قسم هندسة تقنيات الحاسوب
المرحلة الرابعة

HILL CIPHER METHOD

Lecture 10

Introduction

The computation used in the Hill cipher is based on linear algebra techniques. As time progressed, the study of cryptography continued to mature and, more recently, began to involve higher level mathematics. With this more advanced math came more advanced ciphers based on the idea of encryption and decryption keys. Encryption keys are a special value or set of values used in an encryption algorithm to convert a plaintext into a cipher text. A decryption key is the opposite. Decryption keys are used as part of a decryption algorithm to convert the cipher text back into the original plaintext.

Introduction

Encryption Low

$$C = (k * p) \bmod 26$$

Decryption Low

$$P = (k^{-1} * C) \bmod 26$$

- **C** is the cipher text
- **k** is the key matrix or encryption matrix
- $\mathbf{k^{-1}}$ inverse key matrix or decryption matrix
- **P** is the plaintext

Example 1

Use Hill cipher method to encrypt the plaintext ***"TOP SECRET MESSAGE"*** with encryption matrix

$$\begin{bmatrix} 3 & 2 \\ 5 & 7 \end{bmatrix}$$

Answer

- **Encryption process with the Hill Cipher:**

Encrypting text using the Hill cipher is accomplished by breaking a given plaintext into blocks of size *n* (where *n* is an integer), writing these blocks as column vectors, if you have an odd number of letters, repeat the last letter, and then multiplying these column vectors by any invertible *n* x *n* matrix. The

Answer

The encryption matrix must be invertible because its inverse will be used to decrypt the cipher texts created with the Hill cipher and this encryption matrix. The inevitability of the encryption matrix allows us to say that its determinant must not be 0. The determinant of the encryption matrix must also be relatively prime to the size of the alphabet.

Answer

Compute the determinate of the matrix

This matrix has the determinant (3*7) – (2*5) = 21 – 10 = 11. Since 11 is ≠ 0, this matrix is invertible. 11 is also relatively prime to 26. These two qualities satisfy the requirements listed previously, making this encryption matrix a valid choice for use in the Hill cipher.

Answer

Split the plaintext into blocks of size 2 (ignoring spaces), determine the letters' numerical values, and align these as column vectors. If the length of the plaintext is not evenly divisible by 2, add a previously decided character to the end of the string until the plaintext is evenly divisible by 2.

Answer

Divide the message (***TOP SECRET MESSAGE***)to pairs

$$\begin{vmatrix} T \\ O \end{vmatrix} = \begin{vmatrix} 19 \\ 14 \end{vmatrix} \quad \begin{vmatrix} P \\ S \end{vmatrix} = \begin{vmatrix} 15 \\ 18 \end{vmatrix} \quad \begin{vmatrix} E \\ C \end{vmatrix} = \begin{vmatrix} 4 \\ 2 \end{vmatrix} \quad \begin{vmatrix} R \\ E \end{vmatrix} = \begin{vmatrix} 17 \\ 4 \end{vmatrix} \quad \begin{vmatrix} T \\ M \end{vmatrix} = \begin{vmatrix} 19 \\ 12 \end{vmatrix}$$

$$\begin{vmatrix} E \\ S \end{vmatrix} = \begin{vmatrix} 4 \\ 18 \end{vmatrix} \quad \begin{vmatrix} S \\ A \end{vmatrix} = \begin{vmatrix} 18 \\ 0 \end{vmatrix} \quad \begin{vmatrix} G \\ E \end{vmatrix} = \begin{vmatrix} 6 \\ 4 \end{vmatrix}$$

Answer

- Multiply each of these column vectors by the encryption matrix and take mod 26 of the result. The encryption formula for hill method is

$$C = (k * p) \bmod 26$$

TOP SECRET MESSAGE

C = (k * p) mod 26

$$\begin{vmatrix} T \\ O \end{vmatrix} = \begin{vmatrix} 19 \\ 14 \end{vmatrix}$$

$$\begin{vmatrix} 3 & 2 \\ 5 & 7 \end{vmatrix} \begin{vmatrix} 19 \\ 14 \end{vmatrix} = \begin{vmatrix} (3 * 19) + (2 * 14) \\ (5 * 19) + (7 * 14) \end{vmatrix} = \begin{vmatrix} 85 \\ 193 \end{vmatrix} (\text{mod } 26) = \begin{vmatrix} 7 \\ 11 \end{vmatrix} = \begin{vmatrix} H \\ L \end{vmatrix}$$

TOP SECRET MESSAGE

C = (k * p) mod 26

$$\begin{vmatrix} P \\ S \end{vmatrix} = \begin{vmatrix} 15 \\ 18 \end{vmatrix}$$

$$\begin{vmatrix} 3 & 2 \\ 5 & 7 \end{vmatrix} \begin{vmatrix} 15 \\ 18 \end{vmatrix} = \begin{vmatrix} (3 * 15) + (2 * 18) \\ (5 * 15) + (7 * 18) \end{vmatrix} = \begin{vmatrix} 81 \\ 201 \end{vmatrix} (\text{mod } 26) = \begin{vmatrix} 3 \\ 19 \end{vmatrix} = \begin{vmatrix} D \\ T \end{vmatrix}$$

TOP SECRET MESSAGE

C = (k * p) mod 26

$$\begin{vmatrix} E \\ C \end{vmatrix} = \begin{vmatrix} 4 \\ 2 \end{vmatrix}$$

$$\begin{vmatrix} 3 & 2 \\ 5 & 7 \end{vmatrix} \begin{vmatrix} 4 \\ 2 \end{vmatrix} = \begin{vmatrix} (3*4)+(2*2) \\ (5*4)+(7*2) \end{vmatrix} = \begin{vmatrix} 16 \\ 34 \end{vmatrix} (\text{mod } 26) = \begin{vmatrix} 16 \\ 8 \end{vmatrix} = \begin{vmatrix} Q \\ I \end{vmatrix}$$

TOP SECRET MESSAGE

C = (k * p) mod 26

$$\begin{vmatrix} R \\ E \end{vmatrix} = \begin{vmatrix} 17 \\ 4 \end{vmatrix}$$

$$\begin{vmatrix} 3 & 2 \\ 5 & 7 \end{vmatrix} \begin{vmatrix} 17 \\ 4 \end{vmatrix} = \begin{vmatrix} (3 * 17) + (2 * 4) \\ (5 * 17) + (7 * 4) \end{vmatrix} = \begin{vmatrix} 59 \\ 113 \end{vmatrix} (\text{mod } 26) = \begin{vmatrix} 7 \\ 9 \end{vmatrix} = \begin{vmatrix} H \\ J \end{vmatrix}$$

TOP SECRET MESSAGE

C = (k * p) mod 26

$$\begin{vmatrix} T \\ M \end{vmatrix} = \begin{vmatrix} 19 \\ 12 \end{vmatrix}$$

$$\begin{vmatrix} 3 & 2 \\ 5 & 7 \end{vmatrix} \begin{vmatrix} 19 \\ 12 \end{vmatrix} = \begin{vmatrix} (3 * 19) + (2 * 12) \\ (5 * 19) + (7 * 12) \end{vmatrix} = \begin{vmatrix} 81 \\ 179 \end{vmatrix} (\text{mod } 26) = \begin{vmatrix} 3 \\ 23 \end{vmatrix} = \begin{vmatrix} D \\ X \end{vmatrix}$$

TOP SECRET MESSAGE

C = (k * p) mod 26

$$\begin{vmatrix} E \\ S \end{vmatrix} = \begin{vmatrix} 4 \\ 18 \end{vmatrix}$$

$$\begin{vmatrix} 3 & 2 \\ 5 & 7 \end{vmatrix} \begin{vmatrix} 4 \\ 18 \end{vmatrix} = \begin{vmatrix} (3*4)+(2*18) \\ (5*4)+(7*18) \end{vmatrix} = \begin{vmatrix} 48 \\ 146 \end{vmatrix} (\text{mod } 26) = \begin{vmatrix} 22 \\ 16 \end{vmatrix} = \begin{vmatrix} W \\ Q \end{vmatrix}$$

TOP SECRET MESSAGE

C = (k * p) mod 26

$$\begin{vmatrix} S \\ A \end{vmatrix} = \begin{vmatrix} 18 \\ 0 \end{vmatrix}$$

$$\begin{vmatrix} 3 & 2 \\ 5 & 7 \end{vmatrix} \begin{vmatrix} 18 \\ 0 \end{vmatrix} = \begin{vmatrix} (3 * 18) + (2 * 0) \\ (5 * 18) + (7 * 0) \end{vmatrix} = \begin{vmatrix} 54 \\ 90 \end{vmatrix} (\text{mod } 26) = \begin{vmatrix} 2 \\ 12 \end{vmatrix} = \begin{vmatrix} C \\ M \end{vmatrix}$$

TOP SECRET MESSAGE

C = (k * p) mod 26

$$\begin{vmatrix} G \\ E \end{vmatrix} = \begin{vmatrix} 6 \\ 4 \end{vmatrix}$$

$$\begin{vmatrix} 3 & 2 \\ 5 & 7 \end{vmatrix} \begin{vmatrix} 6 \\ 4 \end{vmatrix} = \begin{vmatrix} (3*6)+(2*4) \\ (5*6)+(7*4) \end{vmatrix} = \begin{vmatrix} 26 \\ 58 \end{vmatrix} (\text{mod } 26) = \begin{vmatrix} 0 \\ 6 \end{vmatrix} = \begin{vmatrix} A \\ G \end{vmatrix}$$

Cipher text:

"HLDTQIHJDXWQCMAG"

Decryption process

- We are interested in how the party receiving a secret message encoded by the Hill cipher can decode it into the original plaintext. As previously described, the Hill cipher is based on matrix multiplication and any encryption matrix used in the Hill cipher must be invertible.The process is the same as encryption, but with the inverse matrix instead of the original encryption matrix.
- Decryption of the cipher text “HLDTQIHJDXWQCMAG” with the 2x2 encryption matrix previously defined would go as follows:

Example 2

Use hill cipher method to decryption the cipher text “HLDTQIHJDXWQCMAG” with the 2x2 key

encryption $\begin{bmatrix} 3 & 2 \\ 5 & 7 \end{bmatrix}$

Decryption process

- Split the cipher text into blocks of 2, determine the letters' numerical values, and align these as column vectors.

$$\begin{vmatrix} H \\ L \end{vmatrix} = \begin{vmatrix} 7 \\ 11 \end{vmatrix} \quad \begin{vmatrix} D \\ T \end{vmatrix} = \begin{vmatrix} 3 \\ 19 \end{vmatrix} \quad \begin{vmatrix} Q \\ I \end{vmatrix} = \begin{vmatrix} 16 \\ 8 \end{vmatrix} \quad \begin{vmatrix} H \\ J \end{vmatrix} = \begin{vmatrix} 7 \\ 9 \end{vmatrix} \quad \begin{vmatrix} D \\ X \end{vmatrix} = \begin{vmatrix} 3 \\ 23 \end{vmatrix}$$

$$\begin{vmatrix} W \\ Q \end{vmatrix} = \begin{vmatrix} 22 \\ 16 \end{vmatrix} \quad \begin{vmatrix} C \\ M \end{vmatrix} = \begin{vmatrix} 2 \\ 12 \end{vmatrix} \quad \begin{vmatrix} A \\ G \end{vmatrix} = \begin{vmatrix} 0 \\ 6 \end{vmatrix}$$

Decryption process

Find the inverse key

$$\det\left(\begin{vmatrix} 3 & 2 \\ 5 & 7 \end{vmatrix}\right) = (3*7) - (2*5) = 11$$

$$11^{-1} \bmod 26 = 19$$

$$19 \begin{vmatrix} 7 & -2 \\ -5 & 3 \end{vmatrix} = \begin{vmatrix} 133 & -38 \\ -95 & 57 \end{vmatrix} (\text{mod } 26) = \begin{vmatrix} 3 & 14 \\ 9 & 5 \end{vmatrix}$$

$$K^{-1} = \begin{vmatrix} 3 & 14 \\ 9 & 5 \end{vmatrix}$$

Decryption process

- Multiply each of these column vectors above by the decryption matrix calculated in step 1 and take mod 26 of the result. The decryption formula for hill method is

$$P = (k^{-1} * C) \bmod 26$$

HLDTQIHJDXWQCMAG

$$P = (k^{-1} * C) \bmod 26$$

$$\begin{vmatrix} H \\ L \end{vmatrix} = \begin{vmatrix} 7 \\ 11 \end{vmatrix}$$

$$\begin{vmatrix} 3 & 14 \\ 9 & 5 \end{vmatrix} \begin{vmatrix} 7 \\ 11 \end{vmatrix} = \begin{vmatrix} (3*7)+(14*11) \\ (9*7)+(5*11) \end{vmatrix} = \begin{vmatrix} 175 \\ 118 \end{vmatrix} \bmod 26 = \begin{vmatrix} 19 \\ 14 \end{vmatrix} = \begin{vmatrix} T \\ O \end{vmatrix}$$

HLDTQIHJDXWQCMAG

$$P = (k^{-1} * C) \bmod 26$$

$$\begin{vmatrix} D \\ T \end{vmatrix} = \begin{vmatrix} 3 \\ 19 \end{vmatrix}$$

$$\begin{vmatrix} 3 & 14 \\ 9 & 5 \end{vmatrix} \begin{vmatrix} 3 \\ 19 \end{vmatrix} = \begin{vmatrix} (3*3)+(14*19) \\ (9*3)+(5*19) \end{vmatrix} = \begin{vmatrix} 275 \\ 122 \end{vmatrix} \bmod 26 = \begin{vmatrix} 15 \\ 18 \end{vmatrix} = \begin{vmatrix} P \\ S \end{vmatrix}$$

HLDTQIHJDXWQCMAG

$$P = (k^{-1} * C) \bmod 26$$

$$\begin{vmatrix} Q \\ I \end{vmatrix} = \begin{vmatrix} 16 \\ 8 \end{vmatrix}$$

$$\begin{vmatrix} 3 & 14 \\ 9 & 5 \end{vmatrix} \begin{vmatrix} 16 \\ 8 \end{vmatrix} = \begin{vmatrix} (3*16)+(14*8) \\ (9*16)+(5*8) \end{vmatrix} = \begin{vmatrix} 160 \\ 184 \end{vmatrix} \bmod 26 = \begin{vmatrix} 4 \\ 2 \end{vmatrix} = \begin{vmatrix} E \\ C \end{vmatrix}$$

HLDTQIHJDXWQCMAG

$$P = (k^{-1} * C) \bmod 26$$

$$\begin{vmatrix} H \\ J \end{vmatrix} = \begin{vmatrix} 7 \\ 9 \end{vmatrix}$$

$$\begin{vmatrix} 3 & 14 \\ 9 & 5 \end{vmatrix} \begin{vmatrix} 7 \\ 9 \end{vmatrix} = \begin{vmatrix} (3*7)+(14*9) \\ (9*7)+(5*9) \end{vmatrix} = \begin{vmatrix} 147 \\ 108 \end{vmatrix} \bmod 26 = \begin{vmatrix} 17 \\ 4 \end{vmatrix} = \begin{vmatrix} R \\ E \end{vmatrix}$$

HLDTQIHJDXWQCMAG

$$P = (k^{-1} * C) \bmod 26$$

$$\begin{vmatrix} D \\ X \end{vmatrix} = \begin{vmatrix} 3 \\ 23 \end{vmatrix}$$

$$\begin{vmatrix} 3 & 14 \\ 9 & 5 \end{vmatrix} \begin{vmatrix} 3 \\ 23 \end{vmatrix} = \begin{vmatrix} (3*3)+(14*23) \\ (9*3)+(5*23) \end{vmatrix} = \begin{vmatrix} 331 \\ 142 \end{vmatrix} \bmod 26 = \begin{vmatrix} 19 \\ 12 \end{vmatrix} = \begin{vmatrix} T \\ M \end{vmatrix}$$

HLDTQIHJDXWQCMAG

$$P = (k^{-1} * C) \bmod 26$$

$$\begin{vmatrix} W \\ Q \end{vmatrix} = \begin{vmatrix} 22 \\ 16 \end{vmatrix}$$

$$\begin{vmatrix} 3 & 14 \\ 9 & 5 \end{vmatrix} \begin{vmatrix} 22 \\ 16 \end{vmatrix} = \begin{vmatrix} (3 * 22) + (14 * 16) \\ (9 * 22) + (5 * 16) \end{vmatrix} = \begin{vmatrix} 290 \\ 278 \end{vmatrix} \bmod 26 = \begin{vmatrix} 4 \\ 18 \end{vmatrix} = \begin{vmatrix} E \\ S \end{vmatrix}$$

HLDTQIHJDXWQCMAG

$$P = (k^{-1} * C) \bmod 26$$

$$\begin{vmatrix} C \\ M \end{vmatrix} = \begin{vmatrix} 2 \\ 12 \end{vmatrix}$$

$$\begin{vmatrix} 3 & 14 \\ 9 & 5 \end{vmatrix} \begin{vmatrix} 2 \\ 12 \end{vmatrix} = \begin{vmatrix} (3*2)+(14*12) \\ (9*2)+(5*12) \end{vmatrix} = \begin{vmatrix} 174 \\ 78 \end{vmatrix} \bmod 26 = \begin{vmatrix} 18 \\ 0 \end{vmatrix} = \begin{vmatrix} S \\ A \end{vmatrix}$$

HLDTQIHJDXWQCMAG

$$P = (k^{-1} * C) \bmod 26$$

$$\begin{vmatrix} A \\ G \end{vmatrix} = \begin{vmatrix} 0 \\ 6 \end{vmatrix}$$

$$\begin{vmatrix} 3 & 14 \\ 9 & 5 \end{vmatrix} \begin{vmatrix} 0 \\ 6 \end{vmatrix} = \begin{vmatrix} (3*0)+(14*6) \\ (9*0)+(5*6) \end{vmatrix} = \begin{vmatrix} 84 \\ 30 \end{vmatrix} \bmod 26 = \begin{vmatrix} 6 \\ 4 \end{vmatrix} = \begin{vmatrix} G \\ E \end{vmatrix}$$

Decryption process

We are take the character above we get the Original plaintext:

“TOP SECRET MESSAGE”

Example 3 / In a Hill cipher decrypt the ciphertext

"VOHY" with key $\begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}$

Answer

Step1 Find the key inverse

Determinant : $\begin{bmatrix} d & b \\ c & a \end{bmatrix}$ deterimnant is calucuted by ad – bc

$$\begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix} = (3*5) - (3*2) = 9 \Longrightarrow \text{invers equal } 3$$

$$3 * \begin{bmatrix} 5 & -3 \\ -2 & 3 \end{bmatrix} = \begin{bmatrix} 15 & -9 \\ -6 & 9 \end{bmatrix} \bmod 26 = \begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix}$$

Example 3 / In a Hill cipher decrypt the ciphertext "VOHY" with key $\begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}$

Answer

Step2 The encryption process

$$\begin{bmatrix} V \\ O \end{bmatrix} = \begin{bmatrix} 21 \\ 14 \end{bmatrix}$$

$$\begin{bmatrix} H \\ Y \end{bmatrix} = \begin{bmatrix} 7 \\ 24 \end{bmatrix}$$

$$P = (k^{-1} * C) \bmod 26$$

$$\begin{bmatrix} V \\ O \end{bmatrix} \Longrightarrow \begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix} \begin{matrix} 21 \\ 14 \end{matrix} = \begin{bmatrix} 15*21+ & 17*14 \\ 20*21+ & 9*14 \end{bmatrix} = \begin{matrix} 553 \\ 546 \end{matrix} \bmod 26 = \begin{matrix} 7 \\ 0 \end{matrix} = HA$$

$$\begin{bmatrix} H \\ Y \end{bmatrix} \Longrightarrow \begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix} \begin{matrix} 7 \\ 24 \end{matrix} = \begin{bmatrix} 15*7+ & 17*24 \\ 20*7+ & 9*24 \end{bmatrix} = \begin{matrix} 513 \\ 356 \end{matrix} \bmod 26 = \begin{matrix} 19 \\ 18 \end{matrix} = TS$$

Plaintext = HATS

Example 4 / **If the key is** $\begin{bmatrix} 24 & 19 \\ 5 & 14 \end{bmatrix}$ **and the ciphertext is "RXAODY" find the plaintext using Hill cipher method.**

Answer

Step1 **Find the key inverse**

find the determent d =(24*14)- (5*19) = 241

d = 241 mod26 = 7

d^{-1}= 15

$k^{-1} = d^{-1}(k) * = 15 * \begin{pmatrix} 14 & -19 \\ -5 & 24 \end{pmatrix} = \begin{pmatrix} 210 & -285 \\ -75 & 360 \end{pmatrix} \bmod 26$

$k^{-1} = \begin{pmatrix} 2 & 1 \\ 3 & 22 \end{pmatrix}$

Example 4 / If the key is $\begin{bmatrix} 24 & 19 \\ 5 & 14 \end{bmatrix}$ and the ciphertext is "RXAODY" find the plaintext using Hill cipher method.

Answer

Step2 The encryption process

$$P = (k^{-1} * C) \bmod 26$$

- RX=$\binom{17}{23}$

$$\begin{pmatrix} 2 & 1 \\ 3 & 22 \end{pmatrix} \binom{17}{23} = \binom{57}{557} mod\ 26 = \binom{5}{11}$$ ➔ FL

Example 4 / If the key is $\begin{bmatrix} 24 & 19 \\ 5 & 14 \end{bmatrix}$ and the ciphertext is "RXAODY" find the plaintext using Hill cipher method.

Answer

Step2 The encryption process

- AO=$\begin{pmatrix} 0 \\ 14 \end{pmatrix}$

$$\begin{pmatrix} 2 & 1 \\ 3 & 22 \end{pmatrix}\begin{pmatrix} 0 \\ 14 \end{pmatrix} = \begin{pmatrix} 14 \\ 308 \end{pmatrix} mod\ 26 = \begin{pmatrix} 14 \\ 22 \end{pmatrix}$$ ➔ OW

Example 4 / If the key is $\begin{bmatrix} 24 & 19 \\ 5 & 14 \end{bmatrix}$ and the ciphertext is "RXAODY" find the plaintext using Hill cipher method.

Answer

Step2 The encryption process

- DY=$\begin{pmatrix} 3 \\ 24 \end{pmatrix}$

$$\begin{pmatrix} 2 & 1 \\ 3 & 22 \end{pmatrix}\begin{pmatrix} 3 \\ 24 \end{pmatrix} = \begin{pmatrix} 30 \\ 537 \end{pmatrix} mod\ 26 = \begin{pmatrix} 4 \\ 17 \end{pmatrix}$$ ➔ ER

plaintext : **flower**.