

Cryptanalysis of Affine Hill cipher

Course Code: COMP308.

Number of Research: 00405.


Presented To: د/ضياء نصر & د/حاتم بهيج

Department: Computer science.

Level : 3rd.

The Affine-Hill cipher.

- Plaintexts and ciphertexts spaces are $M = C = (Z_{26})^n$.
- Key space is $K = \{ (a,b): a \text{ is } n \times n \text{ invertible matrix over } Z_{26}, \text{ and } b \in (Z_{26})^n \}$
- Encryption: $E_{(a,b)}(m) = ma + b \pmod{26}; m \in (Z_{26})^n$.
- Decryption: $D_{(a,b)}(c) = (c-b) a^{-1} \pmod{26}; c \in (Z_{26})^n$ where $a^{-1} * a \equiv a * a^{-1} \equiv 1 \pmod{26}$.
- To encrypt any plaintext we have 2 key one 'a' is matrix $n \times n$ over (Z_{26}) and 'b' is integer number $\in (Z_{26})^n$ but we need to make 'b' matrix to can add 'b' to the result of "m*a" so we will multiplication 'b' in $\begin{bmatrix} 1 & 1 \end{bmatrix}$ or $\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$ and so on .
- To decrypt the ciphertext we have two key the same b and a^{-1}

 **Example: Suppose we want to encrypt the plaintext " July"**

and Suppose the key is 'a' = $\begin{bmatrix} 11 & 8 \\ 3 & 7 \end{bmatrix}$ and 'b' = 2.

 **Solution:**

- $\begin{bmatrix} 9 & 20 \end{bmatrix}$ (corresponding to " ju")
- $\begin{bmatrix} 11 & 24 \end{bmatrix}$ (corresponding to " ly").
- From encryption form: $E_{(a,b)}(m) = ma + b \pmod{26}$

○ Compute "ju" $\rightarrow [9 \ 20] * \begin{bmatrix} 11 & 8 \\ 3 & 7 \end{bmatrix} + 2 * [1 \ 1] \text{mod } 26 =$

$$[9 \ 20] * \begin{bmatrix} 11 & 8 \\ 3 & 7 \end{bmatrix} + [2 \ 2] \text{mod } 26 =$$

$$[99 + 60 \ 72 + 140] + [2 \ 2] \text{mod } 26$$

$$=[159 + 2 \ 212 + 2] \text{mod } 26 = [161 \ 214] \text{mod } 26 =$$

$$[5 \ 6] \rightarrow \text{"fg"}.$$

○ The encryption of "ju" is "fg"

○ Compute "ly" $\rightarrow [11 \ 24] * \begin{bmatrix} 11 & 8 \\ 3 & 7 \end{bmatrix} + 2 * [1 \ 1] \text{mod } 26 =$

$$[11 \ 24] * \begin{bmatrix} 11 & 8 \\ 3 & 7 \end{bmatrix} + [2 \ 2] \text{mod } 26 =$$

$$[121 + 72 \ 88 + 168] + [2 \ 2] \text{mod } 26 = [195 \ 258] \text{mod } 26$$

$$= [13 \ 24] \rightarrow \text{"ny"}.$$

○ The encryption of "ly" is "ny"

○ The encryption of "july" $\rightarrow \text{"fgny"}$

 **Example : from the previous example decrypt the ciphertext**

" fgny"

 **Solution :**

- In the first we need to find $a^{-1} = \begin{bmatrix} 7 & 18 \\ 23 & 11 \end{bmatrix}$ $b = 2 * [1 \ 1] = [2 \ 2]$.

- $[5 \ 6]$ (corresponding to " fg ").

- $[13 \ 24]$ (corresponding to " ny ").

- From decryption form : $D_{(a,b)}(c) = (c - b) a^{-1} \text{mod } 26$

- Compute " fg " \rightarrow [5 6]

$$([5 \ 6] - [2 \ 2]) * \begin{bmatrix} 7 & 18 \\ 23 & 11 \end{bmatrix} \bmod 26 = [3 \ 4] *$$

$$\begin{bmatrix} 7 & 18 \\ 23 & 11 \end{bmatrix} \bmod 26 = [113 \ 98] \bmod 26 = [9 \ 20] \rightarrow \text{"ju"}.$$

- The decryption of "fg" \rightarrow "ju".

- Compute " ny " \rightarrow [13 24]

$$([13 \ 24] - [2 \ 2]) * \begin{bmatrix} 7 & 18 \\ 23 & 11 \end{bmatrix} \bmod 26 = [11 \ 22] *$$

$$\begin{bmatrix} 7 & 18 \\ 23 & 11 \end{bmatrix} \bmod 26 = [583 \ 440] \bmod 26 = [11 \ 24]$$

\rightarrow "ly".

- The decryption of " ny " \rightarrow " ly ".

- The decryption of " fgny " \rightarrow " july "

the security of this cipher.

- **brute force attack.**

- if the matrix key is 2×2 over Z_{26} so can brute force on the key $26^4 \times 26$ of 'b' key , 26^5 is the fast operation for computer(breakable).
- if the matrix key is 3×3 over Z_{26} .

- let the computer make 10 million operation in one second.
- In one hour = $10000000 \times 3600 = 3.6 \times 10^{10}$ operation.
- In one day = $24 \times 3.6 \times 10^{10} = 8.64 \times 10^{11}$ operation.

- In one month = $30 * 8.64 * 10^{11} = 2.592 * 10^{13}$ operation.
- In 6 month = $6 * 2.592 * 10^{13} = 1.5552 * 10^{14}$ operation.
- and the matrix $3 * 3$ will take 26^9 for key 'a' and 26 for key 'b' then will take $26^9 * 26 = 26^{10} = 1.412 * 10^{14}$ operation.
- In the end to make a brute force when $n \geq 3$ it will take 6 month at least so it's unbreakable.

- **Known plaintext attack.**

- If I have some plaintext characters and his ciphertext characters I can find the key $\rightarrow (m_i, c_i)$ for some i , $E(m_i) = c_i$.
- if the key is $2 * 2$ matrix we must known at least 8 characters from plaintext and his ciphertext to make 4 equations to know the keys a and b.
- if the key is $3 * 3$ matrix we must known at least 18 characters from plaintext and his ciphertext to make equations to know the keys a and b .

- **Example on Known plaintext attack.**

- the ciphertext is " wpnbcjpenpcpgj " and we have some letters from plaintext " theendof " and their corresponding in cipher is " wpnbcjpe " find the keys and the complete plaintext.

❖ Solution

- We will divide a plaintext to " th "=[19 7] , " ee " = [4 4] , " nd " = [13 3] , " of " = [14 5] , and Ciphertext to " wp " = [22 15] , " nb " = [13 1] , " cj " = [2 9] , " pe " = [15 4] .

- We know $C=M*a+b*[e \ e] \bmod 26$

- "wp" corresponding "th" →

$$[22 \ 15] = [19 \ 7] * \begin{bmatrix} a & b \\ c & d \end{bmatrix} + [e \ e] \bmod 26 \rightarrow [22 \ 15] =$$

$$[19a+7c \quad 19b+7d] + [e \ e] \bmod 26 \rightarrow (1)$$

- "nb" corresponding "ee" →

$$[13 \ 1] = [4 \ 4] * \begin{bmatrix} a & b \\ c & d \end{bmatrix} + [e \ e] \bmod 26 \rightarrow [13 \ 1] =$$

$$[4a + 4c \quad 4b + 4d] + [e \ e] \bmod 26 \rightarrow (2)$$

- By subtract (1) and (2) →

$$[9 \ 14] = [15a + 3c \quad 15b + 3d] \bmod 26 \rightarrow (5)$$

- "cj" corresponding "nd" →

$$[2 \ 9] = [13 \ 3] * \begin{bmatrix} a & b \\ c & d \end{bmatrix} + [e \ e] \bmod 26 \rightarrow$$

$$[2 \ 9] = [13a+3c \ 13b+3d] + [e \ e] \bmod 26 \rightarrow (3)$$

- "pe" corresponding "of" →

$$[15 \ 4] = [14 \ 5] * \begin{bmatrix} a & b \\ c & d \end{bmatrix} + [e \ e] \bmod 26 \rightarrow$$

$$[15 \ 4] = [14a + 5c \quad 14b + 5d] + [e \ e] \bmod 26 \rightarrow (4)$$

- By subtract (3) and (4) $\rightarrow [13 \ 5] = [25a + 24c \ 25b + 24d] \mod 26 \rightarrow (6)$
- The equations from 5,6
- $\begin{cases} 15a + 3c = 9 \mod 26 \\ 25a + 24c = 13 \mod 26 \end{cases} \rightarrow (7) \text{ and } \begin{cases} 15b + 3d = 14 \mod 26 \\ 25b + 24d = 5 \mod 26 \end{cases} \rightarrow (8)$
- By using equations (7) and make substitution in 'a' and 'c' we will find a=5 and c=4
- By using equations (8) and make substitution in 'b' and 'd' we will find b=17 and d=15
- The key 'a' = $\begin{bmatrix} 5 & 17 \\ 4 & 15 \end{bmatrix}$
- By substitution by 'a' in any equation to find 'b' key;
- $[22 \ 15] = [19 \ 7] * \begin{bmatrix} 5 & 17 \\ 4 & 15 \end{bmatrix} + [e \ e] \mod 26 \rightarrow$
 $[22 \ 15] = [19 \ 12] + [e \ e] \mod 26 \rightarrow$
 $[22 \ 15] - [19 \ 12] = [e \ e] \mod 26 \rightarrow [e \ e] = [3 \ 3] \rightarrow$
'b'=3.
- In the end the keys is 'a' = $\begin{bmatrix} 5 & 17 \\ 4 & 15 \end{bmatrix}$ and 'b' = 3
- We will use the keys to know the complete plaintext
- "np" corresponding [13 15]
- "cp" corresponding [2 15]

- "gj" corresponding [6 9]
- We need inverse of 'a' to decryption 'a' = $\begin{bmatrix} 5 & 17 \\ 4 & 15 \end{bmatrix} \rightarrow$
 $a^{-1} = \begin{bmatrix} 17 & 5 \\ 18 & 23 \end{bmatrix}$ and $b = [3 \ 3]$
- We will use $M = (c - b) * a^{-1} \bmod 26$ to decryption.
- "np" $\rightarrow M = ([13 \ 15] - [3 \ 3]) * \begin{bmatrix} 17 & 5 \\ 18 & 23 \end{bmatrix} \bmod 26 \rightarrow [10 \ 12]$
 $* \begin{bmatrix} 17 & 5 \\ 18 & 23 \end{bmatrix} \bmod 26 = [22 \ 14] \rightarrow \text{"wo"}.$
- "cp" $\rightarrow M = ([2 \ 15] - [3 \ 3]) * \begin{bmatrix} 17 & 5 \\ 18 & 23 \end{bmatrix} \bmod 26 \rightarrow [25 \ 12]$
 $* \begin{bmatrix} 17 & 5 \\ 18 & 23 \end{bmatrix} \bmod 26 = [17 \ 11] \rightarrow \text{"rl"}.$
- "gj" $\rightarrow M = ([6 \ 9] - [3 \ 3]) * \begin{bmatrix} 17 & 5 \\ 18 & 23 \end{bmatrix} \bmod 26 \rightarrow [3 \ 6]$
 $* \begin{bmatrix} 17 & 5 \\ 18 & 23 \end{bmatrix} \bmod 26 = [3 \ 23] \rightarrow \text{"dx"}.$
- " wpnbcjpenpcpgj " corresponding " theendofworldx ".

The program

- ❖ my program work with key1 'a' is 2*2 or 3*3 matrix in first the user enter the n of matrix if 2 or 3 and enter the known plaintext and corresponding ciphertext without any space to find the key1 and key2 and to find the inverse of key1 to decryption the complete cipher to know the complete plaintext my program.

- ❖ If we work with key matrix 2×2 when enter all ciphertext must be with even length
- ❖ If we work with key matrix 3×3 when enter all ciphertext the length of all cipher must be divided by 3.
- ❖ The run of program.
- ❖ If matrix is 2×2

```

E:\Third_Year Semester_2\Crypto\programs\00405\Debug\00405.exe
Enter matrix Key 2 or 3 : 2
Enter 8 char from known plaintext without space :
TheEndOf
=====
Enter corresponding ciphertext without space :
wpnbcjpe
=====
The first Key is :
 5 17
 4 15
=====
The second Key is :
13 31
=====
The inverse of first Key is :
17 5
18 23
=====
Enter all cipher without space and with MaxLength 500 :
wpnbcjpenpcpgj
=====
The plaintext after decryption :
THEENDOFWORLDX
=====
press 1 to repeat again
=====
press another number to exit
8
Press any key to continue . . . _

```

If matrix 3×3 : -

Plaintext : - "tomorrowatthesunri"

Corresponding ciphertext : - "bcqchnvrlgiwnptrut"

The all cipher is: - " bcqchnvrlgiwnptrutpndjtpfefkla "

The all plain is: - "the tomorrow at the sun rise we will meet"

```
E:\Third_Year Semester_2\Crypto\programs\00405\Debug\00405.exe
Enter matrix Key 2 or 3 : 3
Enter 18 char from known plaintext without space :
tomorrowatthesunri
=====
Enter corresponding ciphertext without space :
bcqchnvrlgiwnptrut
=====
The first Key is :
 2  3  1
 2  0  1
 1  4  5
=====
The second Key is :
11  1 11
=====
The inverse of first Key is :
 4 11 23
 9 17  0
18  5  6
=====
Enter all cipher without space and with MaxLength 500 :
bcqchnvrlgiwnptrutpndjtpfefkla
=====
The plaintext after decryption :
TOMORROWATTHE SUNRISE WE WILL MEET
=====
press 1 to repeat again
=====
press another number to exit
5
Press any key to continue . . . _
```

References :-

- Introduction to Cryptography with Java Applets By David Bishop
- Cryptography: Theory and Practice By Douglas Robert Stinson,
Maura Paterson