Matrices and Cryptography

32nd Math Conference
16th February, 2019

Presenter: Chi Luong
Advisor: Iason Rusodimos

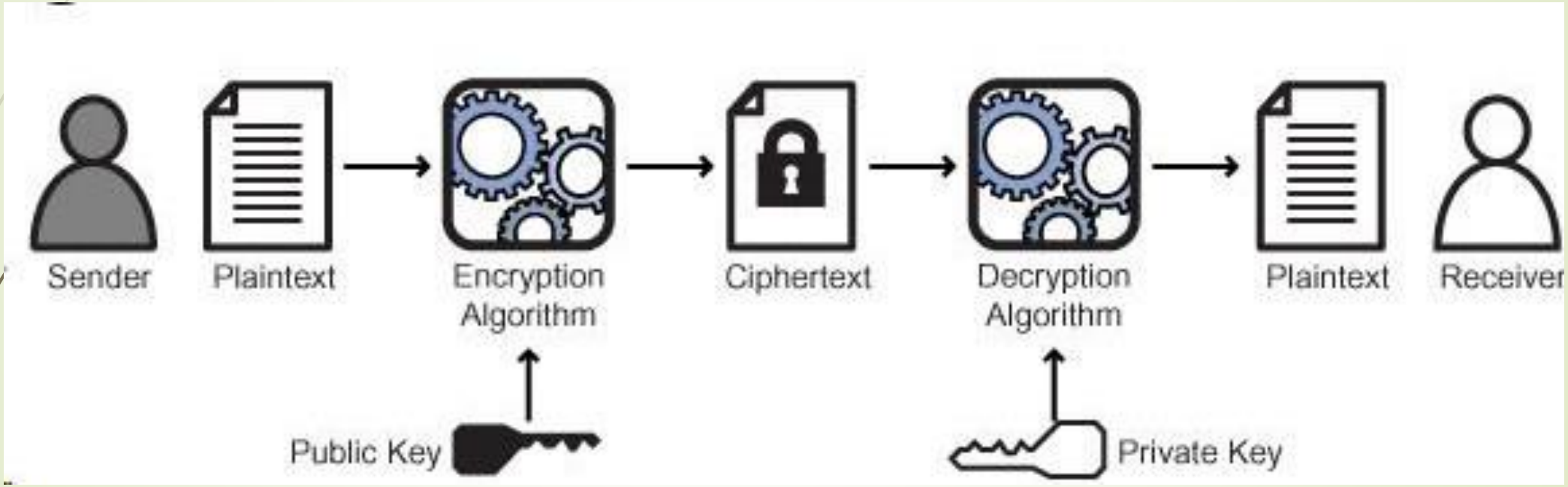
Content

- Cryptography in general
- Methodology
- Example and Result
- Code Breaking
- Conclusion

CRYPTOGRAPHY

- Cryptography, the science of encrypting and decrypting message written in secret code
- Encryption is the transformation of data in to some unreadable form
- Decryption is the reverse of encryption, it is the transformation of encrypted data back in to some intelligible form
- **Key**

CRYPTOGRAPHY



METHODOLOGY

- Encoding process
  - assign a number for each letter of the alphabet, i.e A is 1, B is 2, and so on
  - Convert the message into stream of numbers
  - Place the numerals into some matrices **m**x**n** which is **m** is row-column of key matrix (square matrix)
  - Multiply these matrices by the Encoding matrix (key matrix)
  - Convert the result matrix into stream of numerals and send it to receiver
- Decoding process
  - Place the encrypted stream of numbers that represent the encrypted message in to a matrix **m**x**n**
  - Multiply this matrix by the Decoding matrix(inverse's key matrix)
  - Convert the result matrix into stream of numbers
  - Convert this stream of numbers into text of original message

EXAMPLE AND RESULT

Assume the message is

C O M P U T E R S C I E N C E

3 15 13 16 21 20 5 18 0 19 3 9 5 14 3 5

$$\begin{pmatrix}3\\15\\13\\16\end{pmatrix}, \begin{pmatrix}21\\20\\5\\18\end{pmatrix}, \begin{pmatrix}0\\19\\3\\9\end{pmatrix}, \begin{pmatrix}5\\14\\3\\5\end{pmatrix}$$

The **key** (encoding matrix is invertible matrix) $M = \begin{pmatrix}3 & 0 & 1 & 1\\1 & 2 & 5 & 0\\1 & 1 & 3 & 0\\2 & 0 & 1 & 1\end{pmatrix}$

EXAMPLE AND RESULT

Multiply those column vectors on the left by M:

$$\begin{pmatrix} 3 & 0 & 1 & 1 \\ 1 & 2 & 5 & 0 \\ 1 & 1 & 3 & 0 \\ 2 & 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} 3 \\ 15 \\ 13 \\ 16 \end{pmatrix} = \begin{pmatrix} 38 \\ 98 \\ 57 \\ 35 \end{pmatrix} \qquad M \begin{pmatrix} 21 \\ 20 \\ 5 \\ 18 \end{pmatrix} = \begin{pmatrix} 86 \\ 86 \\ 56 \\ 65 \end{pmatrix} \qquad M \begin{pmatrix} 0 \\ 19 \\ 3 \\ 9 \end{pmatrix} = \begin{pmatrix} 12 \\ 53 \\ 28 \\ 12 \end{pmatrix} \qquad M \begin{pmatrix} 5 \\ 14 \\ 3 \\ 5 \end{pmatrix} = \begin{pmatrix} 23 \\ 48 \\ 28 \\ 18 \end{pmatrix}$$

The encoded numeric message to be sent:

38, 98, 57, 35, 86, 86, 56, 65, 12, 53, 28, 12, 23, 48, 28, 18

EXAMPLE AND RESULT

To decode the message, receiver need compute inverse of matrix M

$$M^{-1} = \begin{pmatrix} 1 & 0 & 0 & -1 \\ 2 & 3 & -5 & -2 \\ -1 & -1 & 2 & 1 \\ -1 & 1 & -2 & 2 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 & -1 \\ 2 & 3 & -5 & -2 \\ -1 & -1 & 2 & 1 \\ -1 & 1 & -2 & 2 \end{pmatrix} \begin{pmatrix} 38 \\ 98 \\ 57 \\ 35 \end{pmatrix} = \begin{pmatrix} 3 \\ 15 \\ 13 \\ 16 \end{pmatrix} \quad M^{-1} \begin{pmatrix} 86 \\ 86 \\ 56 \\ 65 \end{pmatrix} = \begin{pmatrix} 21 \\ 20 \\ 5 \\ 18 \end{pmatrix} \quad M^{-1} \begin{pmatrix} 12 \\ 53 \\ 28 \\ 12 \end{pmatrix} = \begin{pmatrix} 0 \\ 19 \\ 3 \\ 9 \end{pmatrix} \quad M^{-1} \begin{pmatrix} 23 \\ 48 \\ 28 \\ 18 \end{pmatrix} = \begin{pmatrix} 5 \\ 14 \\ 3 \\ 5 \end{pmatrix}$$

The decryption numbers are 3,15, 13, 16, 21, 20, 5, 18, 0, 19, 3, 9, 5, 14, 3, 5

EXAMPLE AND RESULT

```
In[6]:= m = {{3, 0, 1, 1}, {1, 2, 5, 0}, {1, 1, 3, 0}, {2, 0, 1, 1}}
        m.{{3}, {15}, {13}, {16}}
        m.{{21}, {20}, {5}, {18}}
        m.{{0}, {19}, {3}, {9}}
        m.{{5}, {14}, {3}, {5}}

Out[6]= {{3, 0, 1, 1}, {1, 2, 5, 0}, {1, 1, 3, 0}, {2, 0, 1, 1}}

Out[7]= {{38}, {98}, {57}, {35}}

Out[8]= {{86}, {86}, {56}, {65}}

Out[9]= {{12}, {53}, {28}, {12}}

Out[10]= {{23}, {48}, {28}, {18}}
```

```
In[11]:= Inverse[m].{{38}, {98}, {57}, {35}}
         Inverse[m].{{86}, {86}, {56}, {65}}
         Inverse[m].{{12}, {53}, {28}, {12}}
         Inverse[m].{{23}, {48}, {28}, {18}}

Out[11]= {{3}, {15}, {13}, {16}}

Out[12]= {{21}, {20}, {5}, {18}}

Out[13]= {{0}, {19}, {3}, {9}}

Out[14]= {{5}, {14}, {3}, {5}}
```

Code Breaking

Suppose that you intercepted the following coded in war message

275, 25, 161, 15, 307, 205, 173, 181, 120, 101

Your source inform you that the key is 2x2 matrix and your intuition tells you that it is **get** something

Take first 4 letters of encryption message representing for [G,E][T,__] , put them in the 2x2 matrix

$$\begin{pmatrix} 275 & 25 \\ 161 & 15 \end{pmatrix}$$

The key matrix (2x2) can be written as a form

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

We already know that G,E,T,__ were represented by numbers **7, 5, 20, 0**

Code Breaking

Set up the linear system and solve:

$$\begin{cases} 7A+20B=275 \\ 5A=25 \\ 7C+20D=161 \\ 5C=15 \end{cases}$$

solution is

$$\begin{cases} A=5 \\ B=12 \\ C=3 \\ D=7 \end{cases}$$

The key matrix M is $\begin{pmatrix} 5 & 12 \\ 3 & 7 \end{pmatrix}$

The inverse of it: $M^{-1}=\begin{pmatrix} -7 & 12 \\ 3 & -5 \end{pmatrix}$

Multiply the encrypted message by the inverse matrix:

$$\begin{pmatrix} -7 & 12 \\ 3 & -5 \end{pmatrix}\begin{pmatrix} 275 & 25 & 161 & 15 & 307 \\ 205 & 173 & 181 & 120 & 101 \end{pmatrix}=\begin{pmatrix} 7 & 5 & 20 & 0 & 23 \\ 5 & 1 & 16 & 15 & 14 \end{pmatrix}$$

The numeric message is 7,5, 20, 0, 23, 5, 1, 16, 15, 14

Consider the decoded message is **GET WEAPON**

CONCLUSION

- The proposed method is very simple in its principle and has great potential to be applied to other situations
- This provides a transaction of small amount of message between the sender and the receiver
- Higher level of secure can be used by combine many method together such as shift the letter to left/right side, multiply stream of numeric message by a number
- Other methods were used in real life: Hill Cypher, Enigma, RSA

ANY QUESTIONS ?