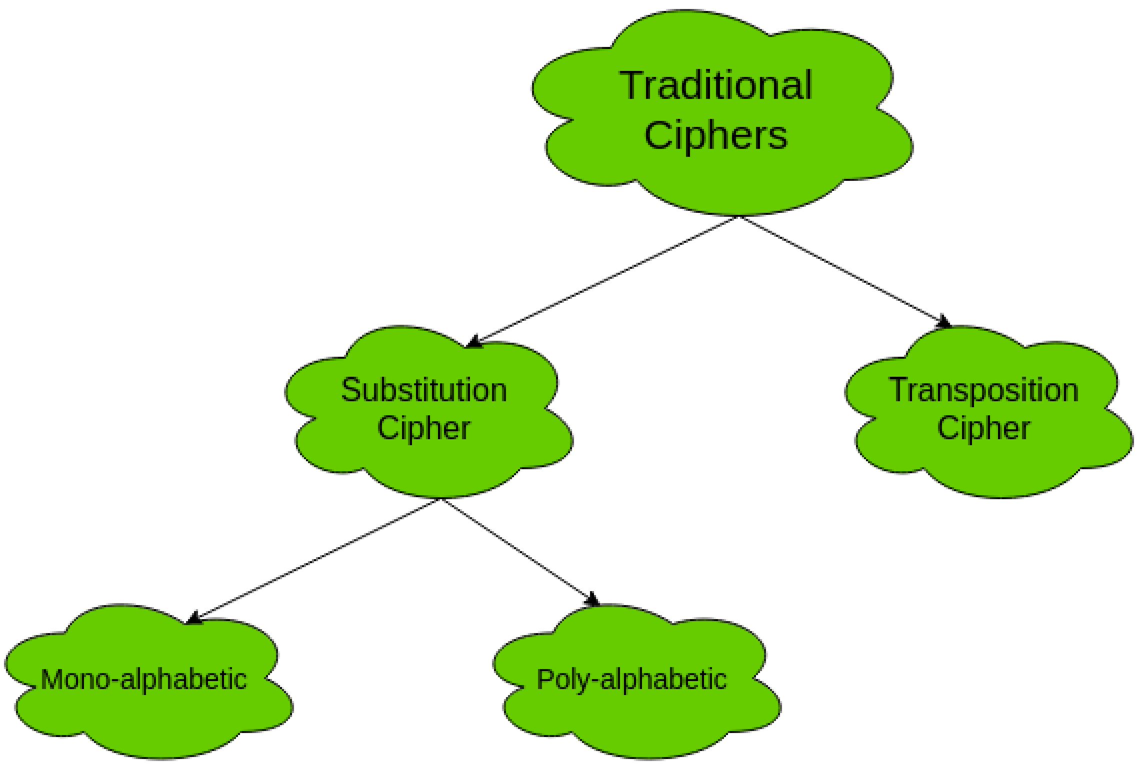
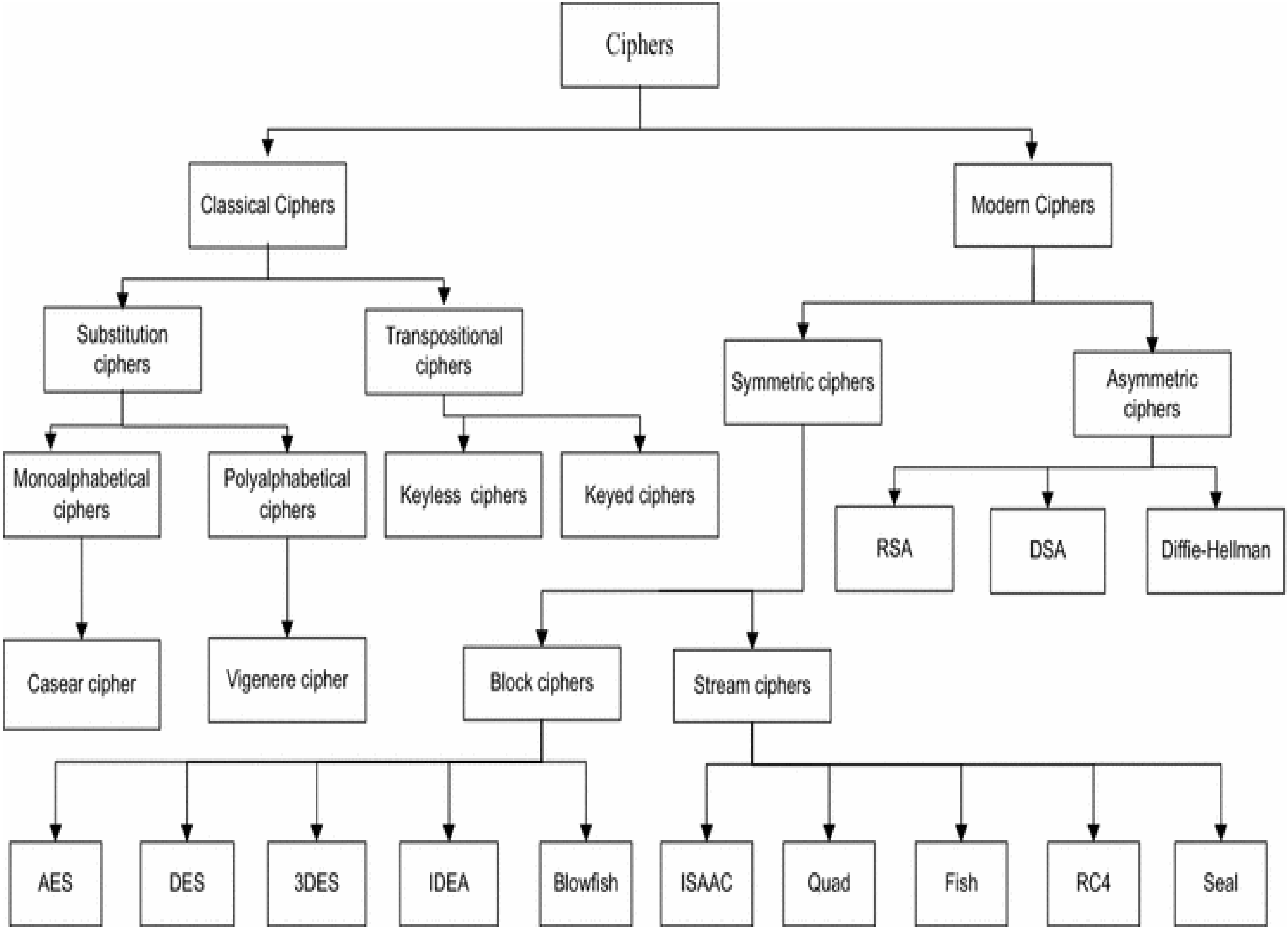
Cryptography

Classical Ciphers

Traditional Symmetric Ciphers

The two types of traditional symmetric ciphers are **Substitution Cipher** and **Transposition Cipher**.
The following flowchart categories the traditional ciphers:

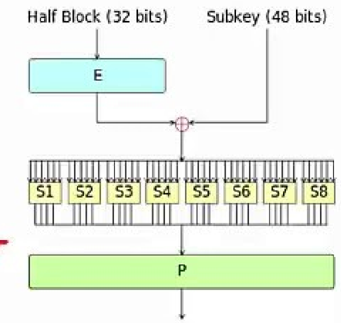



Ciphers
Classical Ciphers
Modern Ciphers
Substitution ciphers
Transpositional ciphers
Symmetric ciphers
Asymmetric ciphers
Monoalphabetical ciphers
Polyalphabetical ciphers
Keyless ciphers
Keyed ciphers
RSA
DSA
Diffie-Hellman
Casear cipher
Vigenere cipher
Block ciphers
Stream ciphers
AES
DES
3DES
IDEA
Blowfish
ISAAC
Quad
Fish
RC4
Seal

Classical vs Modern

Classical

- **Confidentiality**
- Plain text
- Military
- Secrecy of protocol/algorithm



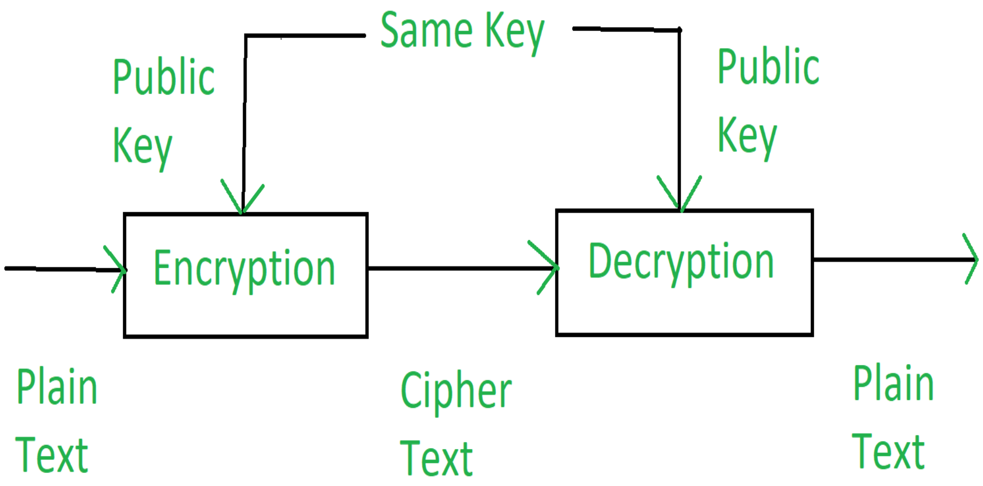
Modern

- **Confidentiality**, Integrity
  - Further digital cash, secure voting etc
- Deals with bits
- Every one
- Provable security based on mathematics (protocol /algorithm often open)

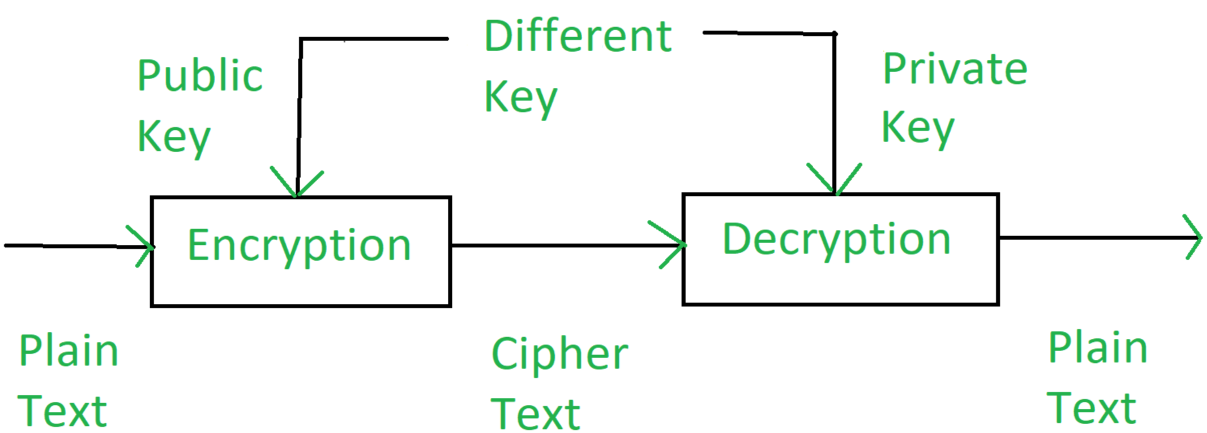
Role of Key

In **cryptography**, a **key** is a piece of information (a parameter) that determines the functional output of a **cryptographic** algorithm.

For **encryption** algorithms, a **key** specifies the transformation of plaintext into ciphertext, and vice versa for decryption algorithms.



Symmetric Cryptography



Asymmetric Cryptography

Various Ciphers

1. Caesar Cipher
2. Vigenere Cipher
3. Affine Cipher
4. Playfair Cipher
5. Pigpen Cipher
6. ADFGVX Cipher
7. Vernam Cipher
8. Hill Cipher
9. Digraph Cipher
10. Rotor Cipher
11. Book Cipher
12. Decimation

1. **Rail fence Cipher**
2. **Keyless transposition Cipher**
3. **Keyed transposition Cipher**
4. **Double Transposition Cipher**

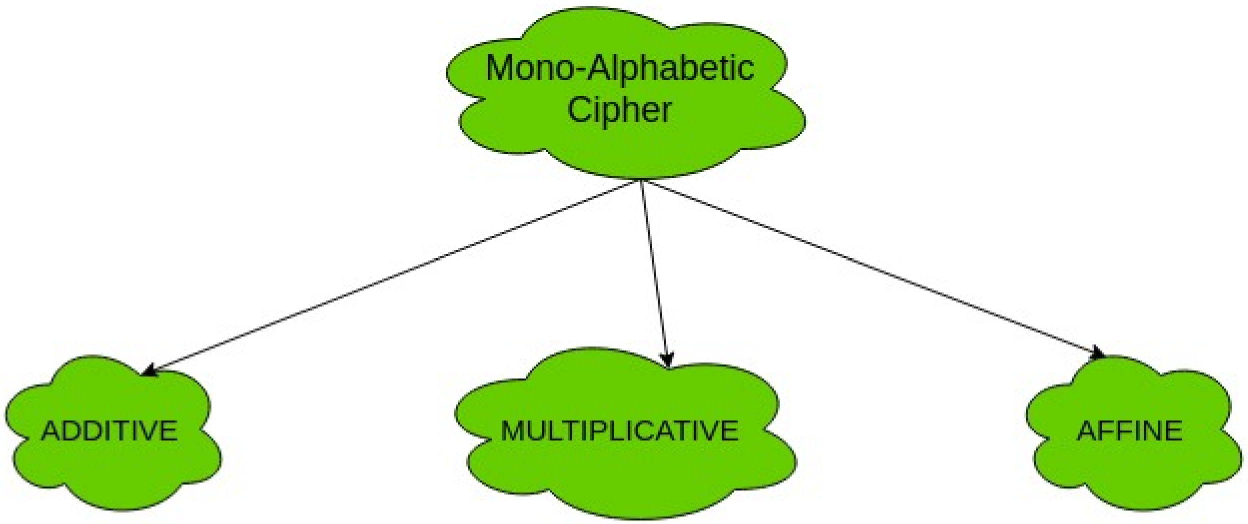
Digraph Cipher

- Playfair Cipher
- Hill cipher

Transposition Cipher

1. **Keyless transposition Cipher**
2. **Keyed transposition Cipher**
3. **Double Transposition Cipher**

Types of mono-alphabetic ciphers are:



Caesar Cipher

- earliest known substitution cipher
- by Julius Caesar
- first attested use in military affairs
- replaces each letter by 3rd letter on
- example:

  meet me after the toga party

  PHHW PH DIWHU WKH WRJD SDUWB

Caesar Cipher

- can define transformation as:

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
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**

- mathematically give each letter a number

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
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**

- then have Caesar cipher as:

$$c = \mathrm{E}(p) = (p + k) \bmod (26)$$

$$p = \mathrm{D}(\mathrm{c}) = (\mathrm{c} - k) \bmod (26)$$

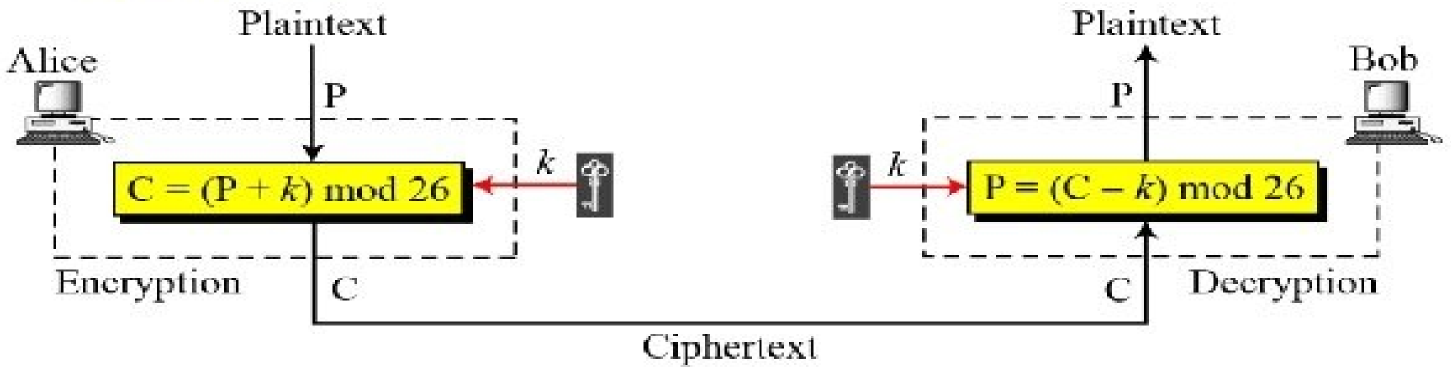
Cryptanalysis of Caesar Cipher

- only have 26 possible ciphers
  - A maps to A,B,..Z
- could simply try each in turn
- a **brute force search**
- given ciphertext, just try all shifts of letters
- do need to recognize when have plaintext

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

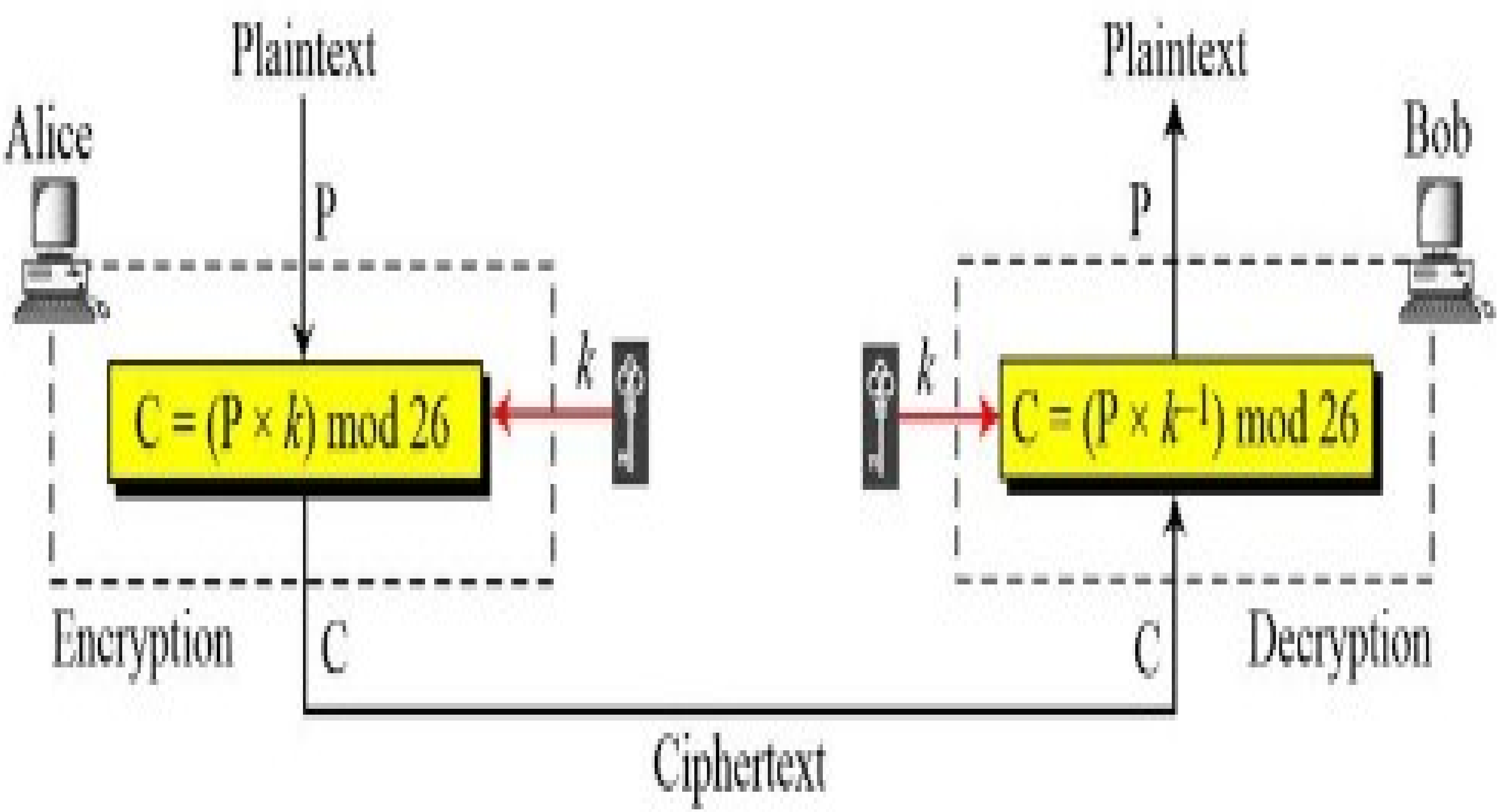
Multiplicative Cipher

- The multiplicative cipher is similar to additive cipher except the fact that the key bit is multiplied to the plain-text symbol during encryption. Likewise, the cipher-text is multiplied by the multiplicative inverse of key for decryption to obtain back the plain-text.

  $C = (M * k) \bmod n$
  $M = (C * k^{-1}) \bmod n$

- where,
  k^{-1} -> multiplicative inverse of k (key)
- The key space of multiplicative cipher is 12. Thus, it is also not very secure.

Multiplicative Cipher



Encryption

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

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

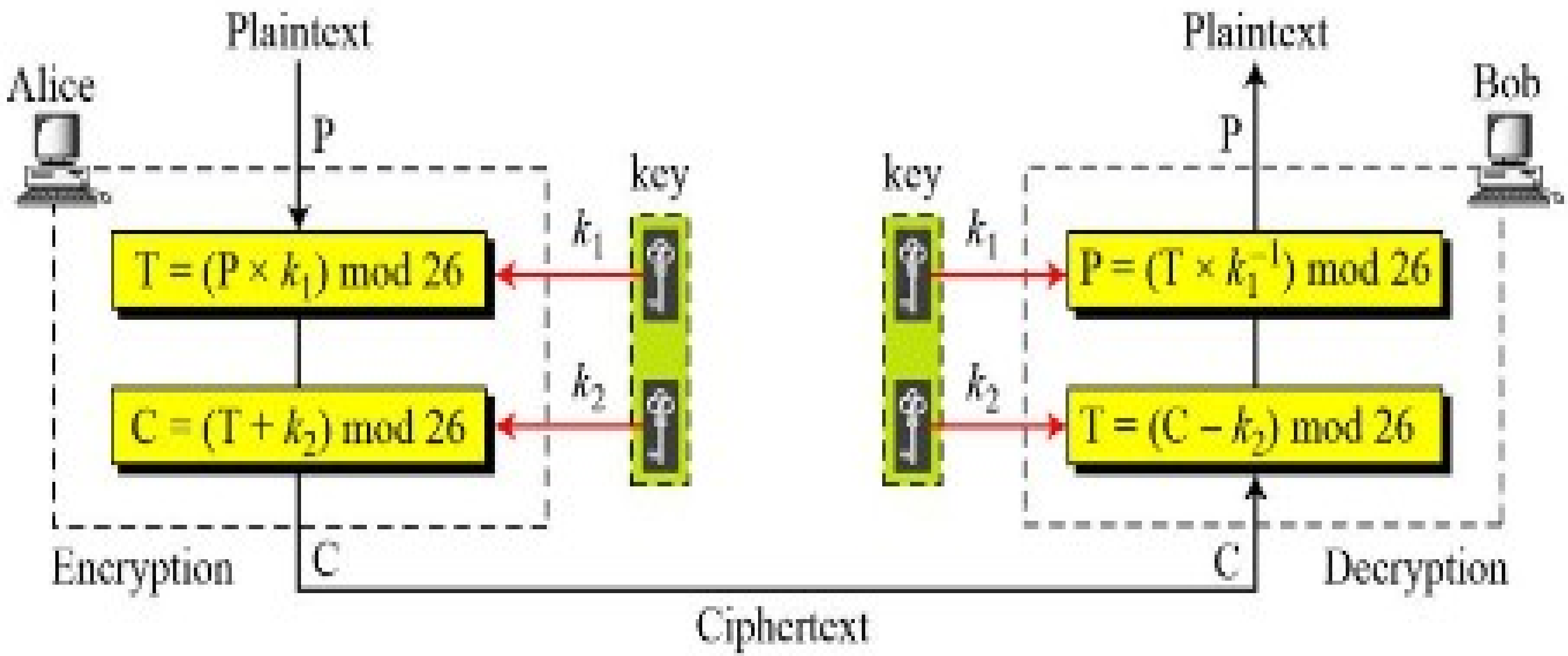
Plaintext: Letters → Numeric Value	Encryption: (P * K) mod 26	Ciphertext: Numeric Value → letters
Plaintext: H = 07	Encryption: (07*07)mod 26	Ciphertext: 23= X
Plaintext: E = 04	Encryption: (04*07)mod 26	Ciphertext: 02 = C
Plaintext: L = 11	Encryption: (11*07)mod 26	Ciphertext: 25 = Z
Plaintext: L =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



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

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…

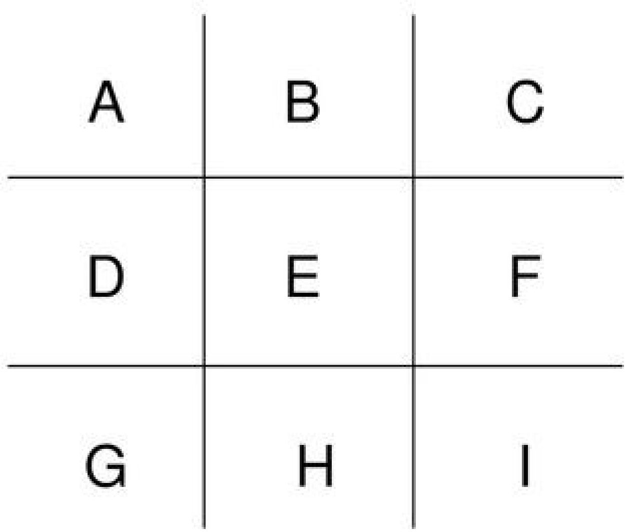
Use the affine cipher to decrypt the message "ZEBBW" with the key pair (7, 2) in modulus 26.

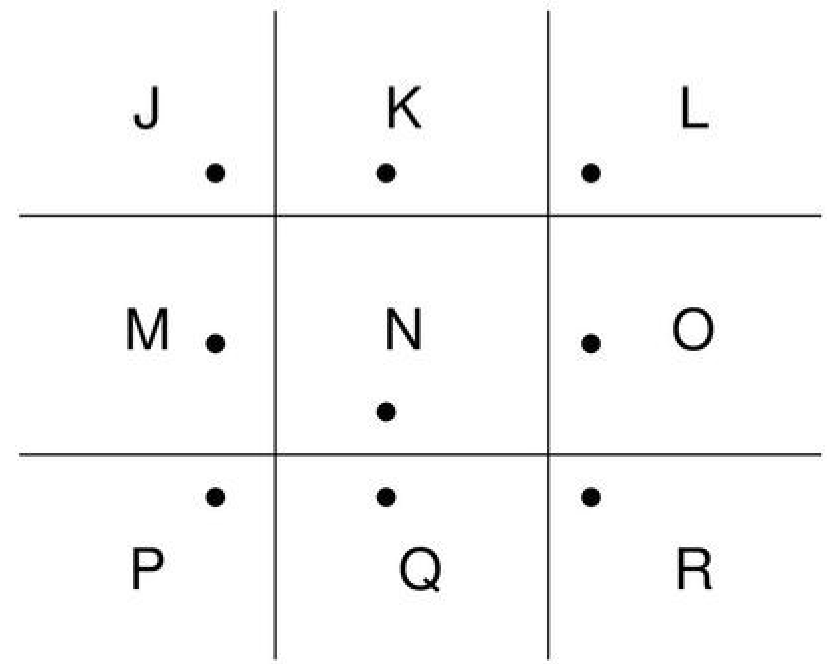
C: Z $\rightarrow$ 25	Decryption: $((25 - 2) \times 7^{-1}) \bmod 26$	P:07 $\rightarrow$ h
C: E $\rightarrow$ 04	Decryption: $((04 - 2) \times 7^{-1}) \bmod 26$	P:04 $\rightarrow$ e
C: B $\rightarrow$ 01	Decryption: $((01 - 2) \times 7^{-1}) \bmod 26$	P:11 $\rightarrow$ l
C: B $\rightarrow$ 01	Decryption: $((01 - 2) \times 7^{-1}) \bmod 26$	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 $k_2 = 0$.

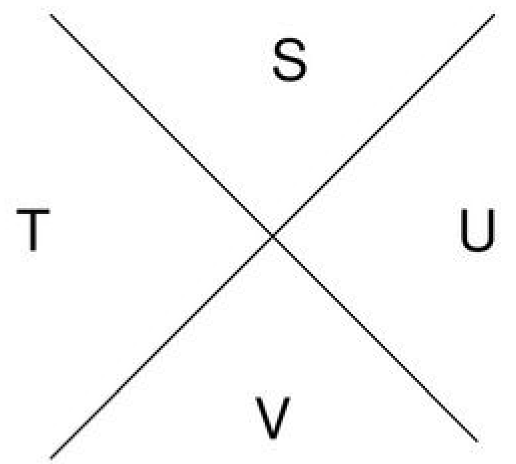
Pigpen Cipher

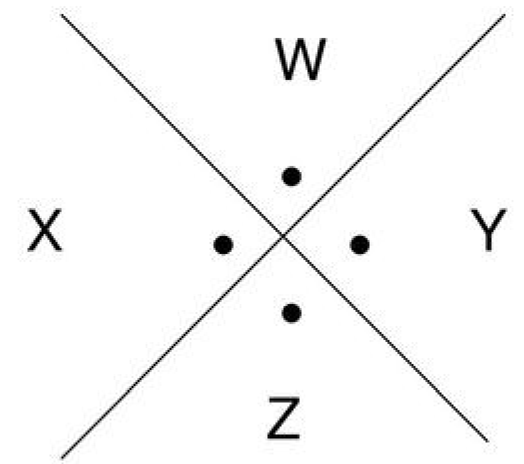
- Pigpen cipher is a variation on letter substitution
- Alphabets are arranged as follows:



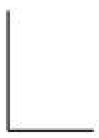


Pigpen Cipher diagram (cont'd)

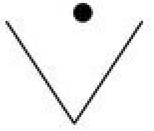




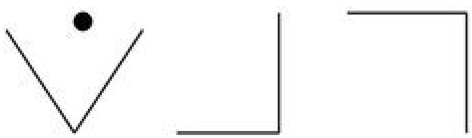
A = 

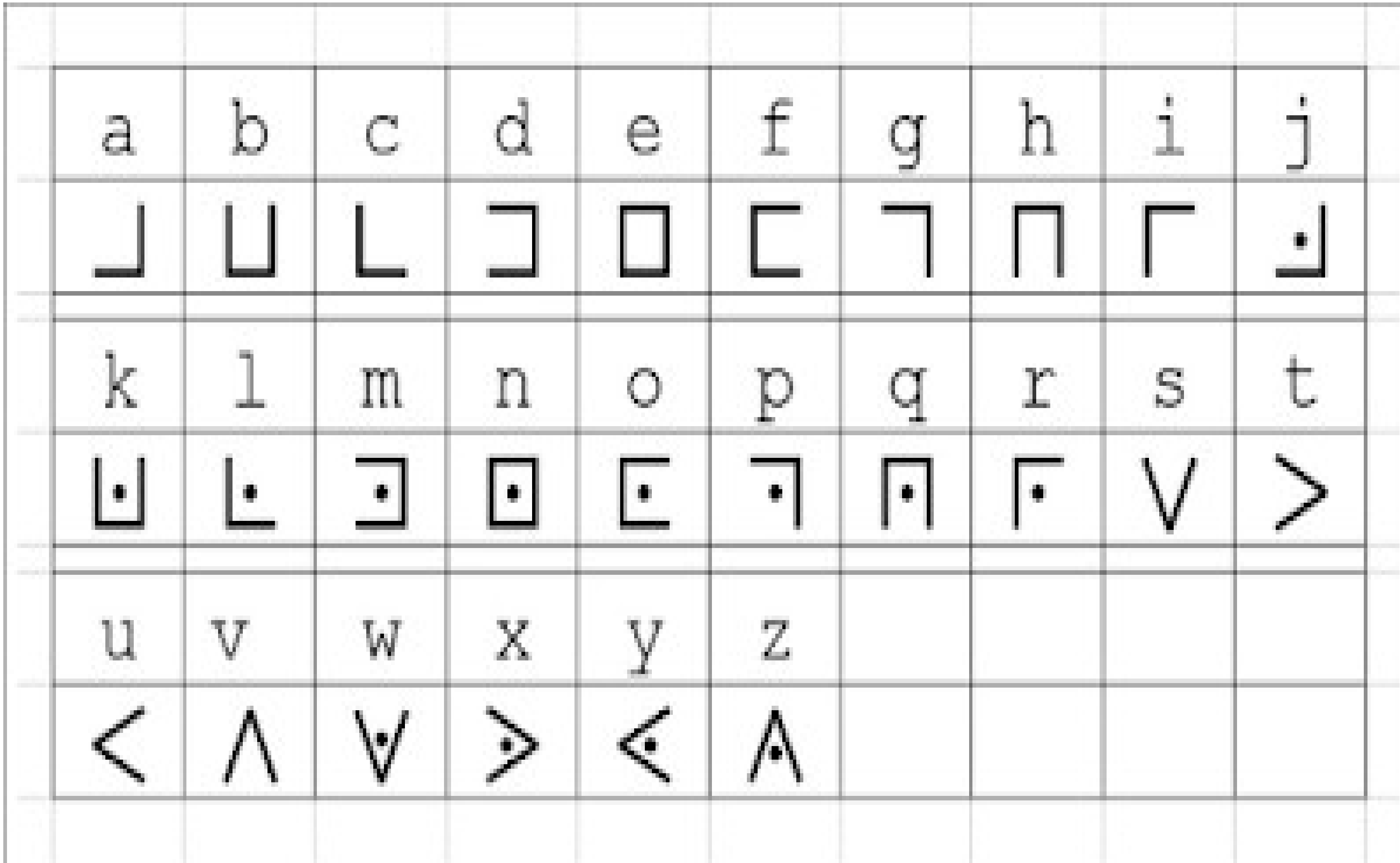
C = 

G = 

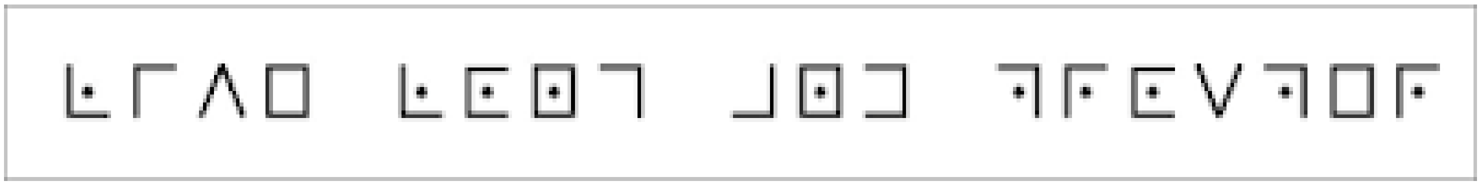
W = 

Pigpen Cipher

- Alphabets will be represented by the corresponding diagram
- E.g., WAG would be 
- This is a weak cipher


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

Decode the following pigpen ciphertext:



Encode the following message using the pigpen cipher:

the truth is out there