CRYPTOGRAPHY

Elaine, Tony, Kenneth, and Alyssa.

WHAT IS CRYPTOGRAPHY?

- The study of code for secure transmission of messages, protection of data, and provide privacy and security in any situation where information is not intended for public consumption.

THE HISTORY OF CRYPTOGRAPHY

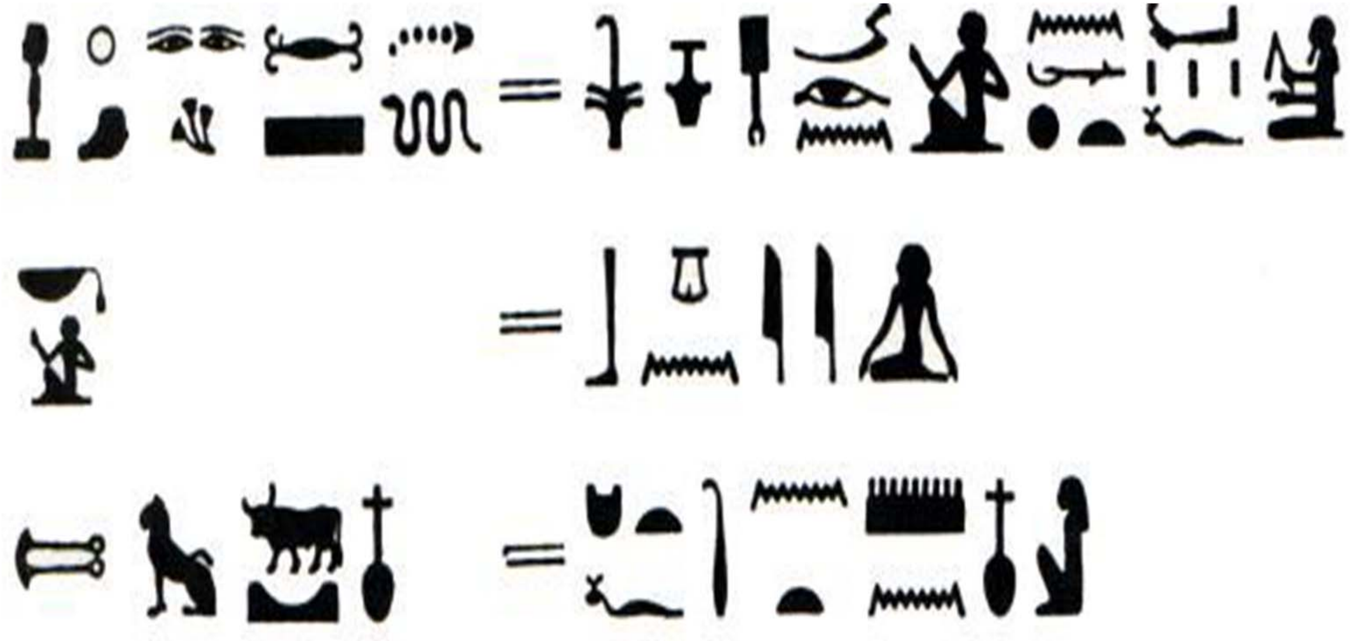
- **Purpose**:
  - *in the past*: **mostly using by the national leaders and the intelligent exchanging message**.
  - ***T*oday**: business, government, and people are used to conceal secret message
    - Example: personal or private access such as bank account, wi-fi, and credit card.

FIRST USE OF CRYPTOGRAPHY

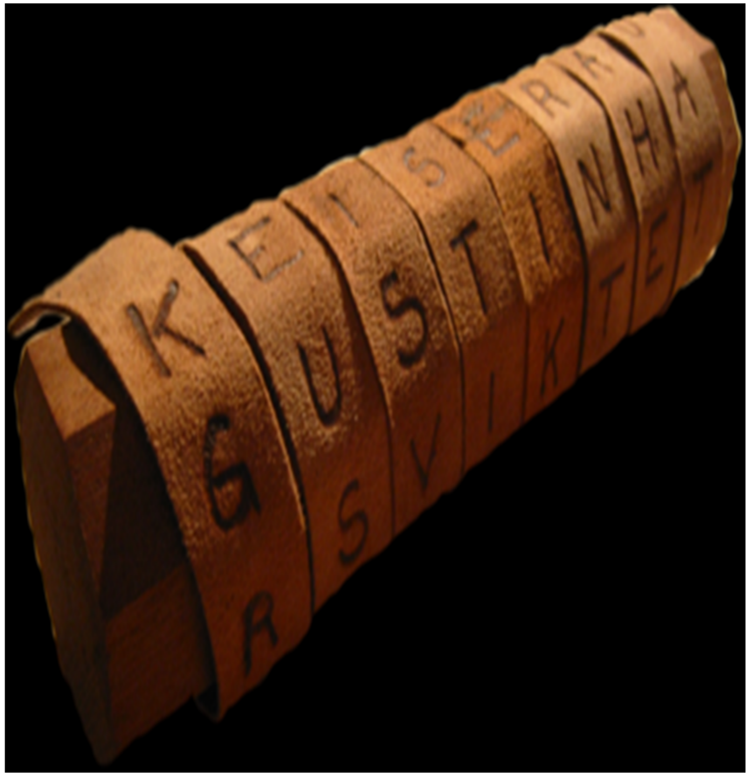
The Early Egyptians, 1900 B.C.:

The first known users of cryptography. It is hypothesized that this encryption existed to guard religious secrets from the eyes of prying outsiders.

Common hieroglyphs were substituted for less common hieroglyphs, so the message would only be clear to the person who encrypted it.



EARLY CRYPTOGRAPHY:



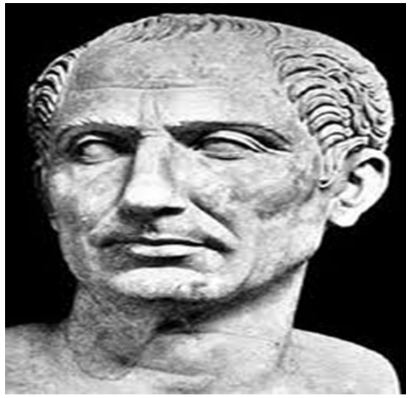
- Greece, 700 BC
- The Scytale. (Pronounced like Italy)
- It is the oldest known military ciphering method.
- The desired message was written along the leather belt, and then revealed once wrapped around a baton.

EARLY CRYPTOGRAPHY:

- The Caesar Cipher, a type of substitution cipher.
- By replacing the individual letters of the message with the corresponding letter three positions down, the message is successfully encrypted,
- Eg: A→D, B→E

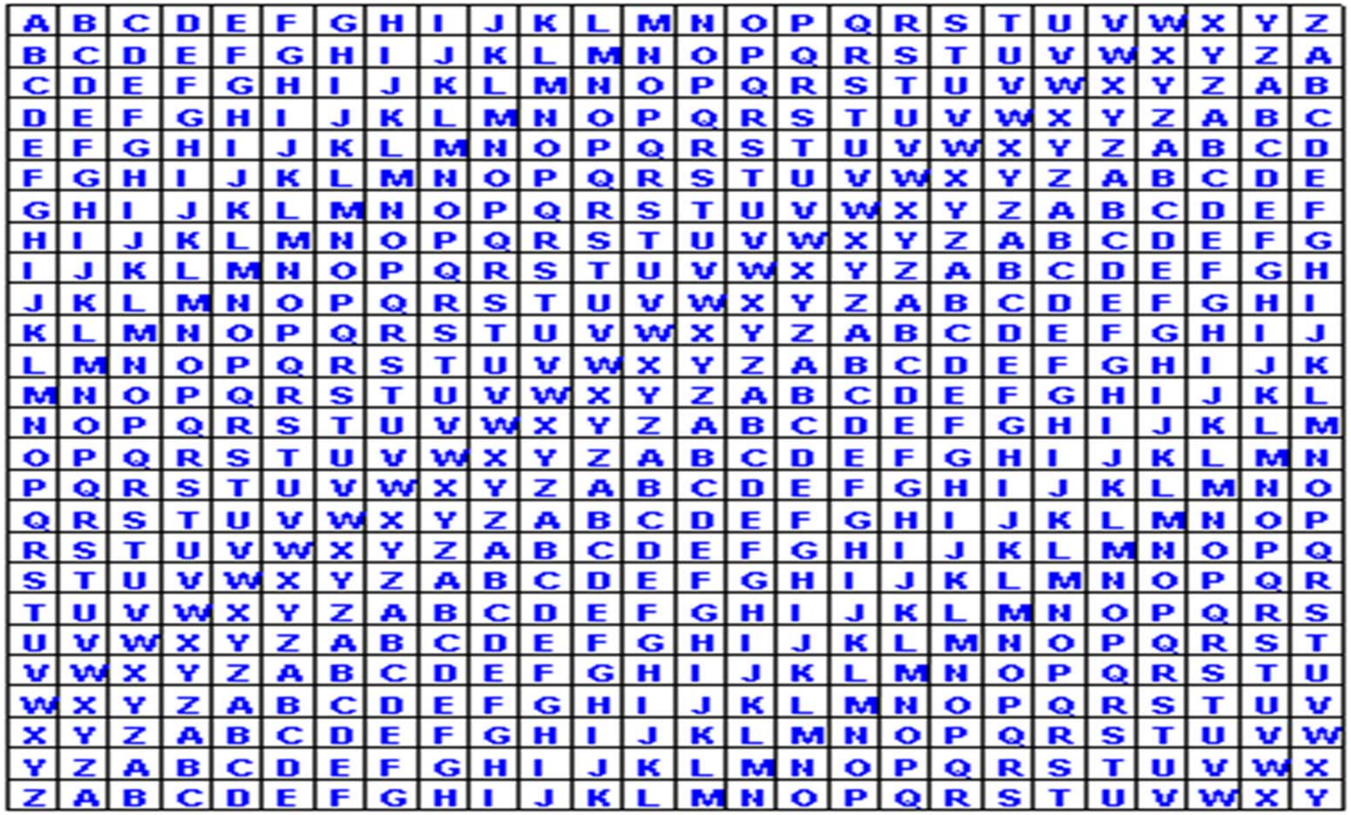
“ATTACK” → “DWWDFN”

Caesar Cipher 50 BC



Julius Caesar

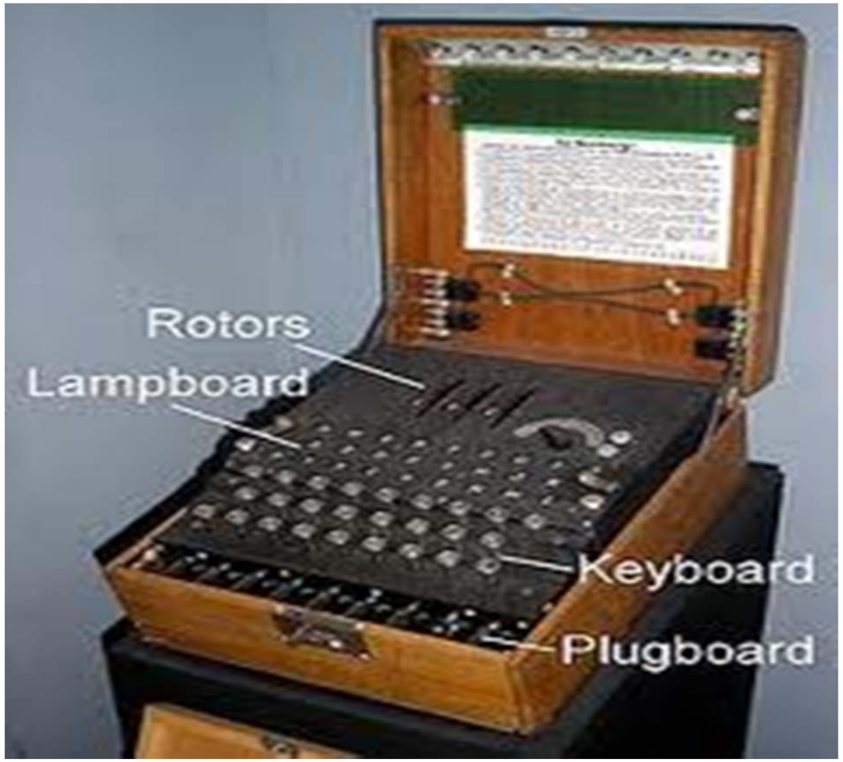
MODERN CRYPTOGRAPHY:



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
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	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	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

- Vigenere cipher

MODERN CRYPTOGRAPHY:



- *Enigma Machine in 1918*

COMPLEX OVER TIME:

- *Brain and computer*: As man grew more advanced, so did their methodology for keeping secrets.
- *Mathematical methods:* provide high level of security from hiding messages from *prying eyes*.

EXAMPLE OF APPLYING THE CRYPTOGRAPHY

Encryption Process by substitution:

- Message: “I LOVE LINEAR ALGEBRA”
- Encrypting by → number substitution: A = 1, B = 2, ... and space = 27

EXAMPLE OF CRYPTOGRAPHY USING TODAY:

Encryption Process:

- After assignment, the numbers are ordered into a **3 x 7** matrix and a specific **encoding matrix** is chosen. When multiplied together, the result is the ciphertext.

$$\begin{bmatrix} -3 & -3 & -4 \\ 0 & 1 & 1 \\ 4 & 3 & 4 \end{bmatrix} \begin{bmatrix} 9 & 15 & 27 & 14 & 18 & 12 & 2 \\ 27 & 22 & 12 & 5 & 27 & 7 & 18 \\ 12 & 5 & 9 & 1 & 1 & 5 & 1 \end{bmatrix}$$

EXAMPLE OF CRYPTOGRAPHY USING TODAY:

- The **cipher-text**:

$$\begin{bmatrix} -156 & -131 & -153 & -61 & -139 & -77 & -64 \\ 39 & 27 & 21 & 6 & 28 & 12 & 19 \\ 165 & 146 & 180 & 75 & 157 & 89 & 66 \end{bmatrix}$$

DECRYPTING THE MESSAGE

- *Invert the encoding matrix*:

$$\begin{bmatrix} 1 & 0 & 1 \\ 4 & 4 & 3 \\ -4 & -3 & -3 \end{bmatrix}$$

Then:

$$\begin{bmatrix} 1 & 0 & 1 \\ 4 & 4 & 3 \\ -4 & -3 & -3 \end{bmatrix} \begin{bmatrix} -156 & -131 & -153 & -61 & -139 & -44 & -165 \\ 39 & 27 & 21 & 6 & 28 & 7 & 28 \\ 165 & 146 & 180 & 75 & 157 & 51 & 183 \end{bmatrix}$$

THE DECRYPTED MESSAGE

$$\begin{bmatrix} 9 & 15 & 27 & 14 & 18 & 12 & 2 \\ 27 & 22 & 12 & 5 & 27 & 7 & 18 \\ 12 & 5 & 9 & 1 & 1 & 5 & 1 \end{bmatrix}$$

- Reading downward from column to column;

- I LOVE LINEAR ALGEBRA

- 9 $\underline{27}$ 12 15 22 5 $\underline{27}$ 12 9 14 5 1 18 $\underline{27}$ 1 12 7 5 2 18 1

FUTURE MATH: