

Lec. 4

5-Affine cipher

Affine cipher is a classical cipher, which is based on a certain equation according to two key. The key are different length, first one has inverse number for decryption equation. A second one is smaller than first one.

Encryption function:

$$Y = a \cdot x + b \pmod{26} \dots\dots\dots (1)$$

The possible values that a could be are 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, and 25.

| Table (1): inverse of a | | | | | | | | | | | |
|-------------------------|---|----|----|---|----|----|----|----|----|----|----|
| 1 | 3 | 5 | 7 | 9 | 11 | 15 | 17 | 19 | 21 | 23 | 25 |
| 1 | 9 | 21 | 15 | 3 | 19 | 7 | 23 | 11 | 5 | 17 | 25 |

Decryption function :

$$X = \text{inv}(a) (y - b) \pmod{26} \dots\dots\dots (2)$$

Example: the plaintext to be encrypted is "AFFINE CIPHER" $a=5$ $b=8$

| | | | | | | | | | | | | |
|--------------|---|----|----|----|----|----|----|----|----|----|----|----|
| plaintext: | A | F | F | I | N | E | C | I | P | H | E | R |
| x: | 0 | 5 | 5 | 8 | 13 | 4 | 2 | 8 | 15 | 7 | 4 | 17 |
| 5x+8 | 8 | 33 | 33 | 48 | 73 | 28 | 18 | 48 | 83 | 43 | 28 | 93 |
| (5x+8)mod 26 | 8 | 7 | 7 | 22 | 21 | 2 | 18 | 22 | 5 | 17 | 2 | 15 |
| cipher text: | I | H | H | W | V | C | S | W | F | R | C | P |

The cipher to decryption:

| | | | | | | | | | | | | |
|-------------------|---|-----|-----|-----|-----|------|-----|-----|-----|-----|------|-----|
| ciphertext: | I | H | H | W | V | C | S | W | F | R | C | P |
| y: | 8 | 7 | 7 | 22 | 21 | 2 | 18 | 22 | 5 | 17 | 2 | 15 |
| 21(y-8): | 0 | -21 | -21 | 294 | 273 | -126 | 210 | 294 | -63 | 189 | -126 | 147 |
| (21(y-8)) mod 26: | 0 | 5 | 5 | 8 | 13 | 4 | 2 | 8 | 15 | 7 | 4 | 17 |
| plaintext: | A | F | F | I | N | E | C | I | P | H | E | R |

6) Transposition:

means a management of letters according to some schema. i.e. rearrange bits or characters in the data.

1. The plaintext was written into the figure according to some (written) path.
2. The cipher text was taken off the figure according to some (take off) path.
3. The key consisted of the figure together with the written in & take off path.

Transposition Types:

1) Simple transposition (columnar transposition):

The plaintext can be written into a matrix by rows the cipher text can obtain by taking the columns in some order.

Example 1 :

CRYPTOGRAPHY = plain text

3 1 4 2 = key

(Encipherment process)

| (Encipherment process) | | | | | | | |
|------------------------|---|---|---|-------|---|-----|-----|
| 3 | 1 | 4 | 2 | | | | |
| C | R | Y | P | | | | |
| T | O | G | R | + key | → | ROP | PRY |
| A | P | H | Y | | | CTA | YGH |
| | | | | | | 1 | 2 |
| | | | | | | 3 | 4 |

| (Decipherment process) | | | |
|-------------------------------|---|---|---|
| key = 3 1 4 2 | | | |
| cipher text = ROP PRY CTA YGH | | | |
| | 1 | 2 | 3 |
| | | | 4 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 3 | 1 | 4 | 2 | | | | |
| C | R | Y | P | | | | |
| T | O | G | R | → | C | R | Y |
| A | P | H | Y | | P | R | Y |

Example 2:

Plaintext = this is transposition

Key = code

| | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|----------------|----------------|----------------|---|---|---|---|---|----|----|----|----|----------------|----|----|----|----|----|----|----|----|----|----|----|
| A | B | ¹ C | ² D | ³ E | F | G | H | I | J | K | L | M | N | ⁴ 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 |

Code=1 4 2 3

(Encipherment process)

| | | | |
|---|---|---|---|
| 1 | 4 | 2 | 3 |
| T | h | i | s |
| a | n | s | p |
| o | s | i | t |
| i | o | n | X |

cipher text = tiaoi itsin srptx hsnso

(Decipherment process)

cipher text = tiaoi itsin srptx hsnso

1 2 3 4

key= code = 1 4 2 3

| | | | |
|---|---|---|---|
| 1 | 4 | 2 | 3 |
| t | h | i | s |
| i | s | t | r |
| a | n | s | p |
| o | s | i | t |
| i | o | n | X |

2) A fixed period d with a permutation function.

$F: \mathbb{Z}_d \rightarrow \mathbb{Z}_d$

Example :

Plain text: CRYPTOGRAPHY , d=4 , f=2 4 1 3

(Encipherment process)

| | | |
|--------------------|---------|---------|
| d=4 | d=4 | d=4 |
| CRYP | TOGR | APHY |
| 1 2 3 4 | 1 2 3 4 | 1 2 3 4 |
| Cipher text : RPCY | ORTG | PYAH |

(Decipherment process)

Cipher text : RPCY ORTG PYAH , d=4, f= 2413

| | | |
|------------------|--------|---------|
| 2 4 1 3 | 2413 | 2413 |
| Plaintext : CRYP | TOGR | APHY |
| 1 2 3 4 | 12 3 4 | 1 2 3 4 |

Note: d represent block length

a) Simple Substitution

replace each plaintext letter with a corresponding cipher text letter.

1- Keyword

Example:

Keyword= CRYPTOGRAPHIC SYSTEM

P: 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

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

To encipher the plaintext= CRYPTOGRAPHY

ciphertext=YKXFNDGKCFAX

2- Shift alphabets

$F(a)=(a+k)\bmod n$ encipher

$M=(c-k)\bmod n$ decipher

i.e. $c=(p+k)\bmod 26$, where $a =0,.....z=25$

- this is called shifted alphabey by k position

- example (caesar cipher use $k=3$)

P= a b c d.....z

C= d e f g.....c

3-Multiplication

$$F(a)=(a.k)\bmod n$$

Or

$$C=(P.k)\bmod 26, \text{ where } \text{GCD}(k,26)=1$$

Example:

$$K=9$$

P: A B C D E F G H I J KZ

C: A J S B K T C L U D.....R