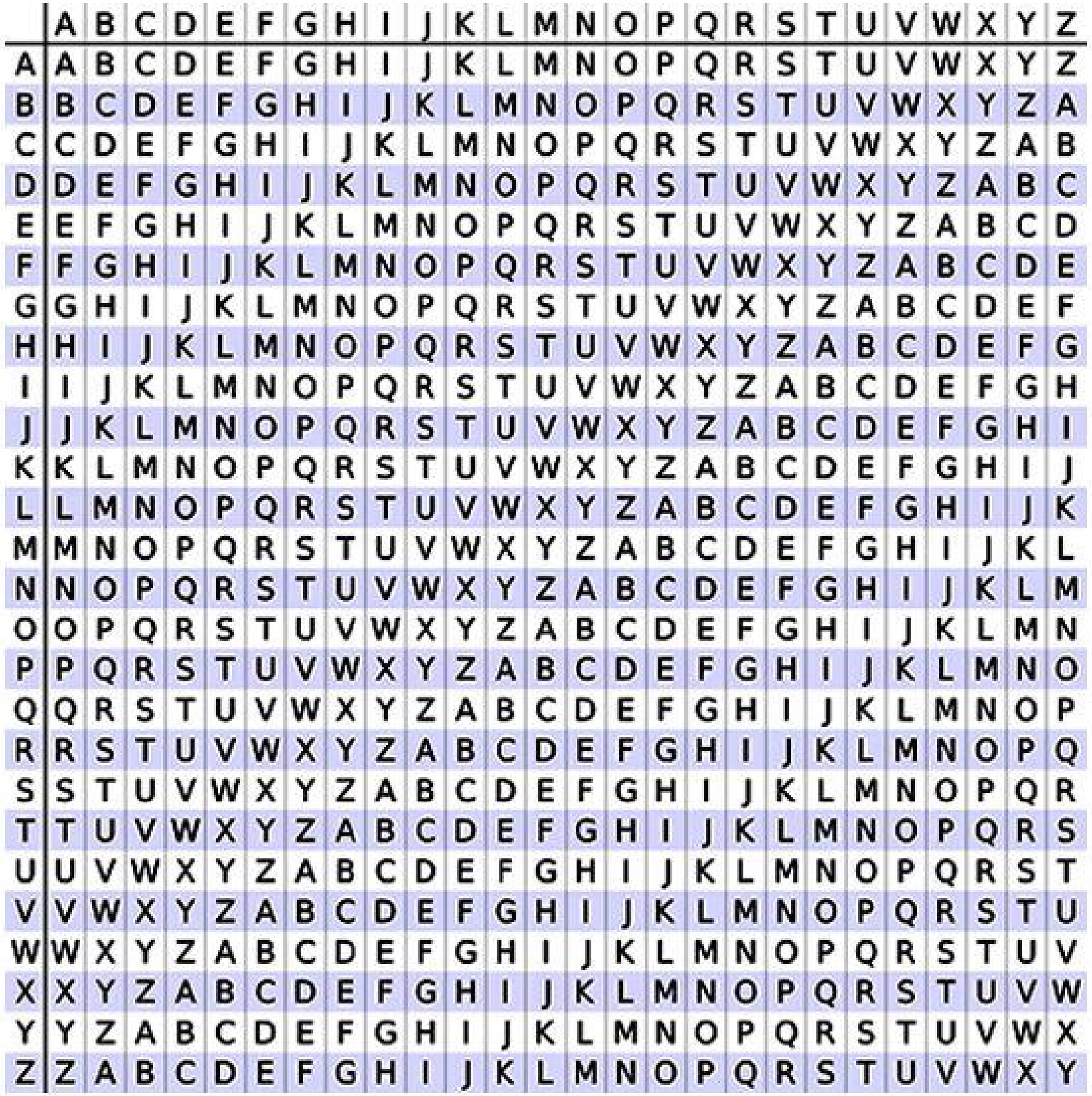
  LEMON

- Keystream:

  LEMONLEMONLE

- Ciphertext:

  LXFOPVEFRNHR



| | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| B | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A |
| C | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B |
| D | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C |
| E | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D |
| F | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E |
| G | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F |
| H | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G |
| I | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H |
| J | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I |
| K | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J |
| L | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K |
| M | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L |
| N | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M |
| O | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N |
| P | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O |
| Q | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P |
| R | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q |
| S | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R |
| T | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S |
| U | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T |
| V | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U |
| W | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V |
| X | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W |
| Y | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X |
| Z | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y |

# Hill Cipher

- Invented by Lester S. Hill in 1929, the Hill cipher is a polyaphabetic substitution cipher based on linear algebra. it can work on digraphs, trigraphs (3 letter blocks) or theoretically any sized blocks.
- The Plaintext is divided into equal size blocks.
- The blocks are encrypted one at a time in such a way that each chracter in the block contributes contributes to the encryption of other chracters in the block.
- Hill Ciphers belongs to the category of **Block Ciphers.**

Encryption: $c = Kp \pmod{26}$

Decryption: $p = K^{-1}c \pmod{26}$

– plaintext : $p \in \{0,1,2,3, .... 25\}$

– ciphertext : $c \in \{0,1,2,3, .... 25\}$

– key : K is an invertible matrix

# Example:

- Encrypt: “shortexample’ with key HILL
- Key  k: **Hill** $\begin{pmatrix} H & I \\ L & L \end{pmatrix}$ $\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix}$
- Plaintext: Short Example

$$\begin{pmatrix} s \\ h \end{pmatrix}\begin{pmatrix} o \\ r \end{pmatrix}\begin{pmatrix} t \\ e \end{pmatrix}\begin{pmatrix} x \\ a \end{pmatrix}\begin{pmatrix} m \\ p \end{pmatrix}\begin{pmatrix} l \\ e \end{pmatrix} \qquad \begin{pmatrix} 18 \\ 7 \end{pmatrix}\begin{pmatrix} 14 \\ 17 \end{pmatrix}\begin{pmatrix} 19 \\ 4 \end{pmatrix}\begin{pmatrix} 23 \\ 0 \end{pmatrix}\begin{pmatrix} 12 \\ 15 \end{pmatrix}\begin{pmatrix} 11 \\ 4 \end{pmatrix}$$

- Encryption:

$$\begin{pmatrix} H & I \\ L & L \end{pmatrix}\begin{pmatrix} s \\ h \end{pmatrix} = \begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix}\begin{pmatrix} 18 \\ 7 \end{pmatrix} = \begin{pmatrix} 182 \\ 275 \end{pmatrix} = \begin{pmatrix} 0 \\ 15 \end{pmatrix} \mathit{mod}\ 26 = \begin{pmatrix} A \\ P \end{pmatrix}$$

- Ciphertext of "APADJ TFTWLFJ".
- Similarly do for rest vectors.

# Example conti..

- To decrypt a ciphertext encoded using the Hill Cipher, we must find the inverse matrix.
- General method to calculate the inverse key matrix. $K^{-1} = d^{-1} \times adj(K)$
- K= $\begin{pmatrix} H & I \\ L & L \end{pmatrix}$ $\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix}$
- The determinant of the key matrix. $\begin{vmatrix} 7 & 8 \\ 11 & 11 \end{vmatrix} = 7 \times 11 - 8 \times 11 = -11 = 15 \; mod \; 26$

- Multiplicative inverse of the determinant working modulo 26.

$$dd^{-1} = 1 \; mod \; 26 \qquad 15 \times x = 1 \; mod \; 26 \qquad 15 \times 7 = 105 \; = 1 \; mod \; 26$$

- Find the adjoint matrix in module 26

$$adj \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \qquad adj \begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix} = \begin{pmatrix} 11 & -8 \\ -11 & 7 \end{pmatrix} = \begin{pmatrix} 11 & 18 \\ 15 & 7 \end{pmatrix}$$

- $K^{-1}$ :

$$7 \times \begin{pmatrix} 11 & 18 \\ 15 & 7 \end{pmatrix} = \begin{pmatrix} 77 & 126 \\ 105 & 49 \end{pmatrix} = \begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix} \; mod \; 26 \qquad if \; K = \begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix}, then \; K^{-1} = \begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix}$$

# Encryption

$$\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix}\begin{pmatrix} 18 \\ 7 \end{pmatrix}$$

$$7 \times 18 + 8 \times 7 = 182$$

$$11 \times 18 + 11 \times 7 = 275$$

$$\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix}\begin{pmatrix} 18 \\ 7 \end{pmatrix} = \begin{pmatrix} 182 \\ 275 \end{pmatrix}$$

$$\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix}\begin{pmatrix} 18 \\ 7 \end{pmatrix} = \begin{pmatrix} 182 \\ 275 \end{pmatrix} = \begin{pmatrix} 0 \\ 15 \end{pmatrix} \mathit{mod}\ 26$$

$$\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix}\begin{pmatrix} 14 \\ 17 \end{pmatrix}$$

$$7 \times 14 + 8 \times 17 = 234$$

$$11 \times 14 + 11 \times 17 = 341$$

$$\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix}\begin{pmatrix} 14 \\ 17 \end{pmatrix} = \begin{pmatrix} 234 \\ 341 \end{pmatrix}$$

$$\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix}\begin{pmatrix} 14 \\ 17 \end{pmatrix} = \begin{pmatrix} 234 \\ 341 \end{pmatrix} = \begin{pmatrix} 0 \\ 3 \end{pmatrix} \mathit{mod}\ 26$$

$$\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix}\begin{pmatrix} 19 \\ 4 \end{pmatrix}$$

$$7 \times 19 + 8 \times 4 = 165$$

$$11 \times 19 + 11 \times 4 = 253$$

$$\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix}\begin{pmatrix} 19 \\ 4 \end{pmatrix} = \begin{pmatrix} 165 \\ 253 \end{pmatrix}$$

$$\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix}\begin{pmatrix} 19 \\ 4 \end{pmatrix} = \begin{pmatrix} 165 \\ 253 \end{pmatrix} = \begin{pmatrix} 9 \\ 19 \end{pmatrix} \mathit{mod}\ 26$$

$$\begin{pmatrix} H & I \\ L & L \end{pmatrix}\begin{pmatrix} s \\ h \end{pmatrix} = \begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix}\begin{pmatrix} 18 \\ 7 \end{pmatrix} = \begin{pmatrix} 182 \\ 275 \end{pmatrix} = \begin{pmatrix} 0 \\ 15 \end{pmatrix} \mathit{mod}\ 26 = \begin{pmatrix} A \\ P \end{pmatrix}$$

$$\begin{pmatrix} H & I \\ L & L \end{pmatrix}\begin{pmatrix} o \\ r \end{pmatrix} = \begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix}\begin{pmatrix} 14 \\ 17 \end{pmatrix} = \begin{pmatrix} 234 \\ 341 \end{pmatrix} = \begin{pmatrix} 0 \\ 3 \end{pmatrix} \mathit{mod}\ 26 = \begin{pmatrix} A \\ D \end{pmatrix}$$

$$\begin{pmatrix} H & I \\ L & L \end{pmatrix}\begin{pmatrix} t \\ e \end{pmatrix} = \begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix}\begin{pmatrix} 19 \\ 4 \end{pmatrix} = \begin{pmatrix} 165 \\ 253 \end{pmatrix} = \begin{pmatrix} 9 \\ 19 \end{pmatrix} \mathit{mod}\ 26 = \begin{pmatrix} J \\ T \end{pmatrix}$$

$$\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix}\begin{pmatrix} 23 \\ 0 \end{pmatrix}$$

$$7 \times 23 + 8 \times 0 = 161$$

$$11 \times 23 + 11 \times 0 = 253$$

$$\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix}\begin{pmatrix} 23 \\ 0 \end{pmatrix} = \begin{pmatrix} 161 \\ 253 \end{pmatrix}$$

$$\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix}\begin{pmatrix} 23 \\ 0 \end{pmatrix} = \begin{pmatrix} 161 \\ 253 \end{pmatrix} = \begin{pmatrix} 5 \\ 19 \end{pmatrix} \mathit{mod}\ 26$$

$$\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix}\begin{pmatrix} 12 \\ 15 \end{pmatrix}$$

$$7 \times 12 + 8 \times 15 = 204$$

$$11 \times 12 + 11 \times 15 = 297$$

$$\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix}\begin{pmatrix} 12 \\ 15 \end{pmatrix} = \begin{pmatrix} 204 \\ 297 \end{pmatrix}$$

$$\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix}\begin{pmatrix} 12 \\ 15 \end{pmatrix} = \begin{pmatrix} 204 \\ 297 \end{pmatrix} = \begin{pmatrix} 22 \\ 11 \end{pmatrix} \mathit{mod}\ 26$$

$$\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix}\begin{pmatrix} 11 \\ 4 \end{pmatrix}$$

$$7 \times 11 + 8 \times 4 = 109$$

$$11 \times 11 + 11 \times 4 = 165$$

$$\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix}\begin{pmatrix} 11 \\ 4 \end{pmatrix} = \begin{pmatrix} 109 \\ 165 \end{pmatrix}$$

$$\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix}\begin{pmatrix} 11 \\ 4 \end{pmatrix} = \begin{pmatrix} 109 \\ 165 \end{pmatrix} = \begin{pmatrix} 5 \\ 9 \end{pmatrix} \mathit{mod}\ 26$$

$$\begin{pmatrix} H & I \\ L & L \end{pmatrix}\begin{pmatrix} x \\ a \end{pmatrix} = \begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix}\begin{pmatrix} 23 \\ 0 \end{pmatrix} = \begin{pmatrix} 161 \\ 253 \end{pmatrix} = \begin{pmatrix} 5 \\ 19 \end{pmatrix} \mathit{mod}\ 26 = \begin{pmatrix} F \\ T \end{pmatrix}$$

$$\begin{pmatrix} H & I \\ L & L \end{pmatrix}\begin{pmatrix} m \\ p \end{pmatrix} = \begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix}\begin{pmatrix} 12 \\ 15 \end{pmatrix} = \begin{pmatrix} 204 \\ 297 \end{pmatrix} = \begin{pmatrix} 22 \\ 11 \end{pmatrix} \mathit{mod}\ 26 = \begin{pmatrix} W \\ L \end{pmatrix}$$

$$\begin{pmatrix} H & I \\ L & L \end{pmatrix}\begin{pmatrix} l \\ e \end{pmatrix} = \begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix}\begin{pmatrix} 11 \\ 4 \end{pmatrix} = \begin{pmatrix} 109 \\ 165 \end{pmatrix} = \begin{pmatrix} 5 \\ 9 \end{pmatrix} \mathit{mod}\ 26 = \begin{pmatrix} F \\ J \end{pmatrix}$$

# Decryption

ciphertext is "APADJ TFTWLFJ".

$$\begin{aligned}\begin{pmatrix}25 & 22\\ 1 & 23\end{pmatrix}\begin{pmatrix}A\\ P\end{pmatrix} &= \begin{pmatrix}25 & 22\\ 1 & 23\end{pmatrix}\begin{pmatrix}0\\ 15\end{pmatrix}\\ &= \begin{pmatrix}25\times 0+22\times 15\\ 1\times 0+23\times 15\end{pmatrix}\\ &= \begin{pmatrix}330\\ 345\end{pmatrix}\\ &= \begin{pmatrix}18\\ 7\end{pmatrix}\ mod\ 26\\ &= \begin{pmatrix}s\\ h\end{pmatrix}\end{aligned}$$

$$\begin{aligned}\begin{pmatrix}25 & 22\\ 1 & 23\end{pmatrix}\begin{pmatrix}A\\ D\end{pmatrix} &= \begin{pmatrix}25 & 22\\ 1 & 23\end{pmatrix}\begin{pmatrix}0\\ 3\end{pmatrix}\\ &= \begin{pmatrix}25\times 0+22\times 3\\ 1\times 0+23\times 3\end{pmatrix}\\ &= \begin{pmatrix}66\\ 69\end{pmatrix}\\ &= \begin{pmatrix}14\\ 17\end{pmatrix}\ mod\ 26\\ &= \begin{pmatrix}o\\ r\end{pmatrix}\end{aligned}$$

$$\begin{aligned}\begin{pmatrix}25 & 22\\ 1 & 23\end{pmatrix}\begin{pmatrix}J\\ T\end{pmatrix} &= \begin{pmatrix}25 & 22\\ 1 & 23\end{pmatrix}\begin{pmatrix}9\\ 19\end{pmatrix}\\ &= \begin{pmatrix}25\times 9+22\times 19\\ 1\times 9+23\times 19\end{pmatrix}\\ &= \begin{pmatrix}643\\ 446\end{pmatrix}\\ &= \begin{pmatrix}19\\ 4\end{pmatrix}\ mod\ 26\\ &= \begin{pmatrix}t\\ e\end{pmatrix}\end{aligned}$$

$$\begin{aligned}\begin{pmatrix}25 & 22\\ 1 & 23\end{pmatrix}\begin{pmatrix}F\\ T\end{pmatrix} &= \begin{pmatrix}25 & 22\\ 1 & 23\end{pmatrix}\begin{pmatrix}5\\ 19\end{pmatrix}\\ &= \begin{pmatrix}25\times 5+22\times 19\\ 1\times 5+23\times 19\end{pmatrix}\\ &= \begin{pmatrix}543\\ 442\end{pmatrix}\\ &= \begin{pmatrix}23\\ 0\end{pmatrix}\ mod\ 26\\ &= \begin{pmatrix}x\\ a\end{pmatrix}\end{aligned}$$

$$\begin{aligned}\begin{pmatrix}25 & 22\\ 1 & 23\end{pmatrix}\begin{pmatrix}W\\ L\end{pmatrix} &= \begin{pmatrix}25 & 22\\ 1 & 23\end{pmatrix}\begin{pmatrix}22\\ 11\end{pmatrix}\\ &= \begin{pmatrix}25\times 22+22\times 11\\ 1\times 22+23\times 11\end{pmatrix}\\ &= \begin{pmatrix}792\\ 275\end{pmatrix}\\ &= \begin{pmatrix}12\\ 15\end{pmatrix}\ mod\ 26\\ &= \begin{pmatrix}m\\ p\end{pmatrix}\end{aligned}$$

$$\begin{aligned}\begin{pmatrix}25 & 22\\ 1 & 23\end{pmatrix}\begin{pmatrix}F\\ J\end{pmatrix} &= \begin{pmatrix}25 & 22\\ 1 & 23\end{pmatrix}\begin{pmatrix}5\\ 9\end{pmatrix}\\ &= \begin{pmatrix}25\times 5+22\times 9\\ 1\times 5+23\times 9\end{pmatrix}\\ &= \begin{pmatrix}323\\ 212\end{pmatrix}\\ &= \begin{pmatrix}11\\ 4\end{pmatrix}\ mod\ 26\\ &= \begin{pmatrix}l\\ e\end{pmatrix}\end{aligned}$$

# 3x3 Example - Encryption

- Key phrase “BACKUP” into a matrix. key phrase is a few letters short, Use A, B, C.

$$\begin{pmatrix} B & A & C \\ K & U & P \\ A & B & C \end{pmatrix} \qquad \begin{pmatrix} 1 & 0 & 2 \\ 10 & 20 & 15 \\ 0 & 1 & 2 \end{pmatrix}$$

- Encrypt "retreat now" using the key phrase *back up* and a 3 x 3 matrix. Use some nulls x, x to make the plaintext the right length.

$$\begin{pmatrix} r \\ e \\ t \end{pmatrix}\begin{pmatrix} r \\ e \\ a \end{pmatrix}\begin{pmatrix} t \\ n \\ o \end{pmatrix}\begin{pmatrix} w \\ x \\ x \end{pmatrix} \qquad \begin{pmatrix} 17 \\ 4 \\ 19 \end{pmatrix}\begin{pmatrix} 17 \\ 4 \\ 0 \end{pmatrix}\begin{pmatrix} 19 \\ 13 \\ 14 \end{pmatrix}\begin{pmatrix} 22 \\ 23 \\ 23 \end{pmatrix}$$

- We perform all the matrix multiplcations, and take the column vectors modulo 26.

$$\begin{aligned}\begin{pmatrix} B & A & C \\ K & U & P \\ A & B & C \end{pmatrix}\begin{pmatrix} r \\ e \\ t \end{pmatrix} &= \begin{pmatrix} 1 & 0 & 2 \\ 10 & 20 & 15 \\ 0 & 1 & 2 \end{pmatrix}\begin{pmatrix} 17 \\ 4 \\ 19 \end{pmatrix} \\ &= \begin{pmatrix} 1 \times 17 + 0 \times 4 + 2 \times 19 \\ 10 \times 17 + 20 \times 4 + 15 \times 19 \\ 0 \times 17 + 1 \times 4 + 2 \times 19 \end{pmatrix} \\ &= \begin{pmatrix} 55 \\ 535 \\ 42 \end{pmatrix} \\ &= \begin{pmatrix} 3 \\ 15 \\ 16 \end{pmatrix} \mathit{mod}\ 26 \\ &= \begin{pmatrix} D \\ P \\ Q \end{pmatrix}\end{aligned}$$

$$\begin{aligned}\begin{pmatrix} B & A & C \\ K & U & P \\ A & B & C \end{pmatrix}\begin{pmatrix} r \\ e \\ a \end{pmatrix} &= \begin{pmatrix} 1 & 0 & 2 \\ 10 & 20 & 15 \\ 0 & 1 & 2 \end{pmatrix}\begin{pmatrix} 17 \\ 4 \\ 0 \end{pmatrix} \\ &= \begin{pmatrix} 1 \times 17 + 0 \times 4 + 2 \times 0 \\ 10 \times 17 + 20 \times 4 + 15 \times 0 \\ 0 \times 17 + 1 \times 4 + 2 \times 0 \end{pmatrix} \\ &= \begin{pmatrix} 17 \\ 250 \\ 4 \end{pmatrix} \\ &= \begin{pmatrix} 17 \\ 16 \\ 4 \end{pmatrix} \mathit{mod}\ 26 \\ &= \begin{pmatrix} R \\ Q \\ E \end{pmatrix}\end{aligned}$$

$$\begin{aligned}\begin{pmatrix} B & A & C \\ K & U & P \\ A & B & C \end{pmatrix}\begin{pmatrix} t \\ n \\ o \end{pmatrix} &= \begin{pmatrix} 1 & 0 & 2 \\ 10 & 20 & 15 \\ 0 & 1 & 2 \end{pmatrix}\begin{pmatrix} 19 \\ 13 \\ 14 \end{pmatrix} \\ &= \begin{pmatrix} 1 \times 19 + 0 \times 13 + 2 \times 14 \\ 10 \times 19 + 20 \times 13 + 15 \times 14 \\ 0 \times 19 + 1 \times 13 + 2 \times 14 \end{pmatrix} \\ &= \begin{pmatrix} 47 \\ 660 \\ 41 \end{pmatrix} \\ &= \begin{pmatrix} 21 \\ 10 \\ 15 \end{pmatrix} \mathit{mod}\ 26 \\ &= \begin{pmatrix} V \\ K \\ P \end{pmatrix}\end{aligned}$$

$$\begin{aligned}\begin{pmatrix} B & A & C \\ K & U & P \\ A & B & C \end{pmatrix}\begin{pmatrix} w \\ x \\ x \end{pmatrix} &= \begin{pmatrix} 1 & 0 & 2 \\ 10 & 20 & 15 \\ 0 & 1 & 2 \end{pmatrix}\begin{pmatrix} 22 \\ 23 \\ 23 \end{pmatrix} \\ &= \begin{pmatrix} 1 \times 22 + 0 \times 23 + 2 \times 23 \\ 10 \times 22 + 20 \times 23 + 15 \times 23 \\ 0 \times 22 + 1 \times 23 + 2 \times 23 \end{pmatrix} \\ &= \begin{pmatrix} 68 \\ 1025 \\ 69 \end{pmatrix} \\ &= \begin{pmatrix} 16 \\ 11 \\ 17 \end{pmatrix} \mathit{mod}\ 26 \\ &= \begin{pmatrix} Q \\ L \\ R \end{pmatrix}\end{aligned}$$

- ciphertext of "DPQRQ EVKPQ LR".

# 3x3 Example - Decryption

- Ciphertext message "SYICHOLER"
- Let key= *ALPHABET*. $\begin{pmatrix} A & L & P \\ H & A & B \\ E & T & A \end{pmatrix}$ $\begin{pmatrix} 0 & 11 & 15 \\ 7 & 0 & 1 \\ 4 & 19 & 0 \end{pmatrix}$
- Step 1 - Find the Multiplicative Inverse of the Determinant of the above matrix

  Finding the determinant of the 3 x 3 matrix with keyword alphabet using mod 26.

$$\begin{vmatrix} 0 & 11 & 15 \\ 7 & 0 & 1 \\ 4 & 19 & 0 \end{vmatrix} = 0\begin{vmatrix} 0 & 1 \\ 19 & 0 \end{vmatrix} - 11\begin{vmatrix} 7 & 1 \\ 4 & 0 \end{vmatrix} + 15\begin{vmatrix} 7 & 0 \\ 4 & 19 \end{vmatrix}$$

$$= 0(0-19) - 11(0-4) + 15(133-0)$$

$$= 0 + 44 + 1995$$

$$= 2039$$

$$= 11 \; mod \; 26$$

Tl $11 \times x = 1 \; mod \; 26$ inverse $dd^{-1} = 1 \; mod \; 26$ we multi $11 \times 19 = 209 = 1 \; mod \; 26$ 26.

multiplicative inverse of the determinant modulo 26 is 19

# 3x3 Example - Decryption

- Step 2 - Find the Adjugate Matrix of the M

$$adj\begin{pmatrix}0 & 11 & 15\\ 7 & 0 & 1\\ 4 & 19 & 0\end{pmatrix} = \begin{pmatrix} +\begin{vmatrix}0 & 1\\ 19 & 0\end{vmatrix} & -\begin{vmatrix}11 & 15\\ 19 & 0\end{vmatrix} & +\begin{vmatrix}11 & 15\\ 0 & 1\end{vmatrix}\\ -\begin{vmatrix}7 & 1\\ 4 & 0\end{vmatrix} & +\begin{vmatrix}0 & 15\\ 4 & 0\end{vmatrix} & -\begin{vmatrix}0 & 15\\ 7 & 1\end{vmatrix}\\ +\begin{vmatrix}7 & 0\\ 4 & 19\end{vmatrix} & -\begin{vmatrix}0 & 11\\ 4 & 19\end{vmatrix} & +\begin{vmatrix}0 & 11\\ 7 & 0\end{vmatrix}\end{pmatrix}$$

$$= \begin{pmatrix}-19 & 285 & 11\\ 4 & -60 & 105\\ 133 & 44 & -77\end{pmatrix}$$

$$= \begin{pmatrix}7 & 25 & 11\\ 4 & 18 & 1\\ 3 & 18 & 1\end{pmatrix} \ mod\ 26$$

Step 3 - Multiply the Multiplicative Inverse Determinant by the Adjugate

$$19 \times \begin{pmatrix}7 & 25 & 11\\ 4 & 18 & 1\\ 3 & 18 & 1\end{pmatrix} = \begin{pmatrix}133 & 475 & 209\\ 76 & 342 & 19\\ 57 & 342 & 19\end{pmatrix} = \begin{pmatrix}3 & 7 & 1\\ 24 & 4 & 19\\ 5 & 4 & 19\end{pmatrix} \ mod\ 26$$

$$if\ K = \begin{pmatrix}0 & 11 & 15\\ 7 & 0 & 1\\ 4 & 19 & 0\end{pmatrix}, then\ K^{-1} = \begin{pmatrix}3 & 7 & 1\\ 24 & 4 & 19\\ 5 & 4 & 19\end{pmatrix}$$

$$\begin{pmatrix}3 & 7 & 1\\ 24 & 4 & 19\\ 5 & 4 & 19\end{pmatrix}\begin{pmatrix}S\\ Y\\ I\end{pmatrix} = \begin{pmatrix}3 & 7 & 1\\ 24 & 4 & 19\\ 5 & 4 & 19\end{pmatrix}\begin{pmatrix}18\\ 24\\ 8\end{pmatrix} = \begin{pmatrix}3 \times 18 + 7 \times 24 + 1 \times 8\\ 24 \times 18 + 4 \times 24 + 19 \times 8\\ 5 \times 18 + 4 \times 24 + 19 \times 8\end{pmatrix} = \begin{pmatrix}230\\ 680\\ 338\end{pmatrix} = \begin{pmatrix}22\\ 4\\ 0\end{pmatrix} mod\ 26 = \begin{pmatrix}w\\ e\\ a\end{pmatrix}$$

$$\begin{pmatrix}3 & 7 & 1\\ 24 & 4 & 19\\ 5 & 4 & 19\end{pmatrix}\begin{pmatrix}C\\ H\\ O\end{pmatrix} = \begin{pmatrix}3 & 7 & 1\\ 24 & 4 & 19\\ 5 & 4 & 19\end{pmatrix}\begin{pmatrix}2\\ 7\\ 14\end{pmatrix} = \begin{pmatrix}3 \times 2 + 7 \times 7 + 1 \times 14\\ 24 \times 2 + 4 \times 7 + 19 \times 14\\ 5 \times 2 + 4 \times 7 + 19 \times 14\end{pmatrix} = \begin{pmatrix}69\\ 342\\ 304\end{pmatrix} = \begin{pmatrix}17\\ 4\\ 18\end{pmatrix} mod\ 26 = \begin{pmatrix}r\\ e\\ s\end{pmatrix}$$

$$\begin{pmatrix}3 & 7 & 1\\ 24 & 4 & 19\\ 5 & 4 & 19\end{pmatrix}\begin{pmatrix}L\\ E\\ R\end{pmatrix} = \begin{pmatrix}3 & 7 & 1\\ 24 & 4 & 19\\ 5 & 4 & 19\end{pmatrix}\begin{pmatrix}11\\ 4\\ 17\end{pmatrix} = \begin{pmatrix}3 \times 11 + 7 \times 4 + 1 \times 17\\ 24 \times 11 + 4 \times 4 + 19 \times 17\\ 5 \times 11 + 4 \times 4 + 19 \times 17\end{pmatrix} = \begin{pmatrix}78\\ 603\\ 394\end{pmatrix} = \begin{pmatrix}0\\ 5\\ 4\end{pmatrix} mod\ 26 = \begin{pmatrix}a\\ f\\ e\end{pmatrix}$$

plaintext of "we are safe"

# Cryptanalysis of Hill Cipher

- Ciphertext only attack is difficult
- known plaintext attack

# Transposition Ciphers

# Introduction to Modern Symmetric Key Ciphers

**MCA- III, Department of Computer Science**

# Modern Block Ciphers

A symmetric-key modern block cipher encrypts an n-bit block of plaintext or decrypts an n-bit block of ciphertext. The encryption or decryption algorithm uses a k-bit key.

# Substitution Ciphers

A modern block cipher can be designed to act as a substitution cipher or a transposition cipher

To be resistant to exhaustive-search attack, a modern block cipher needs to be designed as a substitution cipher.

# Substitution or Transposition Ciphers

**Example:** Suppose that we have a block cipher where n = 64. If there are 10 1’s in the ciphertext, how many trial-and-error tests does Eve need to do to recover the plaintext from the intercepted ciphertext in each of the following cases?

a. The cipher is designed as a substitution cipher.

b. The cipher is designed as a transposition cipher

**Solution:**

a. In the first case, Eve has no idea how many 1’s are in the e in the plaintext. Eve needs to try all possible 264 64-bit blocks to find one that makes sense.

b. In the second case, Eve knows that there are exactly 10 1’s in the plaintext. Eve can launch an exhaustive-search attack using only those 64-bit blocks that have exactly 10 1’s

# Block Ciphers as Permutation Group

## Full-Size key Transposition Block Ciphers:

In a full-size key transposition cipher, we need to have n! possible keys, so the key should have [log2n!] bits.

**Example:**

Show the model and the set of permutation tables for a 3-bit block transposition cipher where the block size is 3 bits.

**Solution:** The set of permutation tables has 3! = 6 elements. The key should be 3 bits long.

# Block Ciphers as Permutation Group

## Full-Size Key Substitution Block Ciphers:

A full-size key substitution cipher does not transpose bits; it substitutes bits. We can model the substitution cipher as a permutation if we can decode the input and encode the output.

**Example:**

Show the model and the set of permutation tables for a 3-bit block substitution cipher.

**Solution:**

Figure 5.3 shows the model and the set of permutation tables. The key is also much longer, élog2 40,320ù =16 bits.

# Block Ciphers as Permutation Group

A full size key n-bit transposition cipher or a substitution block cipher can be modelled as a permutation, but their key sizes are diffrent:

Transposition: the key is [log2n!] bits long

Substitution: the key is [log2(2n)!] bit long.

Actual ciphers use a partial key cipher because the size of the ful-size key becomes so large, especially for a substitution cipher.

A common substition cipher called DES uses a 64-bit block cipher with a key of 56 bits.

# Components of a Modern Block Cipher

Modern Block ciphers normally are keyed substitution ciphers in which the key allows only partial mappings from the possible inputs to the possible outputs.

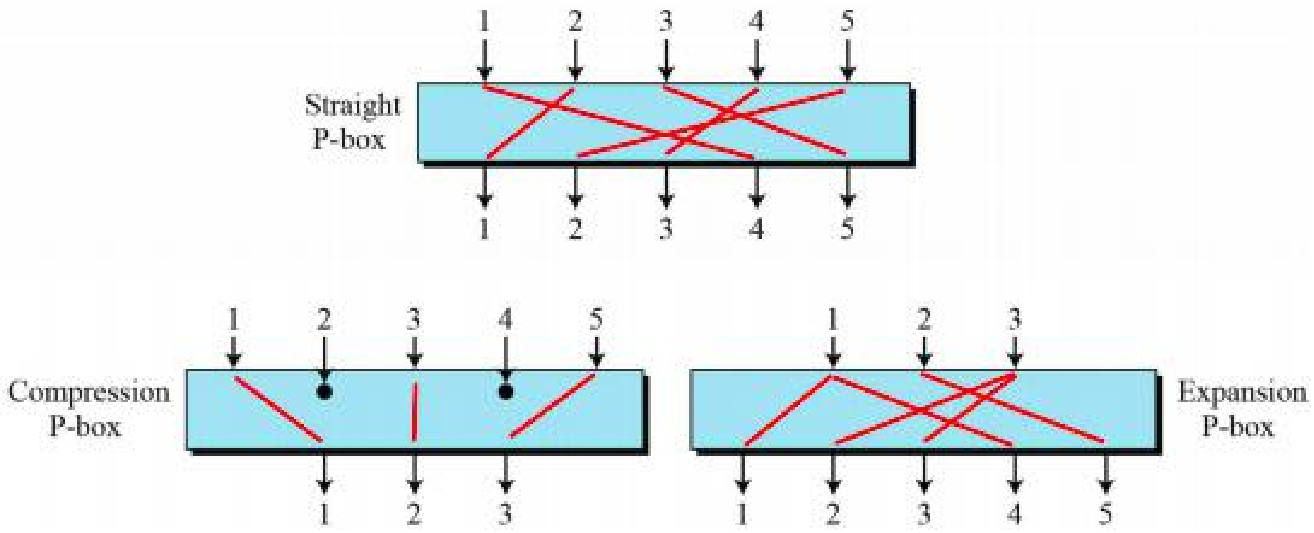
Although a keyless cipher is practically useless by itself, keyless ciphers are used as a components of keyed ciphers.

Keyless Transposition ciphers: P-Boxes

Keyless Substitution Ciphers: S-boxes

# Types of P-Boxes

A P-Box (Permutation box) parallels the traditional transposition cipher for chracters. It transposes bits.



# Types of P-Boxes

**A straight P-box** : all 6 possible mappings of a 3 × 3 P-box.

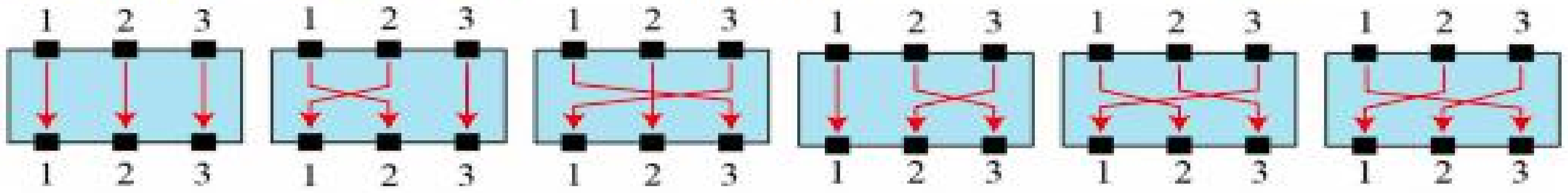
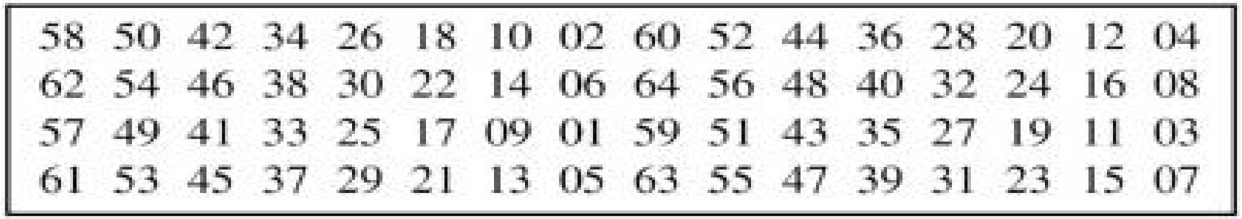


Table 5.1 Example of a 64 x 64 permutation table for a straight P-box.



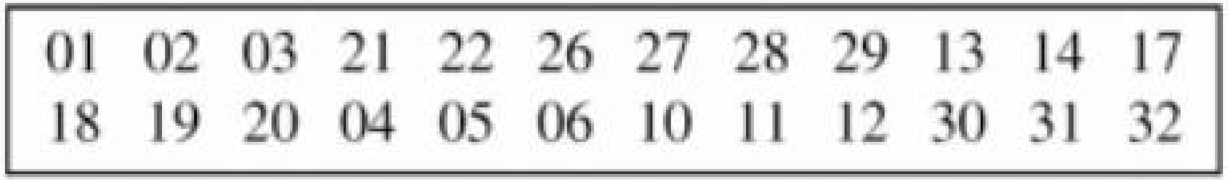
| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 58 | 50 | 42 | 34 | 26 | 18 | 10 | 02 | 60 | 52 | 44 | 36 | 28 | 20 | 12 | 04 |
| 62 | 54 | 46 | 38 | 30 | 22 | 14 | 06 | 64 | 56 | 48 | 40 | 32 | 24 | 16 | 08 |
| 57 | 49 | 41 | 33 | 25 | 17 | 09 | 01 | 59 | 51 | 43 | 35 | 27 | 19 | 11 | 03 |
| 61 | 53 | 45 | 37 | 29 | 21 | 13 | 05 | 63 | 55 | 47 | 39 | 31 | 23 | 15 | 07 |

# Types of P-Boxes

## Compression P-Boxes

A compression P-box is a P-box with n inputs and m outputs where m < n.

Table 5.2 Example of a 32 × 24 permutation table

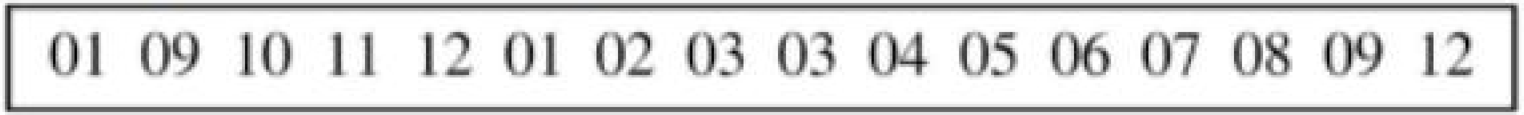


| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 01 | 02 | 03 | 21 | 22 | 26 | 27 | 28 | 29 | 13 | 14 | 17 |
| 18 | 19 | 20 | 04 | 05 | 06 | 10 | 11 | 12 | 30 | 31 | 32 |

## Expansion P-Boxes

An expansion P-box is a P-box with n inputs and m outputs where m > n.

Table 5.3 Example of a 12 × 16 permutation table



| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 01 | 09 | 10 | 11 | 12 | 01 | 02 | 03 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 12 |

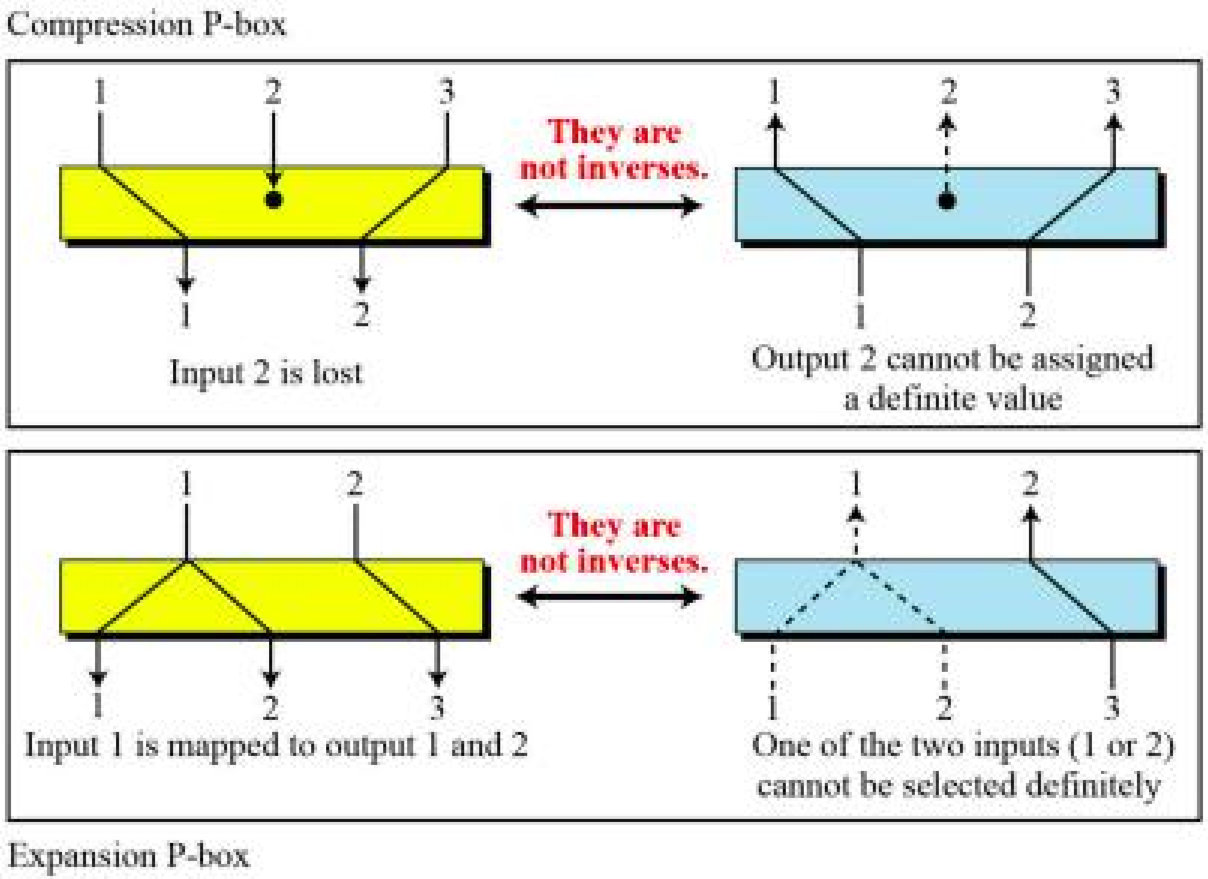
# P-Boxes

P-Boxes: Invertablity.

A straight P-Box is invertible, but compression and expansion P-Boxes are not.

# Types of P-Boxes

Figure 5.7 Compression and expansion P-boxes are non-invertible

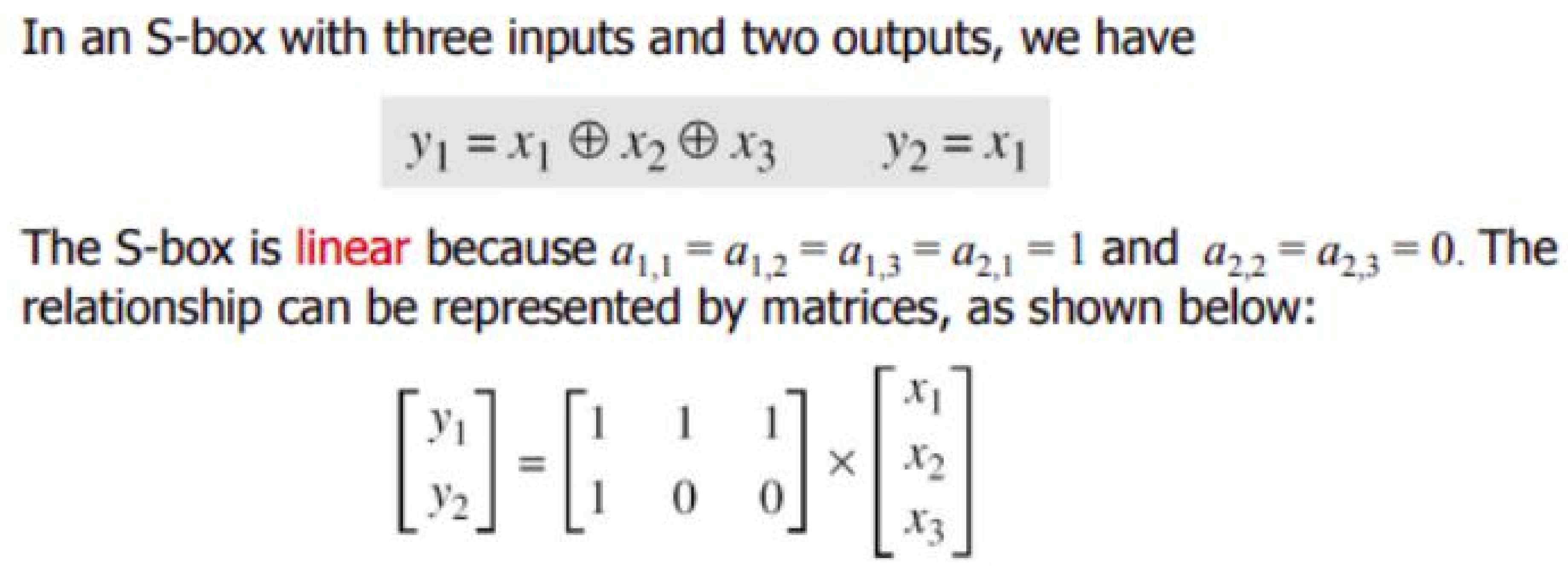

Compression P-box
1
2
3
They are not inverses.
1
2
3
1
2
Input 2 is lost
1
2
Output 2 cannot be assigned a definite value
1
2
They are not inverses.
1
2
1
2
3
Input 1 is mapped to output 1 and 2
1
2
3
One of the two inputs (1 or 2) cannot be selected definitely
Expansion P-box

# S-Box

- An S-box (substitution box) can be thought of as a miniature substitution ciphers.

- An S-box is an mXn substitution unit, where m and n are not necessarily the same

# S-Box



In an S-box with three inputs and two outputs, we have

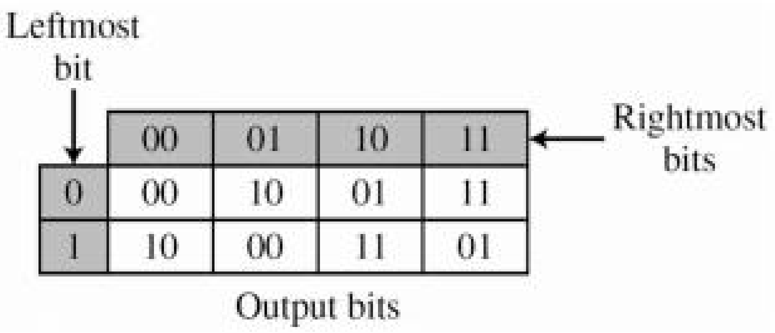
$$y_1 = x_1 \oplus x_2 \oplus x_3 \qquad y_2 = x_1$$

The S-box is linear because $a_{1,1} = a_{1,2} = a_{1,3} = a_{2,1} = 1$ and $a_{2,2} = a_{2,3} = 0$. The relationship can be represented by matrices, as shown below:

$$\begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix} \times \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}$$

# S-Box

The following table defines the input/output relationship for an S-box of size 3 × 2. The leftmost bit of the input defines the row; the two rightmost bits of the input define the column. The two output bits are values on the cross section of the selected row and column.



Leftmost bit
Rightmost bits
Output bits

| | 00 | 01 | 10 | 11 |
|---|---|---|---|---|
| 0 | 00 | 10 | 01 | 11 |
| 1 | 10 | 00 | 11 | 01 |

Based on the table, an input of **010** yields the output **01**. An input of **101** yields the output of **00**.

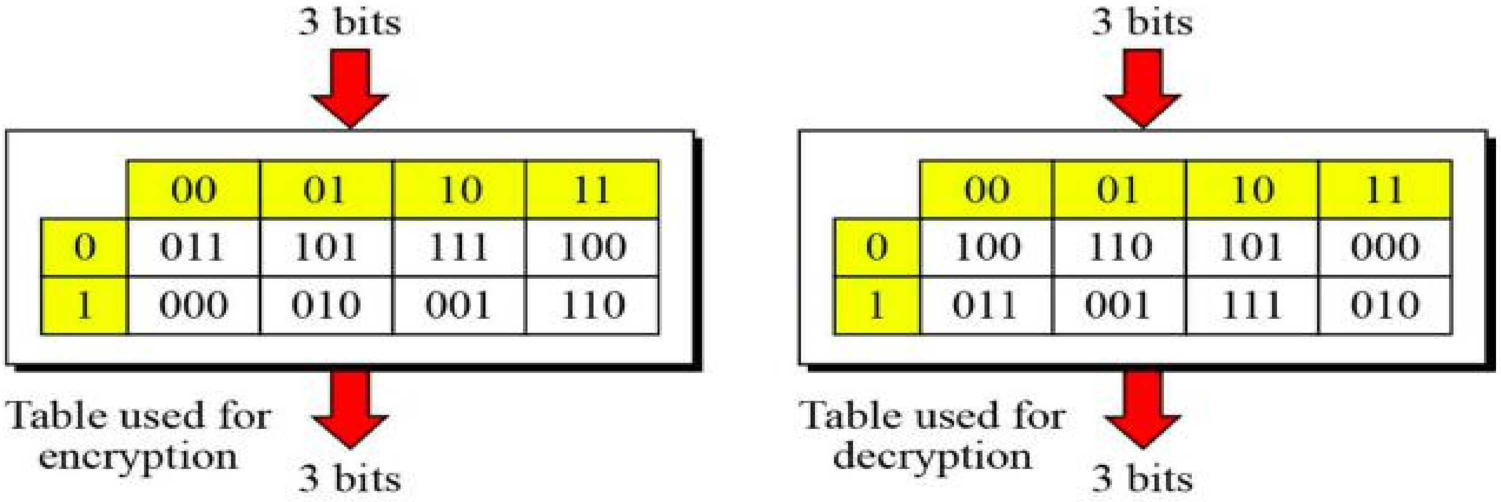
# S-Box

## S-Boxes: Invertibility

An S-box may or may not be invertible. In an invertible S-box, the number of input bits should be the same as the number of output bits.

### Example 5.11

Figure 5.8 shows an example of an invertible S-box. For example, if the input to the left box is 001, the output is 101. The input 101 in the right table creates the output 001, which shows that the two tables are inverses of each other.



|   | 00 | 01 | 10 | 11 |
|---|---|---|---|---|
| 0 | 011 | 101 | 111 | 100 |
| 1 | 000 | 010 | 001 | 110 |

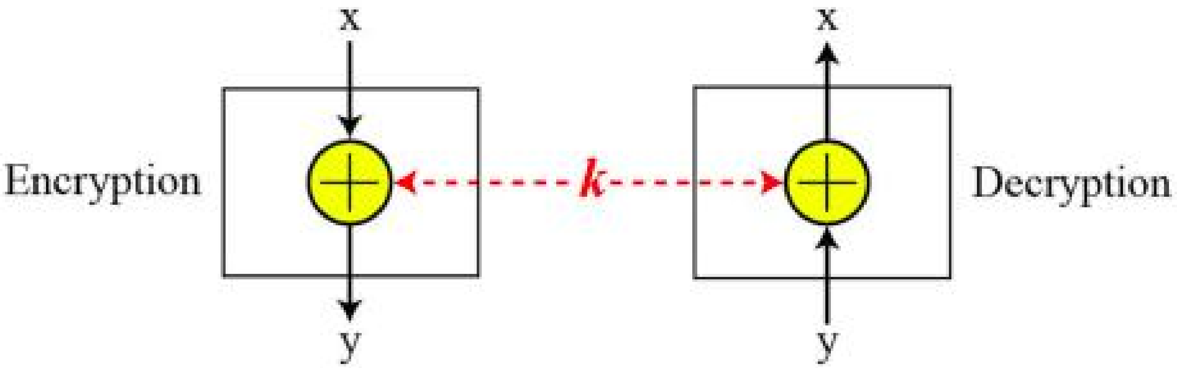
|   | 00 | 01 | 10 | 11 |
|---|---|---|---|---|
| 0 | 100 | 110 | 101 | 000 |
| 1 | 011 | 001 | 111 | 010 |

# S-Box

## Exclusive-Or

An important component in most block ciphers is the exclusive-or operation. As we discussed in Chapter 4, addition and subtraction operations in the GF($2^n$) field are performed by a single operation called the exclusive-or (XOR).

Figure 5.9 Invertibility of the exclusive-or operation

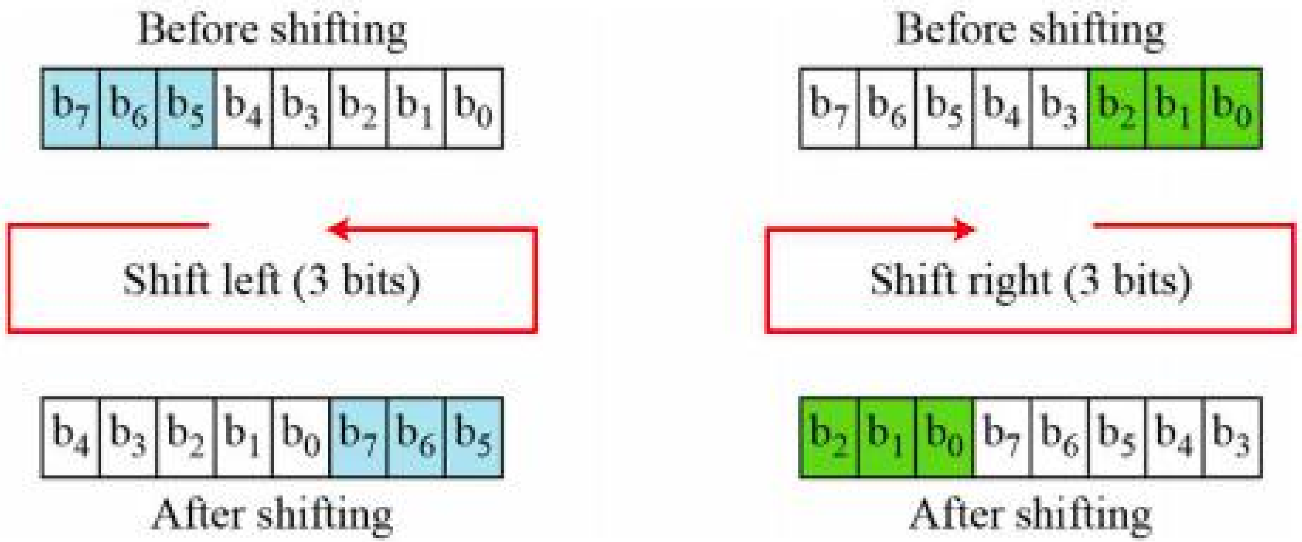


# S-Box

## Circular Shift

Another component found in some modern block ciphers is the circular shift operation.

Figure 5.10 Circular shifting an 8-bit word to the left or right

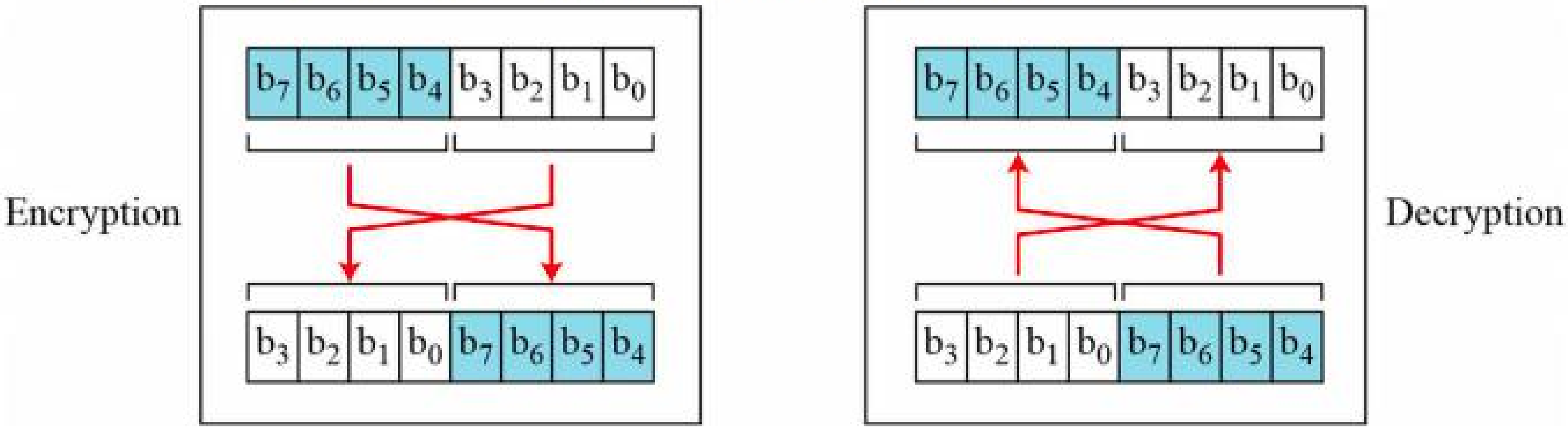

Before shifting
$b_7$ $b_6$ $b_5$ $b_4$ $b_3$ $b_2$ $b_1$ $b_0$
Shift left (3 bits)
$b_4$ $b_3$ $b_2$ $b_1$ $b_0$ $b_7$ $b_6$ $b_5$
After shifting
Before shifting
$b_7$ $b_6$ $b_5$ $b_4$ $b_3$ $b_2$ $b_1$ $b_0$
Shift right (3 bits)
$b_2$ $b_1$ $b_0$ $b_7$ $b_6$ $b_5$ $b_4$ $b_3$
After shifting

# S-Box

**Swap**

The swap operation is a special case of the circular shift operation where k = n/2.

Figure 5.11 Swap operation on an 8-bit word



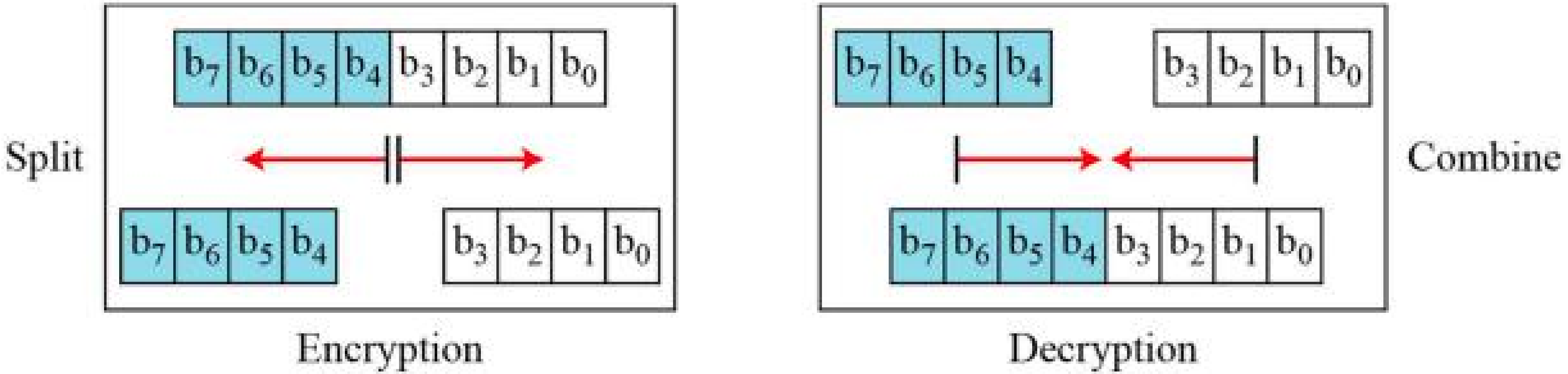
Encryption
$b_7$ $b_6$ $b_5$ $b_4$ $b_3$ $b_2$ $b_1$ $b_0$
$b_3$ $b_2$ $b_1$ $b_0$ $b_7$ $b_6$ $b_5$ $b_4$
Decryption
$b_7$ $b_6$ $b_5$ $b_4$ $b_3$ $b_2$ $b_1$ $b_0$
$b_3$ $b_2$ $b_1$ $b_0$ $b_7$ $b_6$ $b_5$ $b_4$

# S-Box

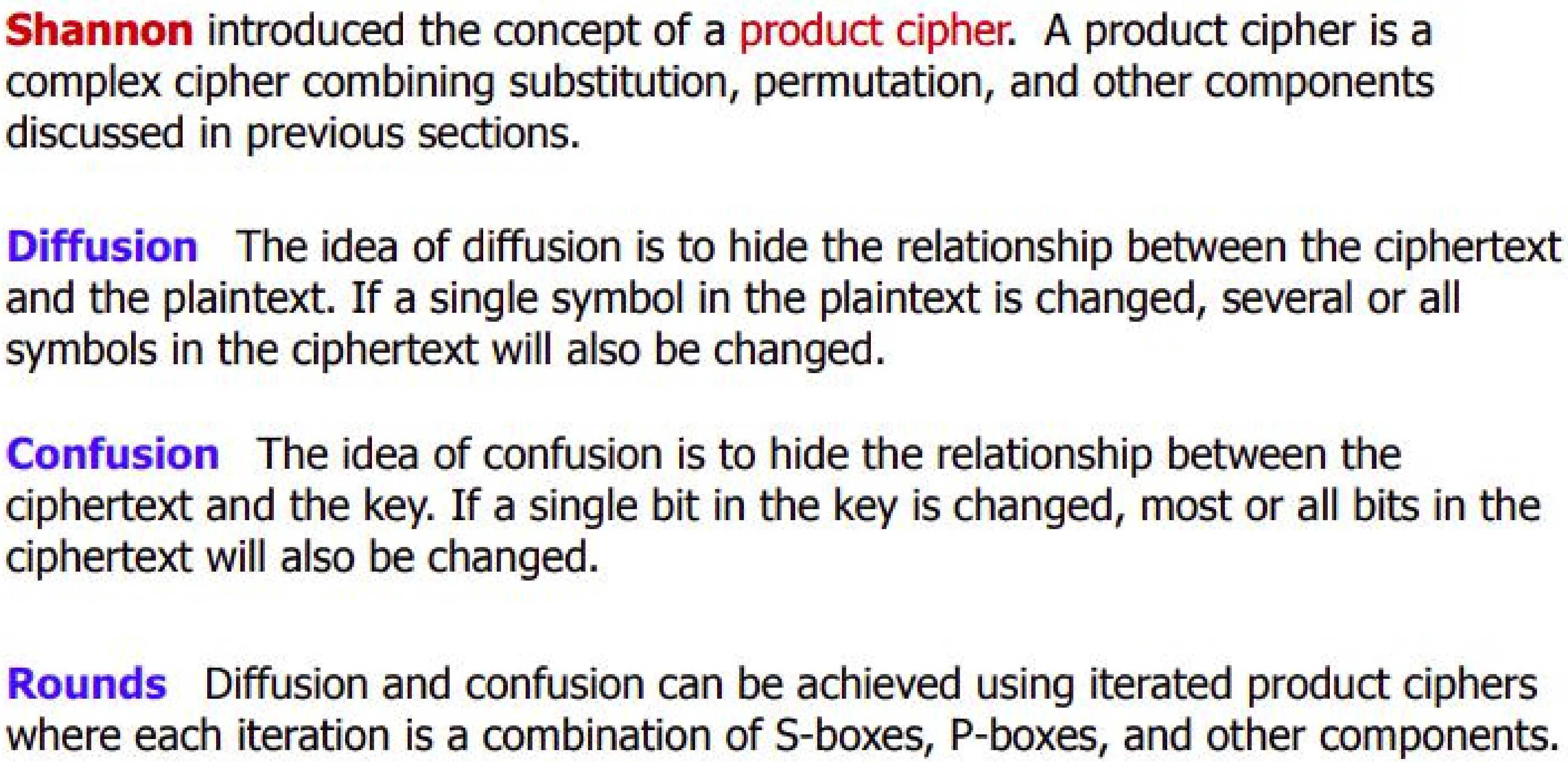
## Split and Combine

Two other operations found in some block ciphers are split and combine.

Figure 5.12 Split and combine operations on an 8-bit word



# Product Cipher



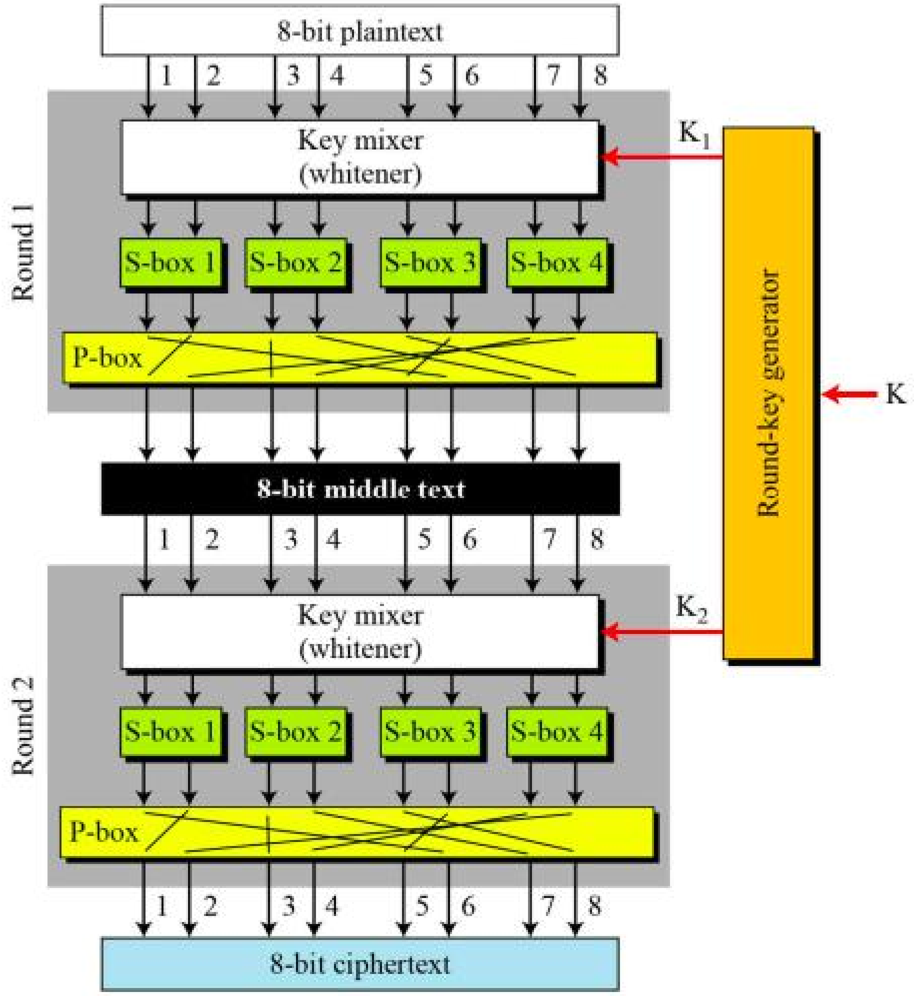
**Shannon** introduced the concept of a product cipher. A product cipher is a complex cipher combining substitution, permutation, and other components discussed in previous sections.

**Diffusion** The idea of diffusion is to hide the relationship between the ciphertext and the plaintext. If a single symbol in the plaintext is changed, several or all symbols in the ciphertext will also be changed.

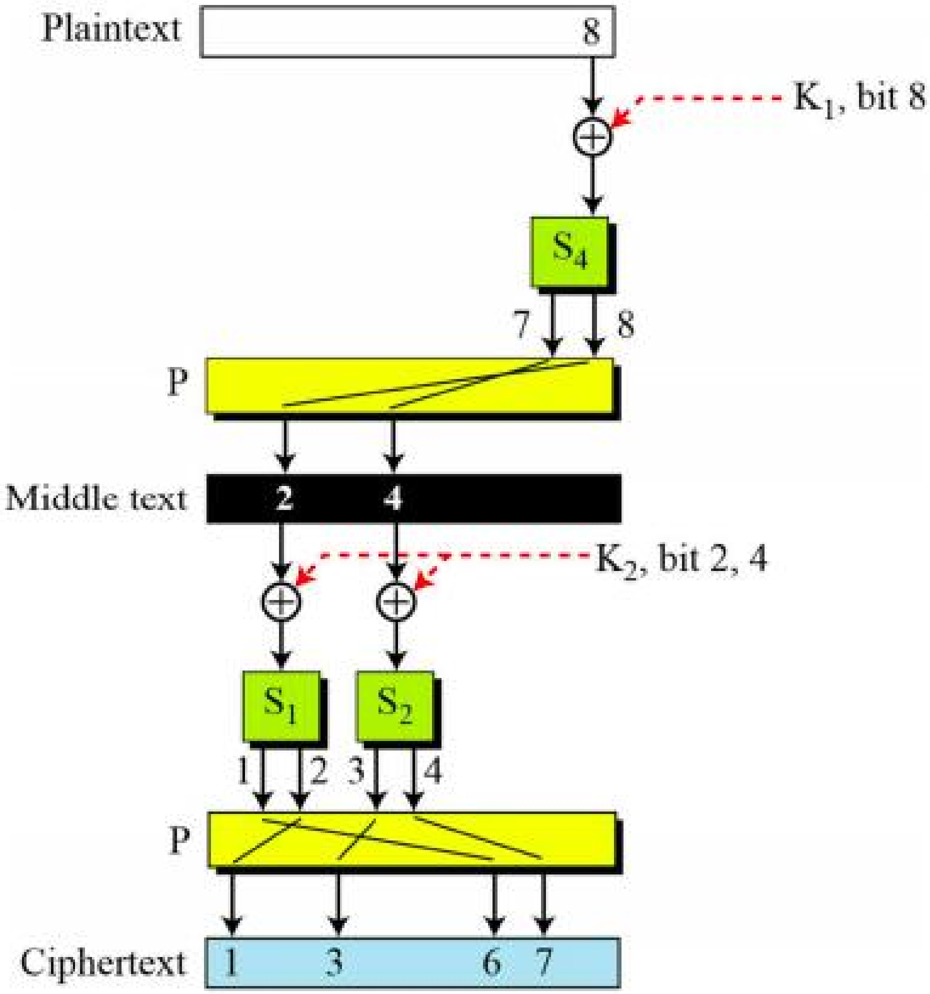
**Confusion** The idea of confusion is to hide the relationship between the ciphertext and the key. If a single bit in the key is changed, most or all bits in the ciphertext will also be changed.

**Rounds** Diffusion and confusion can be achieved using iterated product ciphers where each iteration is a combination of S-boxes, P-boxes, and other components.

# Product Cipher



# Product Cipher



# Two Classes of Product Cipher

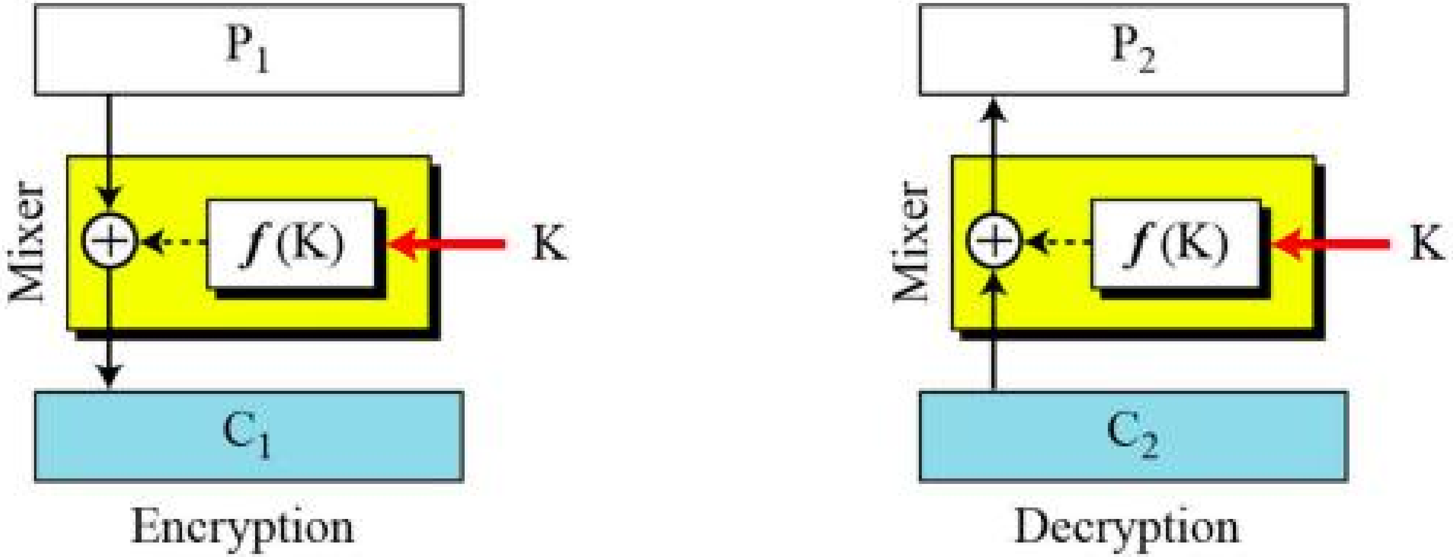
Modern block ciphers are all product ciphers, but they are divided into two classes.

1. Feistel ciphers : DES
   Has been used for decades.
   Can have three types of components :
   self-invertible, invertible, and noninvertible.

2. Non-Feistel ciphers : AES
   Uses only invertible components.
   A component in the encryption cipher has the corresponding component in the decryption cipher.

# Two Classes of Product Cipher

Figure 5.15 The first thought in Feistel cipher design



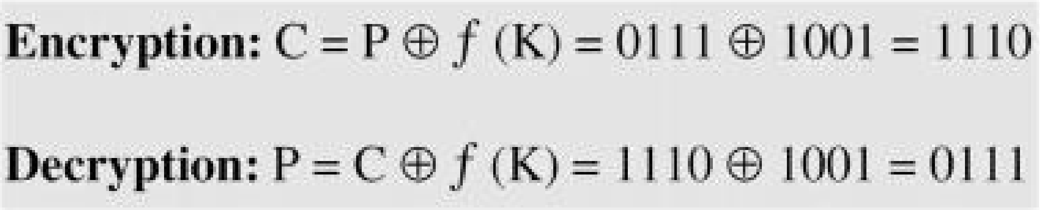
# Two Classes of Product Cipher

## Example 5.12

This is a trivial example. The plaintext and ciphertext are each 4 bits long and the key is 3 bits long. Assume that the function takes the first and third bits of the key, interprets these two bits as a decimal number, squares the number, and interprets the result as a 4-bit binary pattern. Show the results of encryption and decryption if the original plaintext is 0111 and the key is 101.

## Solution

The function extracts the first and second bits to get 11 in binary or 3 in decimal. The result of squaring is 9, which is 1001 in binary.

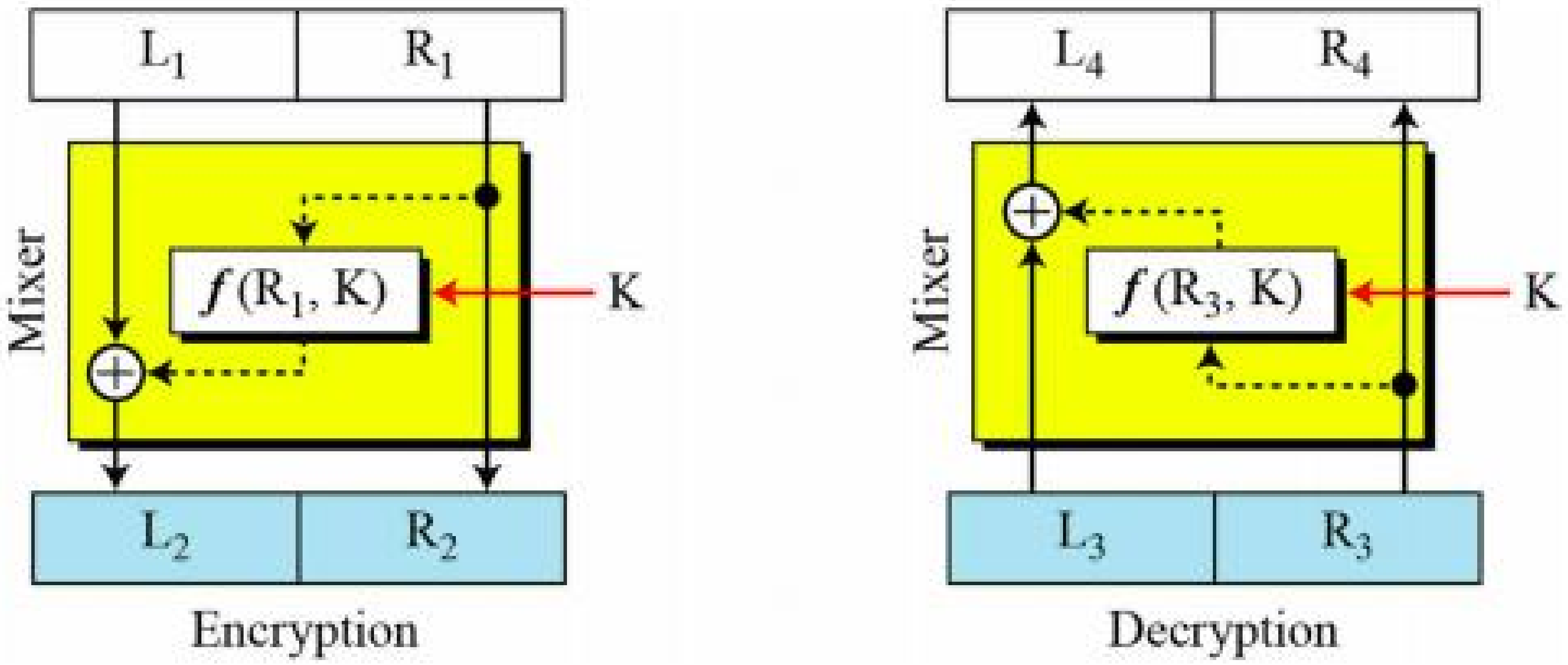


**Encryption:** $C = P \oplus f\,(K) = 0111 \oplus 1001 = 1110$

**Decryption:** $P = C \oplus f\,(K) = 1110 \oplus 1001 = 0111$

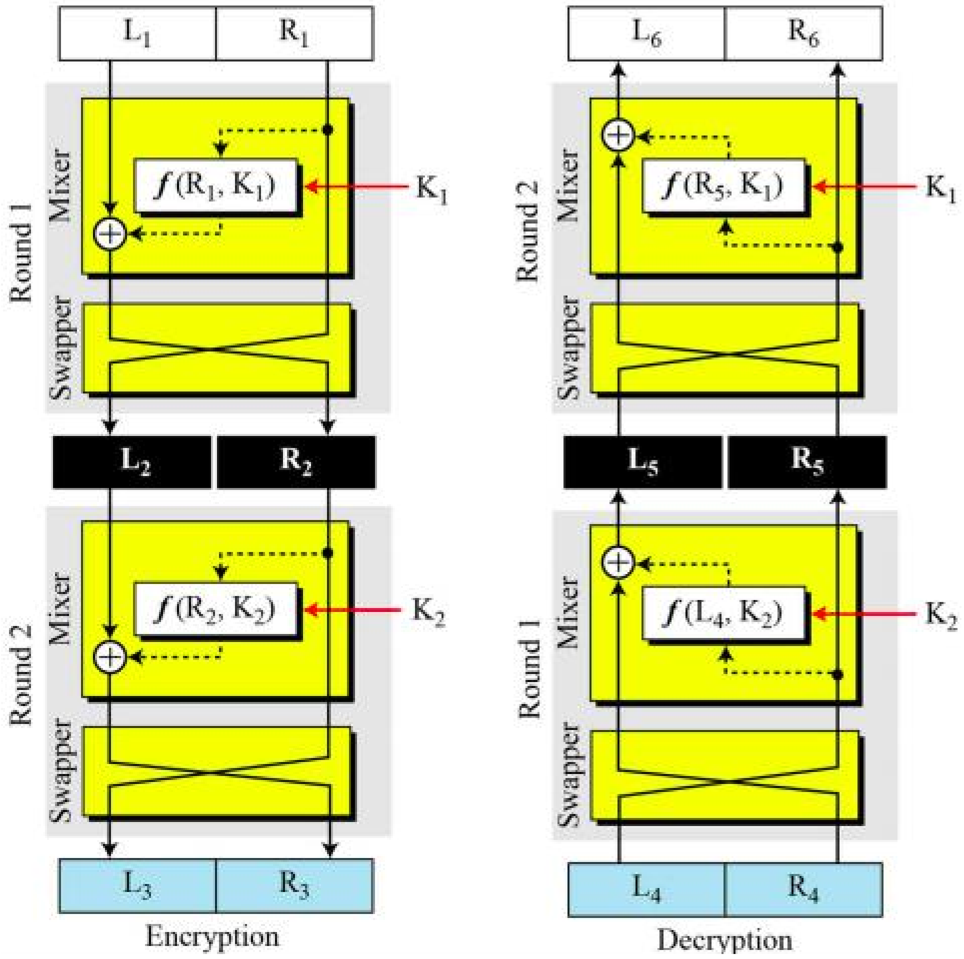
# Two Classes of Product Cipher

Figure 5.16 Improvement of the previous Feistel design



# Two Classes of Product Cipher

Figure 5.17 Final design of a Feistel cipher with two rounds



# Attacks on Block Cipher

Attacks on traditional ciphers can also be used on modern block ciphers, but today's block ciphers resist most of the attacks discussed in Chapter 3.

## Differential Cryptanalysis

Eli Biham and Adi Shamir introduced the idea of differential cryptanalysis. This is a chosen-ciphertext attack.

## Linear Cryptanalysis

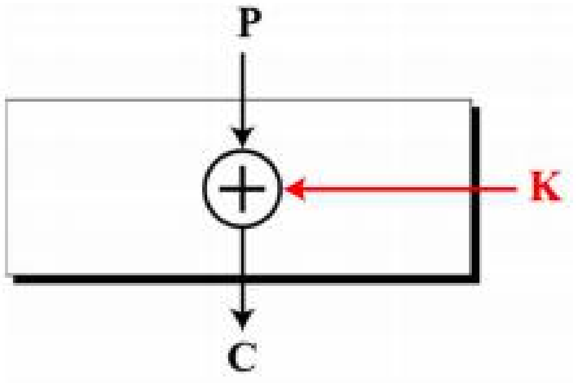
Linear cryptanalysis was presented by Mitsuru Matsui in 1993. The analysis uses known plaintext attacks.

# Attacks on Block Cipher

**Example 5.13**

Assume that the cipher is made only of one exclusive-or operation, as shown in Figure 5.18. Without knowing the value of the key, Eve can easily find the relationship between plaintext differences and ciphertext differences if by plaintext difference we mean $P_1 \oplus P_2$ and by ciphertext difference, we mean $C_1 \oplus C_2$. The following proves that $C_1 \oplus C_2 = P_1 \oplus P_2$:

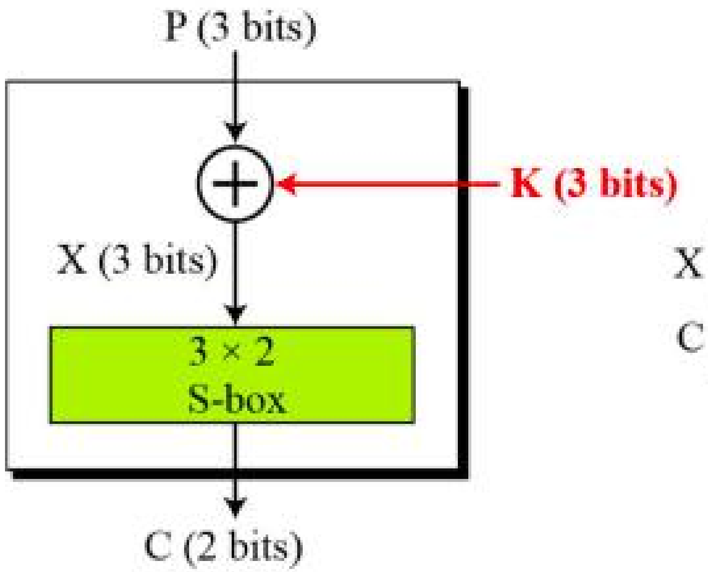
$$C_1 = P_1 \oplus K \quad C_2 = P_2 \oplus K \quad \rightarrow \quad C_1 \oplus C_2 = P_1 \oplus K \oplus P_2 \oplus K = P_1 \oplus P_2$$



# Attacks on Block Cipher

## Example 5.14

We add one S-box to Example 5.13, as shown in Figure 5.19.



| X | 000 | 001 | 010 | 011 | 100 | 101 | 110 | 111 |
|---|---|---|---|---|---|---|---|---|
| C | 11 | 00 | 10 | 10 | 01 | 00 | 11 | 00 |

S-box table

# Attacks on Block Cipher

**Example 5.14** **(Continued)**

Eve now can create a probabilistic relationship as shown in Tables 5.4 and 5.5.

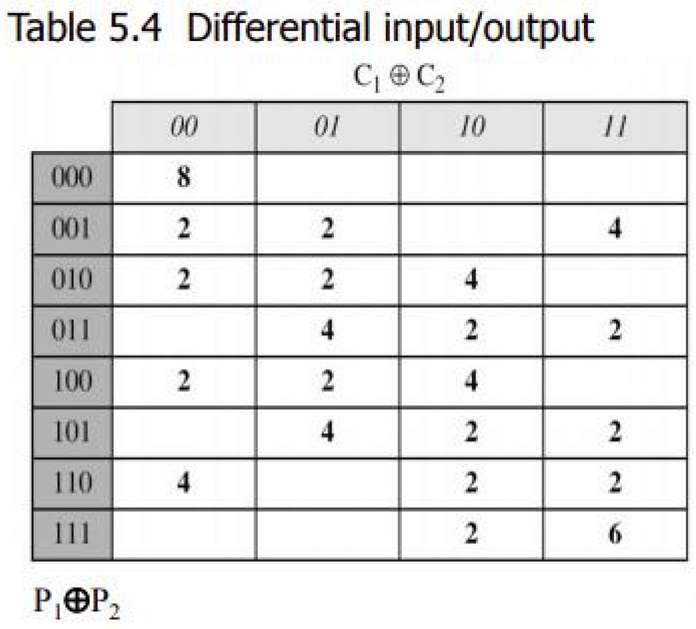


Table 5.4 Differential input/output

| | $C_1 \oplus C_2$ | | | |
|---|---|---|---|---|
| $P_1 \oplus P_2$ | *00* | *01* | *10* | *11* |
| 000 | 8 | | | |
| 001 | 2 | 2 | | 4 |
| 010 | 2 | 2 | 4 | |
| 011 | | 4 | 2 | 2 |
| 100 | 2 | 2 | 4 | |
| 101 | | 4 | 2 | 2 |
| 110 | 4 | | 2 | 2 |
| 111 | | | 2 | 6 |

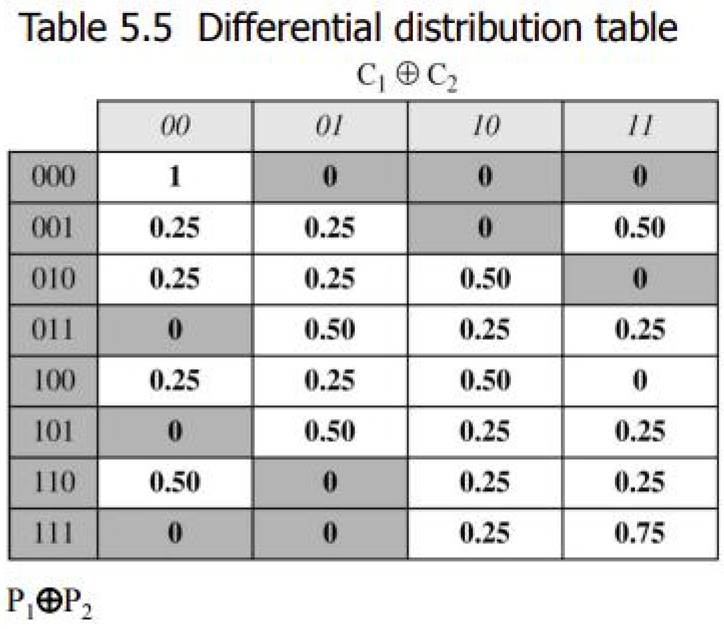


Table 5.5 Differential distribution table

| | $C_1 \oplus C_2$ | | | |
|---|---|---|---|---|
| $P_1 \oplus P_2$ | *00* | *01* | *10* | *11* |
| 000 | 1 | 0 | 0 | 0 |
| 001 | 0.25 | 0.25 | 0 | 0.50 |
| 010 | 0.25 | 0.25 | 0.50 | 0 |
| 011 | 0 | 0.50 | 0.25 | 0.25 |
| 100 | 0.25 | 0.25 | 0.50 | 0 |
| 101 | 0 | 0.50 | 0.25 | 0.25 |
| 110 | 0.50 | 0 | 0.25 | 0.25 |
| 111 | 0 | 0 | 0.25 | 0.75 |

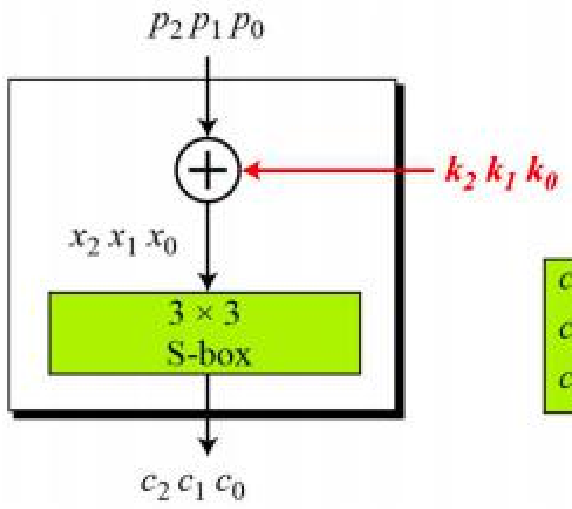
# Attacks on Block Cipher

## Linear Cryptanalysis:

Linear cryptanalysis was presented by Mitsuru Matsui in 1993. The analysis uses known-plaintext attacks.

# Attacks on Block Cipher

Figure 5.20 A simple cipher with a **linear S-box**



$$c_0 = x_0 \oplus x_1$$
$$c_1 = x_0 \oplus x_1 \oplus x_2$$
$$c_2 = x_1 \oplus x_2$$

S-box

$$c_0 = p_0 \oplus k_0 \oplus p_1 \oplus k_1$$
$$c_1 = p_0 \oplus k_0 \oplus p_1 \oplus k_1 \oplus p_2 \oplus k_2$$
$$c_2 = p_1 \oplus k_1 \oplus p_2 \oplus k_2$$

Solving for three unknowns, we get.

$$k_1 = (p_1) \oplus (c_0 \oplus c_1 \oplus c_2)$$
$$k_2 = (p_2) \oplus (c_0 \oplus c_1)$$
$$k_0 = (p_0) \oplus (c_1 \oplus c_2)$$

This means that three known-plaintext attacks can find the values of $k_0$, $k_1$, and $k_2$ .