MATH 314 Spring 2024 - Class Notes

2/7/2024

Scribe: Saintgermain Lopez

Summary: A Brief Introduction to stream cipher and block cipher. Also, An explanation of how to encrypt and decrypt using Hill cipher and how to check encryption and decryption using SageMath.

Notes

Stream Cipher

- encrypts individual letters or bits one at a time (changing one letter/bit of plaintext only changes one letter of ciphertext

Block Cipher

- multiple letters/bits are joined into a block and entire blocks are encrypted at once changing one letter of a block can change the entire block of ciphertext

Hill Cipher

1. pick a block size b
2. break plaintext into block of size b

- Key is a b × b matrix k of numbers (mod 26)
- To encrypt a block we convert it to a vector (vertical vectors)

$$E(\overrightarrow{v}) = k \times \overrightarrow{v} \pmod{26}$$

Example:

b=2

$$k = \begin{bmatrix} 3 & 4 \\ 14 & 17 \end{bmatrix}$$

Encrypt: "Math"

$$E(\begin{bmatrix}12\\0\end{bmatrix}) \equiv \begin{bmatrix}3 & 4\\14 & 17\end{bmatrix}\begin{bmatrix}12\\0\end{bmatrix} \equiv \begin{bmatrix}3\times 12 & 4\times 0\\14\times 12 & 7\times 0\end{bmatrix} \equiv \begin{bmatrix}36 & 0\\168 & 0\end{bmatrix} \equiv \begin{bmatrix}10\\12\end{bmatrix}$$

10 and 12 corresponds to letters K and M.

Now, we encrypt the second block of letters:

$$E(\begin{bmatrix}19\\7\end{bmatrix}) \equiv \begin{bmatrix}3 & 4\\14 & 17\end{bmatrix}\begin{bmatrix}19\\7\end{bmatrix} \equiv \begin{bmatrix}3\times 19 & 4\times 7\\14\times 19 & 7\times 7\end{bmatrix} \equiv \begin{bmatrix}57 & 28\\6 & 23\end{bmatrix} \equiv \begin{bmatrix}7\\3\end{bmatrix}$$

7 and 3 corresponds to letters H and D.

As result, KMHD is the ciphertext for Math

If we change one letter, then the entire block changes.

Ex: Change math to bath.

$$E(\begin{bmatrix}1\\0\end{bmatrix}) \equiv \begin{bmatrix}3 & 4\\14 & 17\end{bmatrix}\begin{bmatrix}1\\0\end{bmatrix} \equiv \begin{bmatrix}3\times 1 & 4\times 0\\14\times 1 & 7\times 0\end{bmatrix} \equiv \begin{bmatrix}3\\14\end{bmatrix}$$

3 and 14 corresponds to letters D and O.

Now, we encrypt the second block of letters:

$$E(\begin{bmatrix}19\\7\end{bmatrix}) \equiv \begin{bmatrix}3 & 4\\14 & 17\end{bmatrix}\begin{bmatrix}19\\7\end{bmatrix} \equiv \begin{bmatrix}3\times 19 & 4\times 7\\14\times 19 & 7\times 7\end{bmatrix} \equiv \begin{bmatrix}57 & 28\\6 & 23\end{bmatrix} \equiv \begin{bmatrix}7\\3\end{bmatrix}$$

7 and 3 corresponds to letters H and D.

As result, DOHD is the ciphertext for bath/

<u>How to decrypt a Hill Cipher?</u>

- reverse it, solve for $\overrightarrow{v}$
- Since we can't divide, matrix k needs an inverse
- to decrypt, k needs to have an inverse k^{-1}

$$\overrightarrow{w} \equiv k\overrightarrow{v}$$

$$k^{-1}\overrightarrow{w} \equiv k^{-1}k\overrightarrow{v}$$

$$\overrightarrow{v} \equiv D(\overrightarrow{w}) \equiv k^{-1}\overrightarrow{w}$$

$k = \begin{bmatrix} c & d \\ e & f \end{bmatrix}$

$k^{-1} \equiv (c \times f - e \times d)^{-1} \begin{bmatrix} f & -d \\ -e & c \end{bmatrix} \pmod{26}$

If b=2 and,

$k = \begin{bmatrix} 3 & 4 \\ 14 & 7 \end{bmatrix}$

$k^{-1} \equiv (3 \times 7 - 4 \times 14)^{-1} \begin{bmatrix} 7 & -4 \\ -14 & 3 \end{bmatrix} \pmod{26}$

$k^{-1} \equiv (21 - 4)^{-1} \begin{bmatrix} 7 & 22 \\ 12 & 3 \end{bmatrix}$

$k^{-1} \equiv (17)^{-1} \begin{bmatrix} 7 & 22 \\ 12 & 3 \end{bmatrix}$

$k^{-1} \equiv 23 \begin{bmatrix} 7 & 22 \\ 12 & 3 \end{bmatrix} \equiv \begin{bmatrix} 23 \times 7 & 23 \times 22 \\ 23 \times 12 & 23 \times 3 \end{bmatrix} \pmod{26} \equiv \begin{bmatrix} 5 & 12 \\ 16 & 17 \end{bmatrix}$

This is the Final Decryption Matrix X

<u>How to attack the Hill Cipher?</u>

- The easiest way to attack the Hill Cipher is by **<u>choosen plaintext attack</u>**

Ex: ab

$E(\begin{bmatrix} 0 \\ 1 \end{bmatrix}) \equiv k \begin{bmatrix} 0 \\ 1 \end{bmatrix} \equiv \begin{bmatrix} c & d \\ e & f \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} \equiv \begin{bmatrix} c \times 0 & d \times 1 \\ e \times 0 & f \times 1 \end{bmatrix} \equiv \begin{bmatrix} d \\ f \end{bmatrix}$

Ex: ba

$E(\begin{bmatrix} 1 \\ 0 \end{bmatrix}) \equiv k \begin{bmatrix} 1 \\ 0 \end{bmatrix} \equiv \begin{bmatrix} c & d \\ e & f \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} \equiv \begin{bmatrix} c \times 1 & d \times 0 \\ e \times 1 & f \times 0 \end{bmatrix} \equiv \begin{bmatrix} c \\ e \end{bmatrix}$

<u>Known Plaintext Attack</u>

- Another method to attack Hill Cipher

- Solve for entries in the matrix
- Use matrix algebra to perform the attack

Ex: suppose linear encrypts to LTPVPI. Using a hill cipher with block size 2:

1. Combine blocks to make plaintext matrix and Cipher matrix:

$$k\begin{bmatrix}11\\8\end{bmatrix} \equiv \begin{bmatrix}11\\19\end{bmatrix}$$

$$k\begin{bmatrix}13\\4\end{bmatrix} \equiv \begin{bmatrix}15\\21\end{bmatrix}$$

$$k\begin{bmatrix}0\\17\end{bmatrix} \equiv \begin{bmatrix}15\\8\end{bmatrix}$$

$$k\begin{bmatrix}11 & 13\\8 & 4\end{bmatrix} \equiv \begin{bmatrix}11 & 15\\19 & 21\end{bmatrix}$$

If p= $\begin{bmatrix}11 & 13\\8 & 4\end{bmatrix}$, then

$$p^{-1} \equiv (44-104)^{-1}\begin{bmatrix}4 & -13\\-8 & 11\end{bmatrix} \pmod{26}$$

$$p^{-1} \equiv -60^{-1} \equiv -8^{-1} \equiv 18^{-1}$$

Even Numbers does not have an inverse.
In This case, p^{-1} does not exist.

so, we have to pick other combination of matrix

Let's Try first and third blocks:

$$k\begin{bmatrix}11 & 0\\8 & 17\end{bmatrix} \equiv \begin{bmatrix}11 & 15\\19 & 8\end{bmatrix}$$

$$p^{-1} \equiv (11\times 17-0)^{-1}\begin{bmatrix}17 & 0\\-8 & 11\end{bmatrix} \pmod{26}$$

$$187^{-1} \equiv 5^{-1}$$

$$21\begin{bmatrix}17 & 0\\18 & 11\end{bmatrix}$$

$$p^{-1} \equiv \begin{bmatrix} 21 \times 17 & 21 \times 0 \\ 21 \times 18 & 21 \times 11 \end{bmatrix}$$

$$p^{-1} \equiv \begin{bmatrix} 19 & 0 \\ 14 & 23 \end{bmatrix}$$

Now, $k \equiv c \times p^{-1} \equiv \begin{bmatrix} 19 & 0 \\ 14 & 23 \end{bmatrix} \begin{bmatrix} 19 & 0 \\ 14 & 23 \end{bmatrix} \equiv \begin{bmatrix} 11 \times 19 + 15 \times 14 & 11 \times 0 + 15 \times 23 \\ 19 \times 19 + 8 \times 14 & 19 \times 0 + 18 \times 23 \end{bmatrix}$

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

SageMath to Encrypt and Decrypt Hill Cipher

- Open SageMath: `https://sagecell.sagemath.org/`
- Copy the following code To Encrypt and decrypt MATH :

```
R=IntegerModRing(26)
K=matrix(R,[[3,4],[14,7]])
print("Encrypt MATH:")
print("Matrix K:")
print(K)
print("Encryption of the first block, M A: ")
print(K*vector([12,0]))
print("Encryption of the second block T H: ")
print(K*vector([19,7]))
print("Now, Decrypt: KMHD")
print("Inverse of Matrix K:")
print(K^-1)
print("Decryption of the first block : K M")
print(K^-1*vector([10,12]))
print("Decryption of the second block : H D")
print(K^-1*vector([7,3]))
```

output:

Encrypt MATH:
Matrix K:
[3 4]
[14 7]
Encryption of the first block, M A:
(10, 12)
Encryption of the second block T H:
(7, 3)

Now, Decrypt: KMHD
Inverse of Matrix K:
[5 12]
[16 17]
Decryption of the first block : K M
(12, 0)
Decryption of the second block : H D
(19, 7)