Practical Session 1

Cryptography 2024-2

February 23, 2024

1 Hill cipher

The Hill cipher [1] is a polygraphic substitution cipher built on concepts from Linear Algebra. This cipher makes use of modulo arithmetic, matrix multiplication, and matrix inverses. It is also a block cipher so it can work on arbitrary sized blocks. Like in other classical ciphers, each letter is represented by a number modulo 26. This means $A = 0, B = 1, ..., Z = 25$ is used. To encrypt a message, each block of n letters (considered as an n-component vector) is multiplied by an invertible $n \times n$ matrix, against modulus 26. To decrypt the message, each block is multiplied by the inverse of the matrix used for 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).

2 Encryption

The following function is used to encrypt with the Hill cipher.

$$E(K, P) = (K * P) \mod 26$$

Where K is our key matrix and P is the plain text in vector form. Matrix multiplying these two terms produces the encrypted cipher text.

The process is the following:

1. Pick a keyword to encrypt your plain text message and transform it into a $n \times n$ matrix. This will be the key K.
2. Next, convert the plain text to a n vector form.
3. Finally, to obtain the cipher text the key is multiplied by the plain text.

2.1 Example

We want to encrypt the plain text $P =$ MORNING using the key $K =$ DCDF.

1. Convert the key to matrix form using the substitution scheme to convert it to a numerical 2×2 key matrix.

$$\text{DCDF} = \begin{bmatrix} D & D \\ C & F \end{bmatrix} = \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}$$

2. Since our key matrix is 2×2, plain text vector needs to be 2×1 for matrix multiplication to be possible. In our case, our message is seven letters long so we can split it into blocks of two and then substitute to get our plain text vectors. We need a padding to complete the vectors when necessary. In our case, padding will be X.

$$\text{MORNING} = \begin{bmatrix} M \\ O \end{bmatrix} \begin{bmatrix} R \\ N \end{bmatrix} \begin{bmatrix} I \\ N \end{bmatrix} \begin{bmatrix} G \\ X \end{bmatrix} = \begin{bmatrix} 12 \\ 14 \end{bmatrix} \begin{bmatrix} 17 \\ 13 \end{bmatrix} \begin{bmatrix} 8 \\ 13 \end{bmatrix} \begin{bmatrix} 6 \\ 23 \end{bmatrix}$$

3. Now, we can multiply the key matrix with each plain text vector. Remember to calculate the module 26 of the resulting vectors and concatenate the results to get the final cipher text.

$$\begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix} \times \begin{bmatrix} 12 \\ 14 \end{bmatrix} = \begin{bmatrix} 0 \\ 16 \end{bmatrix} \quad \text{mod } 26 = \begin{bmatrix} A \\ Q \end{bmatrix}$$

$$\begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix} \times \begin{bmatrix} 17 \\ 13 \end{bmatrix} = \begin{bmatrix} 12 \\ 21 \end{bmatrix} \quad \text{mod } 26 = \begin{bmatrix} M \\ V \end{bmatrix}$$

$$\begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix} \times \begin{bmatrix} 8 \\ 13 \end{bmatrix} = \begin{bmatrix} 11 \\ 3 \end{bmatrix} \quad \text{mod } 26 = \begin{bmatrix} L \\ D \end{bmatrix}$$

$$\begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix} \times \begin{bmatrix} 6 \\ 23 \end{bmatrix} = \begin{bmatrix} 9 \\ 23 \end{bmatrix} \quad \text{mod } 26 = \begin{bmatrix} J \\ X \end{bmatrix}$$

Then, the cipher text resulting is $C =$ AQMVLDJX.

3 Decryption

The following function is used to decrypt with the Hill cipher.

$$D(K, C) = (K^{-1} * C) \mod 26$$

Where K is the key and C is the cipher text in vector form. This means the plain text is produced by multiplying the inverse of the key by the cipher text.

First, the inverse of the key matrix is calculated over modulo 26. Then, the rest of the process is the same as explained before.

3.1 Example

We want to decrypt the cipher text $P =$ AQMVLDJX using the inverse of key $K =$.

1. Find the inverse of the key in matrix form in modulo 26. Remember that not all matrices are invertible and not all numbers in modulo 26 have an inverse.

$$K^{-1} = \text{Det } K * K^{*} \mod 26$$

$$9^{-1} \mod 26 \begin{bmatrix} 5 & 23 \\ 24 & 3 \end{bmatrix} = 3 \begin{bmatrix} 5 & 23 \\ 24 & 3 \end{bmatrix} = \begin{bmatrix} 15 & 69 \\ 72 & 9 \end{bmatrix} = \begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix}$$

2. Now, we can multiply the inverse key matrix with each cipher text vector. Remember to calculate the module 26 of the resulting vectors and concatenate the results to get the final plain text.

$$\begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix} \times \begin{bmatrix} 0 \\ 16 \end{bmatrix} = \begin{bmatrix} 12 \\ 14 \end{bmatrix} \mod 26 = \begin{bmatrix} M \\ O \end{bmatrix}$$

$$\begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix} \times \begin{bmatrix} 12 \\ 21 \end{bmatrix} = \begin{bmatrix} 17 \\ 13 \end{bmatrix} \mod 26 = \begin{bmatrix} R \\ N \end{bmatrix}$$

$$\begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix} \times \begin{bmatrix} 11 \\ 3 \end{bmatrix} = \begin{bmatrix} 8 \\ 13 \end{bmatrix} \mod 26 = \begin{bmatrix} I \\ N \end{bmatrix}$$

$$\begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix} \times \begin{bmatrix} 9 \\ 23 \end{bmatrix} = \begin{bmatrix} 6 \\ 23 \end{bmatrix} \mod 26 = \begin{bmatrix} G \\ X \end{bmatrix}$$

Then, the plain text resulting is $P =$ MORNINGX, where we can remove the padding X to obtain the original message.

4 Deliverables

For this practical session you will implement the Hill cipher in one of the programming languages supported by Alphagrader [1].

- This practical session is individual and it has to be submitted on Alphagrader.
- Both, encryption and decryption processes should be implemented and submitted.
- All test should be successfully passed to get a grade.
- The solution has to be submitted on the date and time previously agreed on.

References

[1] Lester S. Hill. Cryptography in an algebraic alphabet, 1929.

[1] https://www.alphagrader.com/