Cryptosystem

Encryption Decryption

M : plaintext (original message)

C : ciphertext (Secret message)

Example: Decrypt the message

"WRGDB LV IULGDB"

"today is friday"

② Shift ciphers:

Encryption

$C = m + k \pmod{26}$

(k should be a secret)

Decryption

$m = C - k \pmod{26}$

Example: Use shift cipher with key k=10 to encrypt the word "weekend". GOOUOXN

Example:

A shift cipher is used to encrypt "math" into "KYRF". Find the key.

$C = m + k \pmod{26}$

$10 = 12 + k \pmod{26}$

$K = 10 - 12 \pmod{26}$

$k = -2 \pmod{26}$

$k = 24$.

Example: Fatima used the shift cipher and came up with the following ciphertext.

"OXMEE" (K=12)

3 - Affine Cipher

Encryption

$C = ax + k \pmod{26}$

Decryption

$m = a'(C - k) \pmod{26}$

a	1	3	5	7	9	11	15	17	19	21	23	25
a'	1	9	21	15	3	19	7	23	11	5	17	25

R.H.S $= a'(C - k) \pmod{26} = a'(a m + k - k) \pmod{26}$

$= a' a m \pmod{26}$.

$= m \pmod{26} = m =$ L.H.S

R.H.S $= C - K \pmod{26}$

$= m + k - k \pmod{26}$

$= m \pmod{26}$

$= m =$ L.H.S

Example: Encrypt "car" using affine cipher with a=3, k=17

	c	a	r
m	2	0	17
am+k	23	17	68
am+k mod 26	23	17	16
	"X	R	Q"

Example:

Decrypt "ZVW" using a=11, k=9.

$m = a'(C - k) \pmod{26}$

$= 19(C - 9) \pmod{26}$

	Z	V	W
C	25	21	22
19(C-9) mod 26	304	228	247
	18	20	13
	"S	U	N"