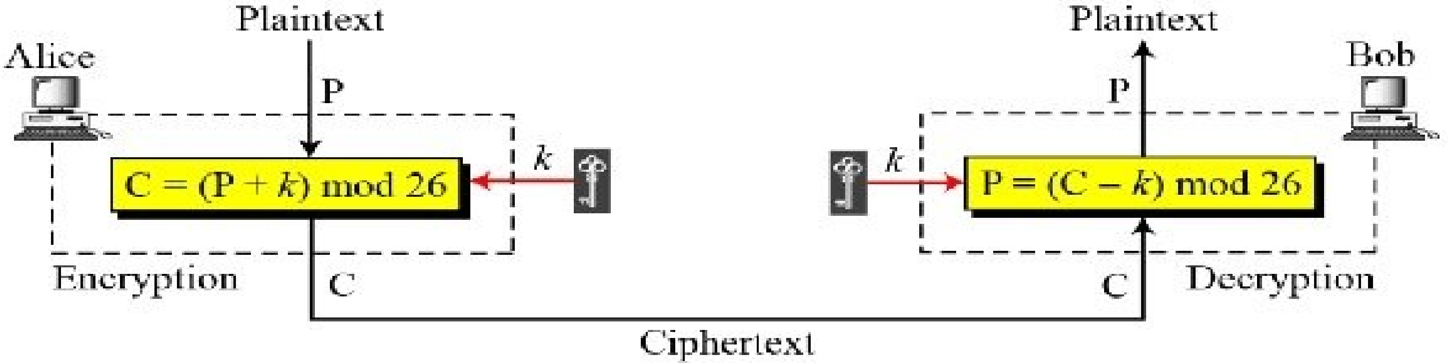
19Z701 - CRYPTOGRAPHY

Additive Cipher

3.2.1 Continued

Figure 3.9 ***Additive cipher***



Note

When the cipher is additive, the plaintext, ciphertext, and key are integers in Z_{26}.

3.2.1 Continued

Example 3.3

Use the additive cipher with **key = 15** to encrypt the message "hello".

Solution

We apply the encryption algorithm to the plaintext, character by character:

Plaintext: h → 07	Encryption: (07 + 15) mod 26	Ciphertext: 22 → W
Plaintext: e → 04	Encryption: (04 + 15) mod 26	Ciphertext: 19 → T
Plaintext: l → 11	Encryption: (11 + 15) mod 26	Ciphertext: 00 → A
Plaintext: l → 11	Encryption: (11 + 15) mod 26	Ciphertext: 00 → A
Plaintext: o → 14	Encryption: (14 + 15) mod 26	Ciphertext: 03 → D

Encryption EK(x) = x + K mod 26

3.2.1 Continued

Example 3.4

Use the additive cipher with **key = 15** to decrypt the message "WTAAD".

Solution

We apply the decryption algorithm to the plaintext character by character:

Ciphertext: W $\rightarrow$ 22	Decryption: (22 – 15) mod 26	Plaintext: 07 $\rightarrow$ h
Ciphertext: T $\rightarrow$ 19	Decryption: (19 – 15) mod 26	Plaintext: 04 $\rightarrow$ e
Ciphertext: A $\rightarrow$ 00	Decryption: (00 – 15) mod 26	Plaintext: 11 $\rightarrow$ l
Ciphertext: A $\rightarrow$ 00	Decryption: (00 – 15) mod 26	Plaintext: 11 $\rightarrow$ l
Ciphertext: D $\rightarrow$ 03	Decryption: (03 – 15) mod 26	Plaintext: 14 $\rightarrow$ o

Decryption DK(x) = x - K mod 26

3.2.1 Continued

Example 3.5

Eve has intercepted the ciphertext "UVACLYFZLJBYL". Show how she can use a brute-force attack to break the cipher.

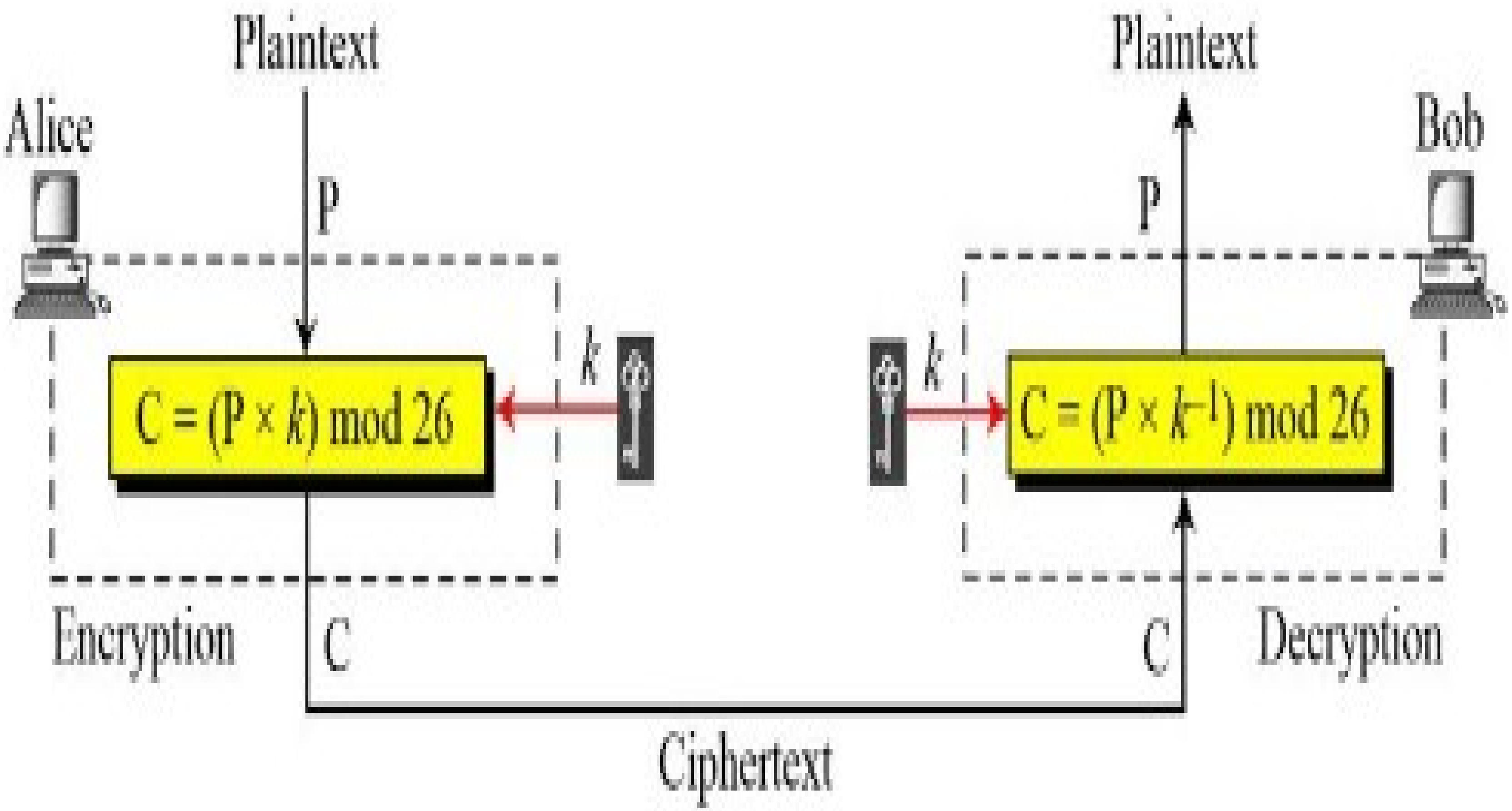
Solution

Eve tries keys from 1 to 7. With a key of 7, the plaintext is "not very secure", which makes sense.

Ciphertext: UVACLYFZLJBYL

$K = 1$ → **Plaintext:** tuzbkxeykiaxk
$K = 2$ → **Plaintext:** styajwdxjhzwj
$K = 3$ → **Plaintext:** rsxzivcwigyvi
$K = 4$ → **Plaintext:** qrwyhubvhfxuh
$K = 5$ → **Plaintext:** pqvxgtaugewtg
$K = 6$ → **Plaintext:** opuwfsztfdvsf
$K = 7$ → **Plaintext:** notverysecure

Multiplicative Cipher



Encryption

$$\mathbf{C = E(K,P)=(P*K) \bmod 26}$$

Decryption

- Decryption algorithm :

$$\mathbf{P=D(K,C)=(C*}K^{-1}\mathbf{)\ mod\ 26}$$

Example

encrypt the message "HELLO" using multiplicative cipher with key = 7

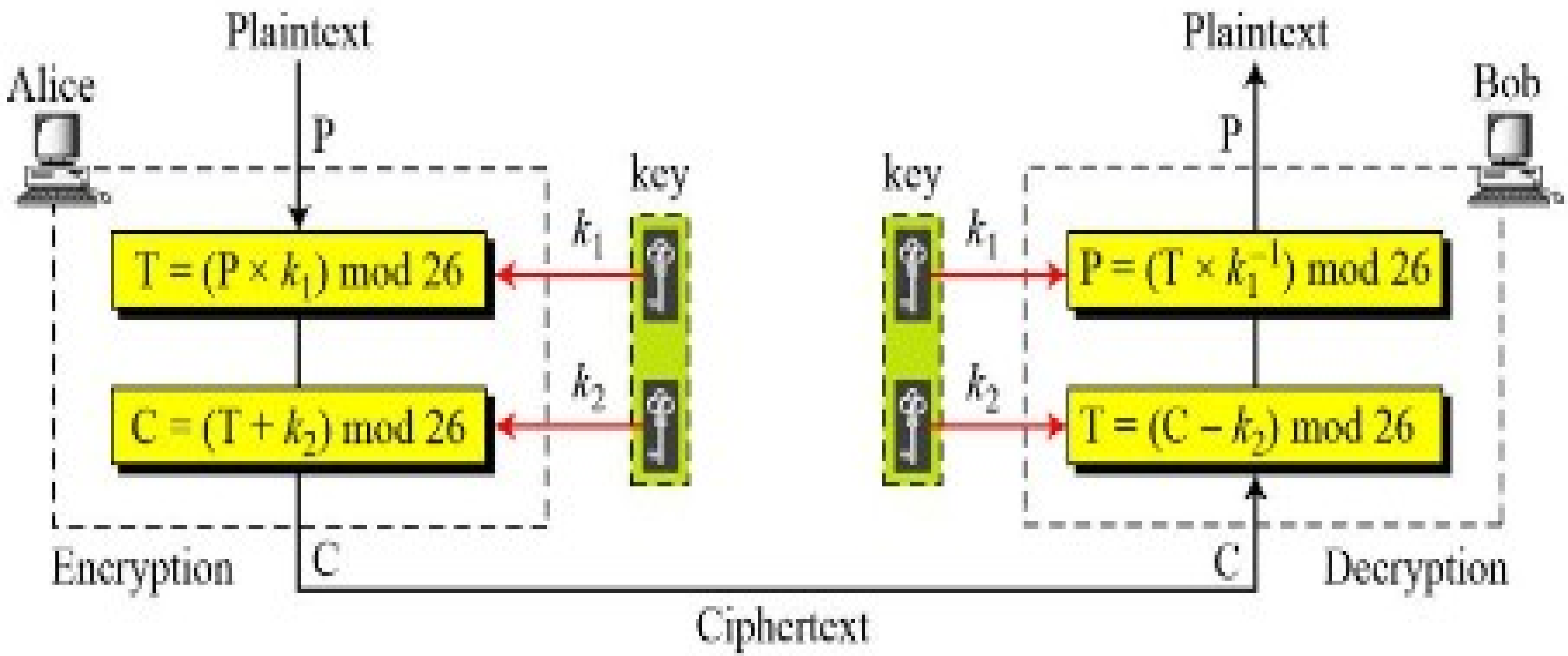
Plaintext: Letters → Numeric Value	Encryption: (P * K) mod 26	Ciphertext: Numeric Value → letters
Plaintext: H = 07	Encryption: (07*07)mod 26	Ciphertext: 23= X
Plaintext: E = 04	Encryption: (04*07)mod 26	Ciphertext: 02 = C
Plaintext: L = 11	Encryption: (11*07)mod 26	Ciphertext: 25 = Z
Plaintext: L = 11	Encryption: (11*07)mod 26	Ciphertext: 25 = Z
Plaintext: 0 = 14	Encryption: (14*07)mod 26	Ciphertext: 20 = U

Table of Multiplicative Inverse

we must use a multiplier which is co-prime (the values do not share any factors when dividing in relation to the size of the alphabet (26), so you should use either 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23 or 25.

key *a*	key a^{-1}
1	1
3	9
5	21
7	15
9	3
11	19
15	7
17	23
19	11
21	5
23	17
25	25

Affine Cipher



$$C = (P \times k_1 + k_2) \bmod 26 \qquad\qquad P = ((C - k_2) \times k_1^{-1}) \bmod 26$$

where k_1^{-1} is the multiplicative inverse of k_1 and $-k_2$ is the additive inverse of k_2

Example

Encrypt the message "HELLO" using Affine Cipher with key pair (7,2)

Plaintext: Letters → Numeric Value	**Encryption:** ((P * K1) + K2)mod 26	**Ciphertext:** Numeric Value → letters
Plaintext: H = 07	Encryption: (07*07+2)mod 26	Ciphertext: 25 = Z
Plaintext: E = 04	Encryption: (04*07+2)mod 26	Ciphertext: 04 = E
Plaintext: L = 11	Encryption: (11*07+2)mod 26	Ciphertext: 01 = B
Plaintext: L = 11	Encryption: (11*07+2)mod 26	Ciphertext: 01 = B
Plaintext: 0 = 14	Encryption: (14*07+2)mod 26	Ciphertext: 22 = W

Affine Ciphers…

Use the affine cipher to decrypt the message "ZEBBW" with the key pair (7, 2) in modulus 26.

C: Z $\rightarrow$ 25	Decryption: $((25 - 2) \times 7^{-1}) \bmod 26$	P:07 $\rightarrow$ h
C: E $\rightarrow$ 04	Decryption: $((04 - 2) \times 7^{-1}) \bmod 26$	P:04 $\rightarrow$ e
C: B $\rightarrow$ 01	Decryption: $((01 - 2) \times 7^{-1}) \bmod 26$	P:11 $\rightarrow$ l
C: B $\rightarrow$ 01	Decryption: $((01 - 2) \times 7^{-1}) \bmod 26$	P:11 $\rightarrow$ l
C: W $\rightarrow$ 22	Decryption: $((22 - 2) \times 7^{-1}) \bmod 26$	P:14 $\rightarrow$ o

The additive cipher is a special case of an affine cipher in which $k_1 = 1$. The multiplicative cipher is a special case of affine cipher in which $k_2 = 0$.

Thank You