CS 413 Information Security

Course Instructor

Naushad Siddiqui

Head of IT Audit, Sui Southern Gas Company

Visiting Faculty, NED University

Director & Faculty Member, ISACA Karachi

CS413 Information Security

Fall 2020

Week 06

Agenda

- Hill Cipher

Hill Cipher

Hill Cipher

- Hill cipher is a polygraphic substitution cipher based on linear algebra.
- Invented by L. S. Hill in 1929.
- Each letter is represented by a number modulo 26.
- Often the simple scheme A = 0, B = 1, …, Z = 25 is used, but this is not an essential feature of the cipher.
- Inputs:
  - String of English letters, A,B,…,Z.
  - An **n x n** matrix K, with entries drawn from 0,1,…,25. (The matrix K serves as the secret key.)

Hill Cipher Encryption

- The matrix used for encryption is the cipher key, and it should be chosen randomly from the set of invertible $n \times n$ matrices (modulo 26).
- Divide the input string into blocks of size ‘n’, considered as an n-component vector
- To encrypt a message, each block of ‘n’ letters is multiplied by the matrix ‘K’

Hill Cipher

Complications exist in picking the encrypting matrix (or cipher key):

- Not all matrices have an inverse (i.e. invertible matrix). The matrix will have an inverse <u>if and only if its determinant is not zero</u>.
- The **determinant** of the encrypting matrix <u>must not have any common factors with the modular base</u>.
- Thus, if we work modulo 26 as above, the determinant must be nonzero, and must not be divisible by 2 or 13.
- If the determinant is 0, or has common factors with the modular base, then the matrix cannot be used in the Hill cipher, and another matrix must be chosen (otherwise it will not be possible to decrypt).
- Fortunately, matrices which satisfy the conditions to be used in the Hill cipher are fairly common.

Hill Cipher – Encryption Example

- We have to encrypt the message ‘ACT’ (n=3).
- The key is ‘GYBNQKURP’ which can be written as the n x n matrix:

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}$$

- The message ‘ACT’ is written as vector:

$$\begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix}$$

Hill Cipher – Encryption Example

- The enciphered vector is given as:

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix} \begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix} = \begin{bmatrix} 67 \\ 222 \\ 319 \end{bmatrix} \equiv \begin{bmatrix} 15 \\ 14 \\ 7 \end{bmatrix} \pmod{26}$$

which corresponds to ciphertext of 'POH'

Hill Cipher Decryption

- The decryption must be the inverse function of the encryption function.
- To decrypt the message, each block is multiplied by the **inverse of the matrix** used for encryption.
  - It is required that $\mathbf{K}^{-1}\,\mathbf{K} = \mathbf{I}_n$ mod 26.
- Provided that det(**K**) has a multiplicative inverse mod 26, i.e., if det(**K**) and n has no common factor, the inverse of **K** can be computed by the adjoint formula for matrix inverse.

Hill Cipher – Decryption Example

- To decrypt the message, we turn the ciphertext back into a vector, then simply multiply by the inverse matrix of the key matrix (IFKVIVVMI in letters).
- The inverse of the matrix used in the previous example is:

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}^{-1} \equiv \begin{bmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{bmatrix} \pmod{26}$$

Hill Cipher – Decryption Example

- For the previous Ciphertext ‘POH’:

$$\begin{bmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{bmatrix} \begin{bmatrix} 15 \\ 14 \\ 7 \end{bmatrix} \equiv \begin{bmatrix} 260 \\ 574 \\ 539 \end{bmatrix} \equiv \begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix} \pmod{26}$$

which gives us back ‘ACT’

Hill Cipher – Encryption Example

$$K = \begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix}$$

be the key and suppose the plaintext message is HELP. Then this plaintext is represented by two pairs

$$HELP \to \begin{pmatrix} H \\ E \end{pmatrix}, \begin{pmatrix} L \\ P \end{pmatrix} \to \begin{pmatrix} 7 \\ 4 \end{pmatrix}, \begin{pmatrix} 11 \\ 15 \end{pmatrix}$$

Then we compute

$$\begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix} \begin{pmatrix} 7 \\ 4 \end{pmatrix} \equiv \begin{pmatrix} 7 \\ 8 \end{pmatrix} \pmod{26}, \text{ and}$$

$$\begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix} \begin{pmatrix} 11 \\ 15 \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 19 \end{pmatrix} \pmod{26}$$

and continue encryption as follows:

$$\begin{pmatrix} 7 \\ 8 \end{pmatrix}, \begin{pmatrix} 0 \\ 19 \end{pmatrix} \to \begin{pmatrix} H \\ I \end{pmatrix}, \begin{pmatrix} A \\ T \end{pmatrix}$$

Hill Cipher – Decryption Example

The matrix K is invertible, hence K^{-1} exists such that $KK^{-1} = K^{-1}K = I_2$. The inverse of K can be computed by using the formula $\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = (ad - bc)^{-1} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$

This formula still holds after a modular reduction if a modular multiplicative inverse is used to compute $(ad - bc)^{-1}$. Hence in this case, we compute

$$K^{-1} \equiv 9^{-1} \begin{pmatrix} 5 & 23 \\ 24 & 3 \end{pmatrix} \equiv 3 \begin{pmatrix} 5 & 23 \\ 24 & 3 \end{pmatrix} \equiv \begin{pmatrix} 15 & 17 \\ 20 & 9 \end{pmatrix} \pmod{26}$$

$$HIAT \to \begin{pmatrix} H \\ I \end{pmatrix}, \begin{pmatrix} A \\ T \end{pmatrix} \to \begin{pmatrix} 7 \\ 8 \end{pmatrix}, \begin{pmatrix} 0 \\ 19 \end{pmatrix}$$

Hill Cipher – Decryption Example

Then we compute

$$\begin{pmatrix} 15 & 17 \\ 20 & 9 \end{pmatrix} \begin{pmatrix} 7 \\ 8 \end{pmatrix} \equiv \begin{pmatrix} 7 \\ 4 \end{pmatrix} \pmod{26}, \text{ and}$$

$$\begin{pmatrix} 15 & 17 \\ 20 & 9 \end{pmatrix} \begin{pmatrix} 0 \\ 19 \end{pmatrix} \equiv \begin{pmatrix} 11 \\ 15 \end{pmatrix} \pmod{26}$$

Therefore,

$$\begin{pmatrix} 7 \\ 4 \end{pmatrix}, \begin{pmatrix} 11 \\ 15 \end{pmatrix} \to \begin{pmatrix} H \\ E \end{pmatrix}, \begin{pmatrix} L \\ P \end{pmatrix} \to HELP.$$

Hill Cipher – Encryption Example

Finding the Modular Inverse

Let $A = \begin{bmatrix} 2 & 1 \\ 3 & 4 \end{bmatrix}$

det $A = (2 \text{ x } 4) - (1 \text{ x } 3) = 8 - 3 = 5$

modular inverse of 5 for Mod 26 = 21

$$B = 21\begin{bmatrix} 4 & -1 \\ -3 & 2 \end{bmatrix} = \begin{bmatrix} 84 & -21 \\ -63 & 42 \end{bmatrix}$$

$$B = \begin{bmatrix} 84 & -21 \\ -63 & 42 \end{bmatrix} \text{Mod } 26 = \begin{bmatrix} 6 & 5 \\ 15 & 16 \end{bmatrix}$$

Therefore $\begin{bmatrix} 6 & 5 \\ 15 & 16 \end{bmatrix}$ is the modular inverse of $\begin{bmatrix} 2 & 1 \\ 3 & 4 \end{bmatrix}$ for Mod 26.

Hill Cipher – Encryption Example

Message to encrypt = HELLO WORLD

$$\begin{bmatrix} H \\ E \end{bmatrix} = \begin{bmatrix} 7 \\ 4 \end{bmatrix}$$

$$\begin{bmatrix} L \\ L \end{bmatrix} = \begin{bmatrix} 11 \\ 11 \end{bmatrix}$$

$$\begin{bmatrix} O \\ W \end{bmatrix} = \begin{bmatrix} 14 \\ 22 \end{bmatrix}$$

$$\begin{bmatrix} O \\ R \end{bmatrix} = \begin{bmatrix} 14 \\ 17 \end{bmatrix}$$

$$\begin{bmatrix} L \\ D \end{bmatrix} = \begin{bmatrix} 11 \\ 3 \end{bmatrix}$$

Hill Cipher – Encryption Example

Multiply Matrix by Vectors

$$\begin{bmatrix} 2 & 1 \\ 3 & 4 \end{bmatrix} \times \begin{bmatrix} 7 \\ 4 \end{bmatrix} = \begin{bmatrix} 14+4 \\ 21+16 \end{bmatrix} = \begin{bmatrix} 18 \\ 37 \end{bmatrix}$$

$$\begin{bmatrix} 2 & 1 \\ 3 & 4 \end{bmatrix} \times \begin{bmatrix} 11 \\ 11 \end{bmatrix} = \begin{bmatrix} 22+11 \\ 33+44 \end{bmatrix} = \begin{bmatrix} 33 \\ 77 \end{bmatrix}$$

$$\begin{bmatrix} 2 & 1 \\ 3 & 4 \end{bmatrix} \times \begin{bmatrix} 14 \\ 22 \end{bmatrix} = \begin{bmatrix} 28+22 \\ 42+88 \end{bmatrix} = \begin{bmatrix} 50 \\ 130 \end{bmatrix}$$

$$\begin{bmatrix} 2 & 1 \\ 3 & 4 \end{bmatrix} \times \begin{bmatrix} 14 \\ 17 \end{bmatrix} = \begin{bmatrix} 28+17 \\ 42+68 \end{bmatrix} = \begin{bmatrix} 45 \\ 110 \end{bmatrix}$$

$$\begin{bmatrix} 2 & 1 \\ 3 & 4 \end{bmatrix} \times \begin{bmatrix} 11 \\ 3 \end{bmatrix} = \begin{bmatrix} 22+3 \\ 33+12 \end{bmatrix} = \begin{bmatrix} 25 \\ 45 \end{bmatrix}$$

Hill Cipher – Encryption Example

Convert to Mod 26

$$\begin{bmatrix} 18 \\ 37 \end{bmatrix} \text{Mod } 26 = \begin{bmatrix} 18 \\ 11 \end{bmatrix} \qquad \begin{bmatrix} 18 \\ 11 \end{bmatrix} = \begin{bmatrix} S \\ L \end{bmatrix}$$

$$\begin{bmatrix} 33 \\ 77 \end{bmatrix} \text{Mod } 26 = \begin{bmatrix} 7 \\ 25 \end{bmatrix} \qquad \begin{bmatrix} 7 \\ 25 \end{bmatrix} = \begin{bmatrix} H \\ Z \end{bmatrix}$$

$$\begin{bmatrix} 50 \\ 130 \end{bmatrix} \text{Mod } 26 = \begin{bmatrix} 24 \\ 0 \end{bmatrix} \rightarrow \begin{bmatrix} 24 \\ 0 \end{bmatrix} = \begin{bmatrix} Y \\ A \end{bmatrix}$$

$$\begin{bmatrix} 45 \\ 110 \end{bmatrix} \text{Mod } 26 = \begin{bmatrix} 19 \\ 6 \end{bmatrix} \qquad \begin{bmatrix} 19 \\ 6 \end{bmatrix} = \begin{bmatrix} T \\ G \end{bmatrix}$$

$$\begin{bmatrix} 25 \\ 45 \end{bmatrix} \text{Mod } 26 = \begin{bmatrix} 25 \\ 19 \end{bmatrix} \qquad \begin{bmatrix} 25 \\ 19 \end{bmatrix} = \begin{bmatrix} Z \\ T \end{bmatrix}$$

Hill Cipher – Encryption Example

Convert Numbers to Letters

$$\begin{bmatrix} 18 \\ 11 \end{bmatrix} = \begin{bmatrix} S \\ L \end{bmatrix}$$

$$\begin{bmatrix} 7 \\ 25 \end{bmatrix} = \begin{bmatrix} H \\ Z \end{bmatrix}$$

$$\begin{bmatrix} 24 \\ 0 \end{bmatrix} = \begin{bmatrix} Y \\ A \end{bmatrix}$$

$$\begin{bmatrix} 19 \\ 6 \end{bmatrix} = \begin{bmatrix} T \\ G \end{bmatrix}$$

$$\begin{bmatrix} 25 \\ 19 \end{bmatrix} = \begin{bmatrix} Z \\ T \end{bmatrix}$$

HELLO WORLD has been encrypted to

SLHZY ATGZT

Hill Cipher – Decryption Example

Convert Ciphertext

SLHZY ATGZT

To Plaintext

HELLO WORLD

End of Week 06