Cryptography-Hill Cipher MTH 261

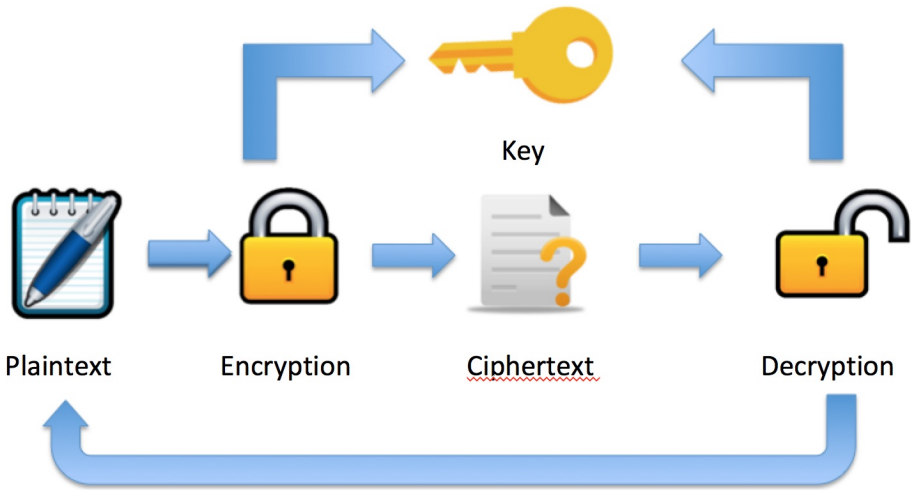
Kendra Young

May 16, 2024

Table of Contents

Cryptography

- Cryptography-the study and practice of using secret writing techniques such as code and cipher systems
- Cipher-algorithm or operation for encryption or decryption



History

- Egypt 1900 BCE

History

- Egypt 1900 BCE
- Classical cryptography

History

- Egypt 1900 BCE
- Classical cryptography
  - Substitution Cipher

History

- Egypt 1900 BCE
- Classical cryptography
  - Substitution Cipher
  - Transpose Cipher

History

- Egypt 1900 BCE
- Classical cryptography
  - Substitution Cipher
  - Transpose Cipher
- WWI and WWII

The Hill Cipher

- Lester S. Hill 1929

The Hill Cipher

- Lester S. Hill 1929
- Polygraphic Substitution Cipher
  - Monoalphabetic substitution vs.polyalphabetic substitution transformed.

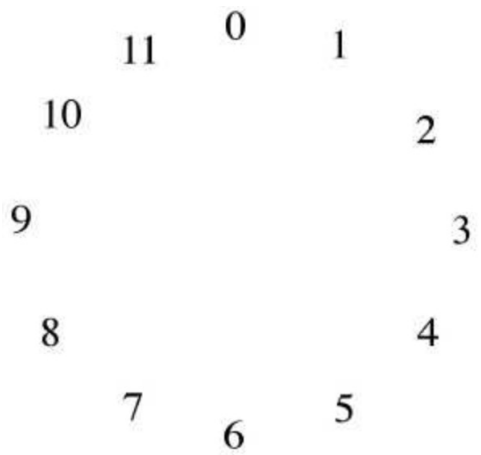
The Hill Cipher

- Lester S. Hill 1929
- Polygraphic Substitution Cipher
  - Monoalphabetic substitution vs.polyalphabetic substitution transformed.
- Utilizes linear algebra

Modular Arithmetic

$$a \equiv b \mod m$$

$$35 \equiv 6(mod 29) \quad \text{and} \quad 64 \equiv 6(mod 29)$$



Encryption

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	.	?	␣
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28

Table: Numerical coding of alphabet and punctuation marks.

Encryption

Next, an $n \times n$ encryption matrix A is chosen to encrypt the message.

$$A = \begin{bmatrix} 2 & 4 \\ -6 & 8 \end{bmatrix}$$

Encryption

Choose message to encrypt.

Encryption

Choose message to encrypt. **YIPPEE KI YAY MF**

Encryption

Choose message to encrypt. **YIPPEE KI YAY MF**

$$\begin{bmatrix} Y & P & E & \sqcup & I & Y & Y & M \\ I & P & E & K & \sqcup & A & \sqcup & F \end{bmatrix}$$

Encryption

Choose message to encrypt. **YIPPEE KI YAY MF**

$$\begin{bmatrix} Y & P & E & \sqcup & I & Y & Y & M \\ I & P & E & K & \sqcup & A & \sqcup & F \end{bmatrix}$$

From table 1, each letter is converted into its unique number, creating matrix B.

Encryption

Choose message to encrypt. **YIPPEE KI YAY MF**

$$\begin{bmatrix} Y & P & E & \sqcup & I & Y & Y & M \\ I & P & E & K & \sqcup & A & \sqcup & F \end{bmatrix}$$

From table 1, each letter is converted into its unique number, creating matrix B.

$$B = \begin{bmatrix} 24 & 15 & 4 & 28 & 8 & 24 & 24 & 12 \\ 8 & 15 & 4 & 10 & 28 & 0 & 28 & 5 \end{bmatrix}$$

Encryption

Now multiply the matrix B by the encryption matrix A to get the encrypted matrix C.

$$\begin{bmatrix} 2 & 4 \\ -6 & 8 \end{bmatrix} \begin{bmatrix} 24 & 15 & 4 & 28 & 8 & 24 & 24 & 12 \\ 8 & 15 & 4 & 10 & 28 & 0 & 28 & 5 \end{bmatrix}$$

$$\begin{bmatrix} 80 & 90 & 24 & 96 & 128 & 48 & 160 & 4 \\ -80 & 30 & 8 & -88 & 176 & -144 & 80 & -32 \end{bmatrix}$$

Encryption

Taking the modulus 29 of each encrypted vector

$$\begin{bmatrix} 80 & 90 & 24 & 96 & 128 & 48 & 160 & 4 \\ -80 & 30 & 8 & -88 & 176 & -144 & 80 & -32 \end{bmatrix} mod 29 =$$

$$\begin{bmatrix} 22 & 3 & 24 & 9 & 12 & 19 & 15 & 15 \\ 7 & 1 & 8 & 28 & 2 & 1 & 22 & 26 \end{bmatrix}$$

Encryption

Use Table 1 to convert the matrix C values back to letters:

$$C = \begin{bmatrix} W & D & Y & J & M & T & P & P \\ H & B & T & \_ & C & B & W & . \end{bmatrix}$$

"WHDBYIJ_MCTBPWP."

Decryption

- Similar to the encryption process
- Decryption key is matrix A^{-1}

$$A^{-1}AB = A^{-1}C$$

Decryption

mod29 determinant of A

$$A = \begin{bmatrix} 2 & 4 \\ -6 & 8 \end{bmatrix}, detA = (2 \cdot 8) - (-6 \cdot 4) = 40$$

$$40 \equiv 11 \mod 29$$

Decryption

Multiplicative Modular Inverse

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
1	15	10	22	6	5	25	11	13	3	8	17	9	27	2	20	12	21	26	16	18	4	24	23	7	19	14	28

Table: Multiplicative inverses modulo 29.

8 is the multiplicative modular inverse of 11

Decryption

Multiply the modular inverse value, 8, and the adjugate of A and find the mod29 value to get the decryption key matrix, A^{-1}.

$$A = \begin{bmatrix} 2 & 4 \\ -6 & 8 \end{bmatrix} \longrightarrow \text{adj}A = \begin{bmatrix} 8 & -4 \\ 6 & 2 \end{bmatrix}$$

$$\longrightarrow 8 \begin{bmatrix} 8 & -4 \\ 6 & 2 \end{bmatrix} = \begin{bmatrix} 64 & -32 \\ 48 & 16 \end{bmatrix}$$

$$\longrightarrow \begin{bmatrix} 64 & -32 \\ 48 & 16 \end{bmatrix} \mod 29 \equiv \begin{bmatrix} 6 & 26 \\ 19 & 16 \end{bmatrix}$$

Decryption

Return ciphertext back into numbered matrix

$$\begin{bmatrix} W & D & Y & J & M & T & P & P \\ H & B & T & \_ & C & B & W & . \end{bmatrix} =$$

$$\begin{bmatrix} 22 & 3 & 24 & 9 & 12 & 19 & 15 & 15 \\ 7 & 1 & 8 & 28 & 2 & 1 & 22 & 26 \end{bmatrix} = C$$

Decryption

Multiply matrix C by the decryption matrix A^{-1}, resulting in $A^{-1}C=B$.

$$\begin{bmatrix} 6 & 26 \\ 19 & 16 \end{bmatrix} * \begin{bmatrix} 22 & 3 & 24 & 9 & 12 & 19 & 15 & 15 \\ 7 & 1 & 8 & 28 & 2 & 1 & 22 & 26 \end{bmatrix} =$$

$$\begin{bmatrix} 314 & 44 & 352 & 782 & 124 & 140 & 662 & 766 \\ 530 & 73 & 584 & 619 & 260 & 377 & 637 & 701 \end{bmatrix}$$

Decryption

Take the mod 29 value of the matrix

$$\begin{bmatrix} 314 & 44 & 352 & 782 & 124 & 140 & 662 & 766 \\ 530 & 73 & 584 & 619 & 260 & 377 & 637 & 701 \end{bmatrix} \mod 29 =$$

$$\begin{bmatrix} 24 & 15 & 4 & 28 & 8 & 24 & 24 & 12 \\ 8 & 15 & 4 & 10 & 28 & 0 & 28 & 5 \end{bmatrix}$$

Decryption

Use Table 1 to convert each of the values in the resulting vectors back to letters.

$$\begin{bmatrix} 24 & 15 & 4 & 28 & 8 & 24 & 24 & 12 \\ 8 & 15 & 4 & 10 & 28 & 0 & 28 & 5 \end{bmatrix} =$$

$$\begin{bmatrix} Y & P & E & \_ & I & Y & Y & M \\ I & P & E & K & \_ & A & \_ & F \end{bmatrix}$$

Decryption

Use Table 1 to convert each of the values in the resulting vectors back to letters.

$$\begin{bmatrix} 24 & 15 & 4 & 28 & 8 & 24 & 24 & 12 \\ 8 & 15 & 4 & 10 & 28 & 0 & 28 & 5 \end{bmatrix} =$$

$$\begin{bmatrix} Y & P & E & \_ & I & Y & Y & M \\ I & P & E & K & \_ & A & \_ & F \end{bmatrix}$$

“YIPPEE KI YAY MF”

Challenges

- Large encryption key pose challenge

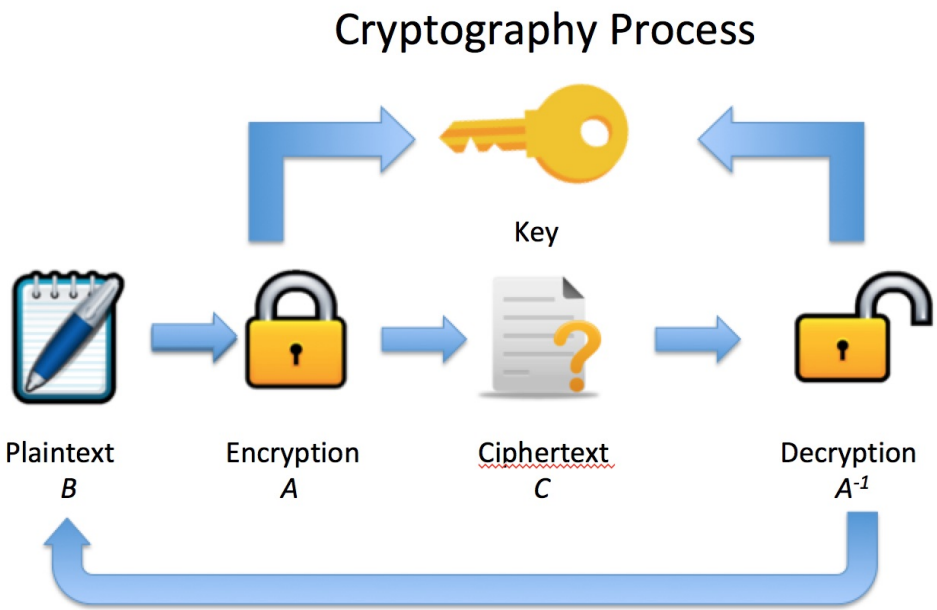
Challenges

- Large encryption key pose challenge
- However, not an issue in modern day

Challenges

- Large encryption key pose challenge
- However, not an issue in modern day
- Important step towards modern cryptography
  - elliptical curve cryptography

Hill Cipher Process



$$A^{-1}AB = A^{-1}C$$

Summary

- Hill Cipher uses linear algebra to encrypt and decrypt messages!

Summary

- Hill Cipher uses linear algebra to encrypt and decrypt messages!
- Influence in modern day cryptograpy.

Summary

- Hill Cipher uses linear algebra to encrypt and decrypt messages!
- Influence in modern day cryptograpy.
- Everywhere: email, credit card transaction, ATM

Thank you for listening!

Questions?