

# Matrices and Cryptography



32<sup>nd</sup> Math Conference  
16<sup>th</sup> February, 2019

Presenter: Chi Luong  
Advisor: Iason Rusodimos

# Content

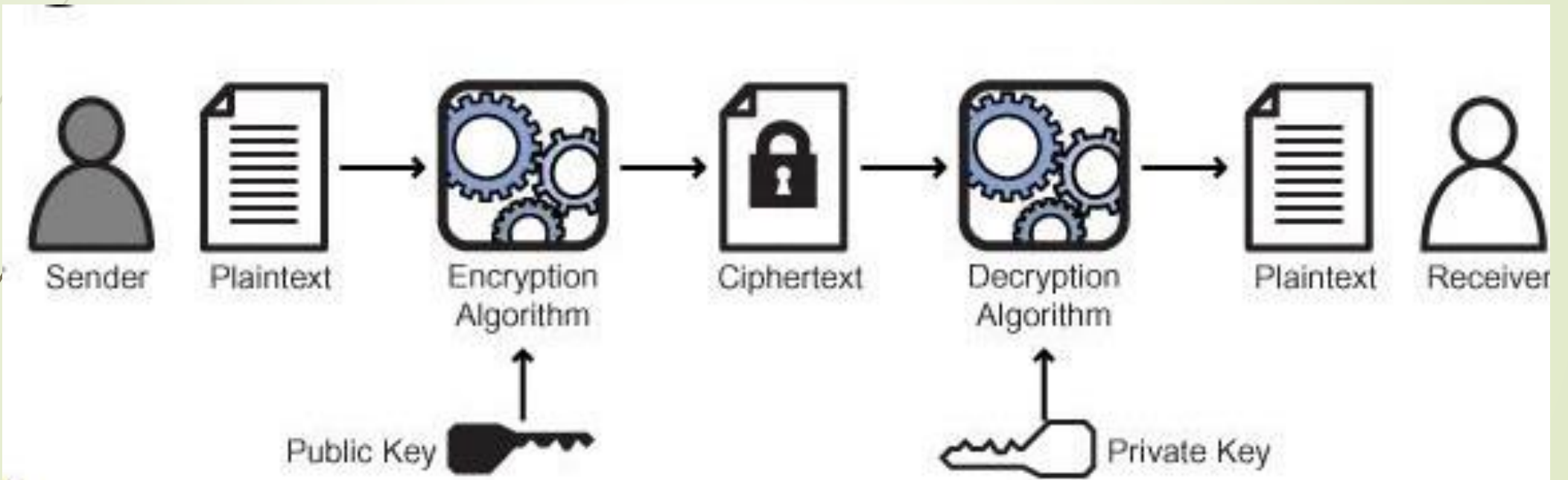
- Cryptography in general
- Methodology
- Example and Result
- Code Breaking
- Conclusion



# 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  $m \times n$  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  $m \times n$
- ❖ 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  $M$ :

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

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

11

Set up the linear system and solve:

$$\begin{cases} 7A + 20B = 275 \\ 5A = 25 \\ 7C + 20D = 161 \\ 5C = 15 \end{cases} \quad \text{solution is} \quad \begin{cases} A = 5 \\ B = 12 \\ C = 3 \\ D = 7 \end{cases}$$

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



13

52768597	02605554864	22301123254	56452768597	02605554864	22301123254	56452768597	02605554864	22301123
97546567	52107905648	89780158595	45197546567	52107905648	89780158595	45197546567	52107905648	89780158
66666666	9201.265340	46243801255	67666666666	9201.265340	46243801255	67666666666	9201.265340	46243801
65468597	5326498235.	56897845022	66665468597	5326498235.	56897845022	66665468597	5326498235.	56897845
21342430	3125643754	24584686530	52421342430	03125643754	24584686530	52421342430	03125643754	24584686
29752834	34201326497	44565752389	43529752834	34201326497	44565752389	43529752834	34201326497	44565752
56749758	88260214687	70122648654	01356749758	88260214687	70122648654	01356749758	88260214687	7012264
01326798	95462032156	89901245984	53701326798	95462032156	89901245984	53701326798	95462032156	89901245
60546412	87546200012	56578021657	78760546412	87546200012	56578021657	78760546412	87546200012	56578021
01352679	56489854222	89535670000	56701352679	56489854222	89535670000	56701352679	56489854222	89535670
524.2134	30215021569	01444587901	886524.2134	30215021569	01444587901	886524.2134	30215021569	01444587
54240404	87459823654	89564875564	54654240404	87459823654	89564875564	54654240404	87459823654	89564875
21404359	85123030213	02654895465	23421404359	85123030213	02654895465	23421404359	85123030213	02654895
53402213	13311123150	13025165465	78553402213	13311000011	13025165465	78553402213	13311125644	13025165
58672464	25468952654	76540215497	49758672464	25468952654	76540215497	49758672464	25468952654	76540215
68652031	78021328503	87654860216	97968652031	78021328503	87654860216	97968652031	78021328503	87654860
79561203	57920045685	54897564202	25679561203	57920045685	54897564202	25679561203	57920045685	54897564
56530979	48314904153	15465465460	26456530979	48314904153	15465465460	26456530979	48314904153	15465465
32031246	18946516746	21654					1246	18946516746
56452123	51561687515	40216					2123	51561687515
45754545	23162685421	56102					4545	23162685421
91675425	62964975421	62165					5425	62964975421
59782135	35656497652	13245450154	34659782135	35656497652	13245450154	34659782135	35656497652	13245450
23100002	31200124556	84987984301	64023100002	31200124556	84987984301	64023100002	31200124556	84987984
56462857	87976423120	24568765435	13656462857	87976423120	24568765435	13656462857	87976423120	24568765
45622256	31655976421	01235435435	55645622256	31655976421	01235435435	55645622256	31655976421	01235435
66566433	05234605242	43021648576	79866566433	05234605242	43021648576	79866566433	05234605242	43021648
23101346	59257561221	53441100000	59823101346	59257561221	53441100000	59823101346	59257561221	53441100
57242104	56024565237	00000001243	56457242104	56024565237	00000001243	56457242104	56024565237	00000001
68976543	85421245454	53727672034	23168976543	85421245454	53727672034	23168976543	85421245454	53727672
12124567	45456402124	25375763520	24212124567	45456402124	25375763520	24212124567	45456402124	25375763
12054976	24575454012	43597572672	54212054976	24575454012	43597572672	54212054976	24575454012	43597572
23051564	42245454440	40133727967	85323051564	42245454440	40133727967	85323051564	42245454440	40133727
46791630	55546520303	97801322479	65246791630	55546520303	97801322479	65246791630	55546520303	97801322
52675642	40555120245	69675014372	21352675642	40555120245	69675014372	21352675642	40555120245	69675014
21000231	21205512563	97846520434	13421000231	21205512563	97846520434	13421000231	21205512563	97846520
00000005	23564012452	52768975403	24000000005	23564012452	52768975403	24000000005	23564012452	52768975
24242412	54545450215	24214672732	42424242412	54545450215	24214672732	42424242412	54545450215	24214672
52424524	88879564501	03427679854	75452424524	88879564501	03427679854	75452424524	88879564501	03427679
01243424	55556523154	64031254596	97501243424	55556523154	64031254596	97501243424	55556523154	64031254

**ANY QUESTIONS ?**