

# Cryptography

## Symmetric Key Cryptography Cipher Algorithms

M S Vilku

-- 23 Sep 2024(C1/ C3) class cancelled

27 Sep 2024(C5)

Sat 21 Sep 2024(C1/ C3/c5)

Sat 28 Sep 2024(C1/ C3)

--07/9 Sep 24 (C1)

# Symmetric Key Cryptography techniques

- Substitution Techniques
- Polyalphabetic ciphers
- The Vigenère cipher

# Symmetric Key Cryptography techniques

- Substitution Techniques
- Polyalphabetic ciphers
- Another way to improve on the simple **monoalphabetic** technique is to use **different monoalphabetic substitutions** as one proceeds through the plaintext message.
- The general name for this **approach** is **polyalphabetic cipher**.
- All the techniques have the following features in common.
  - A **set of related monoalphabetic substitution rules** are used
  - A **key determines** which particular rule is chosen for a given transformation.


# Symmetric Key Cryptography techniques

- Substitution Techniques
- The Vigenère cipher
- Vigenère cipher
- Vigenère (French) pronunciation: [viʒnɛːʁ])
- Vigenère cipher is a method of encrypting alphabetic text by using a **simple form of polyalphabetic substitution**.
- The Vigenère cipher is a **polyalphabetic substitution** cipher that uses a **keyword** to shift letters in the plaintext.
- It's a **stronger cipher than monoalphabetic** ciphers because it uses **multiple Caesar shifts** based on the keyword, which makes it more **resistant to frequency analysis**.
- In essence, **each plaintext character** is encrypted with a **different Caesar cipher**, depending on the corresponding key character.

The cipher uses a **keyword** to shift letters in the plaintext.

# Symmetric Key Cryptography techniques

- Substitution Techniques
- Vigenère cipher
- Encryption: Each **letter in the plaintext** is shifted by the **corresponding letter in the key**.
- The **amount of shift** is determined by the **position of the key letter in the alphabet** (A = 0, B = 1, C = 2, etc.).
- Encryption Process:
  - For example,
  - let's encrypt the plaintext **HELLO**
  - with the key **KEY**
  - Repeat the key **until it matches the length** of the plaintext:
  - **key - KEYKE**



```
Plaintext: H E L L O
Key:      K E Y K E
```

# Symmetric Key Cryptography techniques

```
Plaintext: H E L L O  
Key:      K E Y K E
```

- Substitution Techniques
- Vigenère cipher
- Now, shift each letter in the plaintext by the corresponding letter in the key:
- H shifted by K (10 positions) becomes R
- E shifted by E (4 positions) becomes I
- L shifted by Y (24 positions) becomes J
- L shifted by K (10 positions) becomes V
- O shifted by E (4 positions) becomes S
- So, the ciphertext would be **RIJVS**.

# Symmetric Key Cryptography techniques

- Vigenère table

	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
A	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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



# Symmetric Key Cryptography techniques

- Vigenère table

MICHIGAN TECHNOLOGICAL UNIVERSITY

HOUGHTON

	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
A	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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



# Symmetric Key Cryptography techniques

- Vigenère table

MICHIGAN TECHNOLOGICAL UNIVERSITY

HOUGHTON

MICHIGAN TECHNOLOGICAL UNIVERSITY  
HOUGHTON HOUGHTONHOUGH TONHOUGHTO

	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
A	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

# Symmetric Key Cryptography techniques

- Vigenère table

MICHIGAN TECHNOLOGICAL UNIVERSITY

HOUGHTON

MICHIGAN TECHNOLOGICAL UNIVERSITY  
HOUGHTON HOUGHTONHOUGH TONHOUGHTO

	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
A	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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



# Symmetric Key Cryptography techniques

- Vigenère table

MICHIGAN TECHNOLOGICAL UNIVERSITY

HOUGHTON

MICHIGAN TECHNOLOGICAL UNIVERSITY  
HOUGHTON HOUGHTONHOUGH TONHOUGHTO

MICHI GANTE CHNOL OGICA LUNIV ERSIT Y  
HOUGH TONHO UGHTO NHOUG HTONH OUGHT O

TWWNP ZOAAS WNUHZ BNWWG SNBVC SLYPM M

	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
A	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

# Symmetric Key Cryptography techniques

- **Vigenère table**
- To decrypt, pick a letter in the ciphertext and its corresponding letter in the keyword, use the keyword letter to find the corresponding row, and the letter heading of the column that contains the ciphertext letter is the needed plaintext letter. For example, to decrypt the first letter **T** in the ciphertext, we find the corresponding letter **H** in the keyword. Then, the row of **H** is used to find the corresponding letter **T** and the column that contains **T** provides the plaintext letter **M** (see the above figures). Consider the fifth letter **P** in the ciphertext. This letter corresponds to the keyword letter **H** and row **H** is used to find **P**. Since **P** is on column **I**, the corresponding plaintext letter is **I**.

	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
A	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

MICHI GANTE CHNOL OGICA LUNIV ERSIT Y  
HOUGH TONHO UGHTO NHOUG HTONH OUGHT O

TWWNP ZOAAS WNUHZ BNWWG SNBVC SLYPM M

# Symmetric Key Cryptography techniques

- **Vigenère table**

- For example, to decrypt the first letter **T** in the ciphertext, we find the corresponding letter **H** in the keyword.
- Then, the row of **H** is used to find the corresponding letter **T** and the column that contains **T** provides the plaintext letter **M**
- Consider the fifth letter **P** in the ciphertext. This letter corresponds to the keyword letter **H** and row **H** is used to find **P**.
- Since **P** is on column **I**, the corresponding plaintext letter is **I**.

MICHI GANTE CHNOL OGICA LUNIV ERSIT Y  
HOUGH TONHO UGHTO NHOUG HTONH OUGHT O

TWWNP ZOAAS WNUHZ BNWWG SNBVC SLYPM M

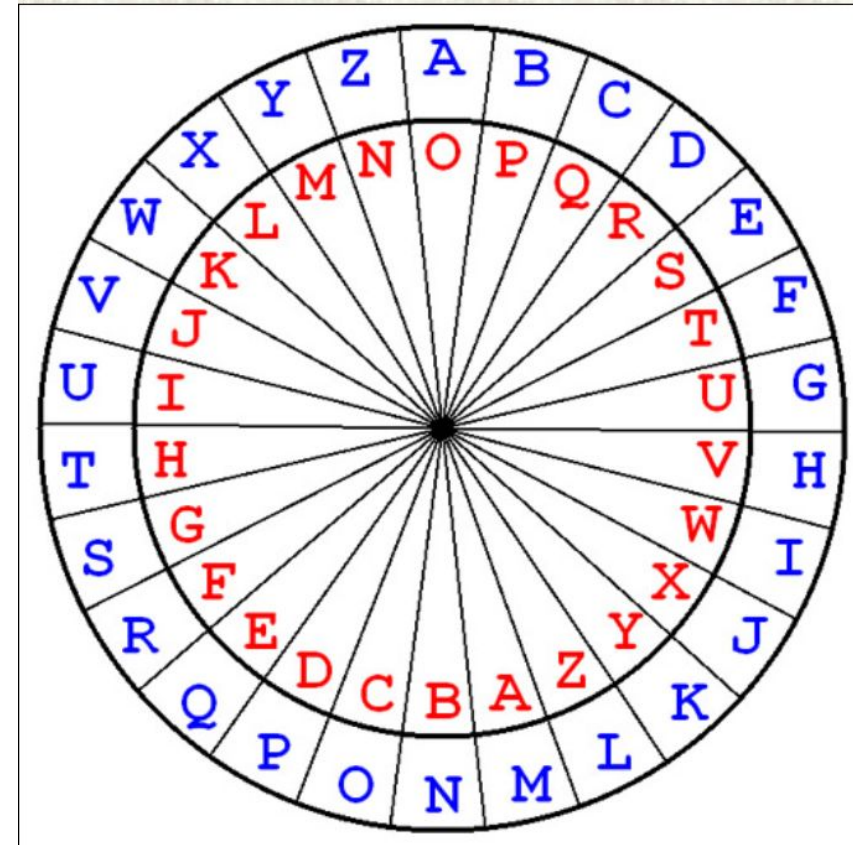
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T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



# Symmetric Key Cryptography techniques

- **Other Vigenère Cipher Devices**

- Since the **Vigenère table** is large and not very convenient,
- two portable devices were developed to make encryption and decryption easier. The first device, the ***cipher disk***, was invented by Leon Battista Alberti (1404--1472).
- This cipher disk has two concentric disks, with the large bottom one fixed and the small top one rotatable. The 26 English letters are shown along the perimeter of each disk. One can rotate the top disk to align any letter with the letter **A** on the bottom disk. The plaintext and ciphertext use the letters on the bottom and top disks, respectively

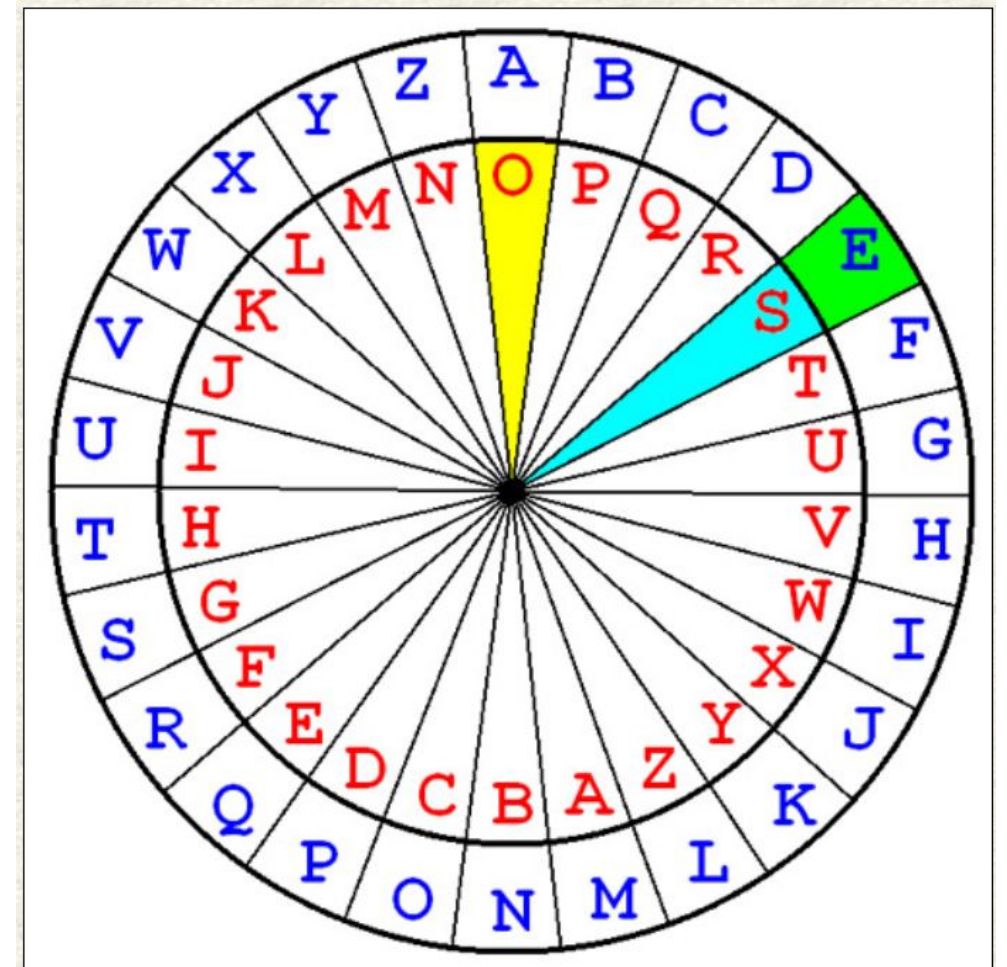


MICHI GANTE CHNOL OGICA LUNIV ERSIT Y  
HOUGH TONHO UGHTO NHOUG HTONH OUGHT O

TWWNP ZOAAS WNUHZ BNWWG SNBVC SLYPM M

# Symmetric Key Cryptography techniques

- **Other Vigenère Cipher Devices**
- **Rotate the top disk** so that the keyword letter being used aligns with the letter A on the bottom disk, and the corresponding plaintext and ciphertext letters are on the bottom and top disks, respectively.
- This **alignment procedure** is equivalent to **shifting the rows down**. For example, if two As are aligned together, we are using row A; if B is aligned with A, we are using row B; and if C is aligned with A, we are using row C. Therefore, the cipher disk uses a rotatable disk to replace a large table, and is more convenient.



MICHI GANTE CHNOL OGICA LUNIV ERSIT Y  
HOUGH TONHO UGHTO NHOUG HTONH OUGHT O

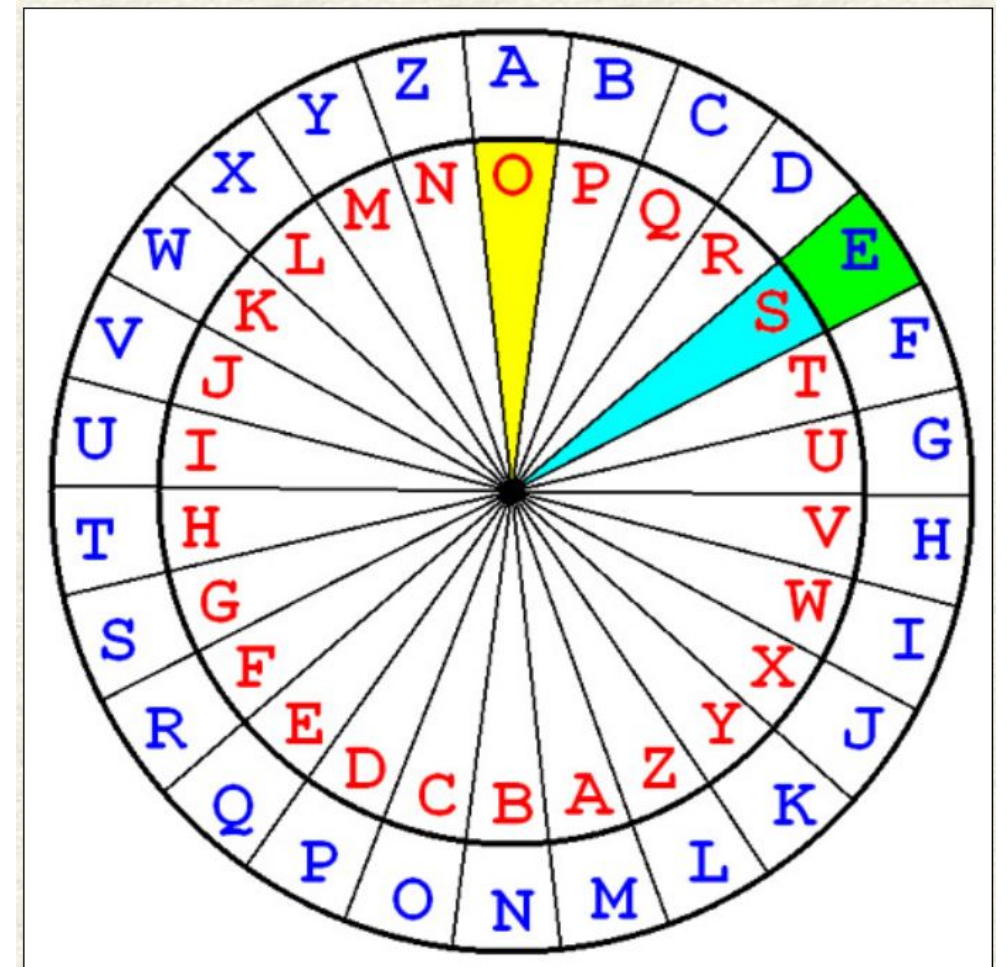
TWWNP ZOAAS WNUHZ BNWWG SNBVC SLYPM M



# Symmetric Key Cryptography techniques

- **Other Vigenère Cipher Devices**

- Consider the **10-th letter E** in the **plaintext** and the corresponding **keyword letter O**
- Rotate the top disk until **O aligns with A** (see the figure below) and, consequently, the plaintext letter E on the bottom disk aligns with the letter S on the top disk. Therefore, E is encrypted to S.



MICHI GANTE CHNOL OGICA LUNIV ERSIT Y  
HOUGH TONHO UGHTO NHOUG HTONH OUGHT O

TWWNP ZOAAS WNUHZ BNWWG SNBVC SLYPM M

# Symmetric Key Cryptography techniques

- **Saint Cyr Slide** or just simply **slide**
- bottom row can be slided left and right and has two sets of the 26 letters (i.e., repeating the 26 letters twice).
- Consider **the 5-th letter I** in our example. Its corresponding keyword letter is **H**.
- Slide the bottom portion so that **H aligns with the A** of the **fixed portion** and
- the plaintext **letter I corresponds to the letter P**.
- Therefore, I is encrypted by H to P.

		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		
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	M	N	O	P

		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		
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	F	G	H	I

MICHI GANTE CHNOL OGICA LUNIV ERSIT Y  
HOUGH TONHO UGHTO NHOUG HTONH OUGHT O

TWWNP ZOAAS WNUHZ BNWWG SNBVC SLYPM M

# Symmetric Key Cryptography techniques

- Substitution Techniques
- Vigenère cipher
- Strength of Vigenere cipher
  - o There are **multiple cipher text letters** for each plaintext letter.
  - o **Letter frequency** information is **obscured**.

# Symmetric Key Cryptography techniques

- **Substitution Techniques**

- **Vigenère cipher**

- Mathematically

- $C = (P + d) \bmod 26$

- For plaintext  $p_1p_2...p_n$ , keyword  $k_1k_2...k_n$  and ciphertext  $c_1c_2...c_n$ , we have

- $c_i = (p_i + k_i) \bmod 26$

- decryption is the reversed procedure by shifting the ciphertext to the left. Since shifting to the left is a subtraction, the decryption procedure is simply:

- $p_i = (c_i - k_i) \bmod 26$

# Symmetric Key Cryptography techniques

- Substitution Techniques
- One Time Pad

# Symmetric Key Cryptography techniques

- **Substitution Techniques**

- **One Time Pad**

- An **Army Signal Corp officer**, Joseph Mauborgne, proposed an **improvement to the Vernam cipher** that yields the ultimate in security.
- Mauborgne suggested using a **random key** that is **as long as the message**, so that the **key need not be repeated**.
- In addition, the key is to be **used to encrypt and decrypt a single message**, and then is **discarded**.
- Each new message **requires a new key** of the **same length as the new message**. Such a scheme, known as a **one-time pad, is unbreakable**.
- It produces **random output** that bears **no statistical relationship** to the plaintext. Because the ciphertext **contains no information whatsoever about the plaintext**, there is simply **no way to break the code**.

# Symmetric Key Cryptography techniques

- **Substitution Techniques**

- **One Time Pad**

- The **security** of the one-time pad is entirely due to the **randomness of the key**. If the stream of characters that constitute the key is truly random, then the stream of characters that constitute the ciphertext will be truly random.
- there are **no patterns or regularities** that a **cryptanalyst can use to attack** the ciphertext.

- **Advantage:**

- Encryption method is completely unbreakable for a ciphertext only attack.

- **Disadvantages**

- It requires a **very long key** which is **expensive** to produce and **expensive** to transmit.
- Once a key is used, it is **dangerous to reuse** it for a second message; any knowledge on the first message would give knowledge of the second.

- **Problems**

- 1) generating larger keys
- 2) distribution of the keys



# Symmetric Key Cryptography techniques

## Transposition Techniques

# Symmetric Key Cryptography techniques

- **Transposition Techniques**

- All the techniques examined so far involve the **substitution** of a cipher text symbol for a plaintext symbol.
- A very different kind of mapping is achieved by performing some sort of **permutation on the plaintext letters**.
- This technique is referred to as a **transposition cipher**.

# Symmetric Key Cryptography techniques

- **Transposition Techniques**
- **Three type**
- Rail Fence Transposition Cipher
- Block (Single Columnar) Transposition Cipher
- Double Columnar Transposition Cipher

# Symmetric Key Cryptography techniques

- Transposition Techniques
- Rail fence ("rails" (lines) )

# Symmetric Key Cryptography techniques

- Transposition Techniques
- Rail fence ("rails" (lines) )
- is simplest of such cipher, in which the **plaintext is written down as a sequence of diagonals and then read off as a sequence of rows.**
- It is also termed as a **zigzag cipher**

# Symmetric Key Cryptography techniques

- Transposition Techniques

- Rail fence ("rails" (lines) )

- is simplest of such cipher, in which the plaintext is written down as a sequence of diagonals and then read off as a sequence of rows.

- Plaintext - *meet at the school house*

- To encipher this message with a rail fence of **depth 2**, we write the message as follows:

*m e a t e c o l o s*

*e t t h s h o h u e*

- The encrypted message is - **MEATECOLOSETTHSHOHUE**

- This sort of thing would **be trivial to cryptanalyze**.

# Symmetric Key Cryptography techniques

- Transposition Techniques

- Rail fence

- A **more complex scheme** is to write the message in a **rectangle, row by row**, and read the message off, **column by column**,

- but **permute** the **order of the columns**.

- The **order of the columns** then becomes the **key** to the algorithm.

- For example, ***Attack postponed until two am***

- Key:       4 3 1 2 5 6 7

- Plaintext: a t t a c k p

o s t p o n e

d u n t i l t

w o a m x y z

- Ciphertext: TTNAAPTMTSUOAODWCOIXKNLYPETZ

Key       4 3 1 2 5 6 7

Plaintext: a t t a c k p

o s t p o n e

d u n t i l t

w o a m x y z



# Symmetric Key Cryptography techniques

- **Transposition Techniques**
- **Rail fence**
- A pure transposition cipher is **easily recognized** because it has the **same letter frequencies** as the original plaintext.
- For the type of columnar transposition above shown, **cryptanalysis is fairly straightforward** and involves laying out the ciphertext in a matrix and playing around with column positions.
- **Digram and trigram** frequency tables can be useful.
- The **transposition** cipher can be made significantly **more secure** by performing **more than one stage of transposition**.
- The result is a more complex permutation that is not easily reconstructed.

# Symmetric Key Cryptography techniques

- Transposition Techniques

- Rail fence

- To visualize the result of this **double transposition**, designate the letters in the original plaintext message by the **numbers designating their position**. Thus, with 28 letters in the message, the original sequence of letters is

```
01 02 03 04 05 06 07 08 09 10 11 12 13 14  
15 16 17 18 19 20 21 22 23 24 25 26 27 28
```

- After the **first transposition**, we have

```
03 10 17 24 04 11 18 25 02 09 16 23 01 08  
15 22 05 12 19 26 06 13 20 27 07 14 21 28
```

- which has a **somewhat regular** structure.
- But after the **second transposition**, the result is

```
17 09 05 27 24 16 12 07 10 02 22 20 03 25  
15 13 04 23 19 14 11 01 26 21 18 08 06 28
```

- This is a much less structured permutation and is much **more difficult to cryptanalyze**.

# Symmetric Key Cryptography techniques

- Transposition Techniques
- Some more techniques
- Columnar Transposition Cipher:
  - The plaintext is written into a **grid of fixed columns, row by row**. The ciphertext is then generated by reading the characters **column by column** in a specified order.
- Double Transposition Cipher:
  - This involves performing the **columnar transposition technique twice** using **different keys** for each transposition. This provides an **additional layer of security by further scrambling** the order of the characters.
- Route Cipher:
  - The plaintext is **written in a grid** and the characters are **read off according to a pre-defined route or pattern**, such as reading **diagonally, spirally, or in an L-shape**.

# Symmetric Key Cryptography techniques

- Transposition Techniques

Given Text = GEEKSFORGEEKS

Keyword = NICK

Keyword 2= BOAT

N	I	C	K
4	2	1	3
G	E	E	K
S	F	O	R
G	E	E	K
s	—	—	—

# Symmetric Key Cryptography techniques

- **Transposition Techniques**
- The message is read in the order in by the keyword.

---

Given Text = GEEKSFORGEES

Keyword = NICK

Keyword 2= BOAT

B	O	A	T
2	3	1	4
G	E	E	K
S	F	O	R
G	E	E	K
S	-	-	-

Cipher Text = EOE\_GSGSEFE\_KRK\_

# Symmetric Key Cryptography techniques

- Transposition Techniques
- Some more techniques
- Scytale Cipher (an ancient transposition cipher):
  - A **strip of parchment is wrapped** around a rod of a certain diameter.
  - The message is written across the strip, and when **unwrapped**, the characters appear scrambled.
  - The correct arrangement is revealed only by **wrapping the parchment** around a **rod of the same diameter**.
  - This method was used in **ancient Greece** and is one of the earliest forms of transposition ciphers.



# Symmetric Key Cryptography techniques

- Transposition Techniques
- Some more techniques
- Disrupted Transposition:
  - In this cipher, the text is **first transposed**, and
  - then **additional characters are added** to disrupt the normal flow of the message.
  - These **added characters are not part of the original message** and are meant to confuse anyone attempting to decrypt the message without knowing the rules of disruption.



# Symmetric Key Cryptography techniques

- **Transposition Techniques**
- **Characteristics of Transposition Techniques:**
- **No Character Substitution:** The characters in the message are only rearranged, not replaced.
- **Same Frequency of Letters:** The **frequency of letters in the ciphertext matches** that of the plaintext, making it vulnerable to certain types of analysis like frequency analysis if the cipher is simple.
- **More Secure with Larger Keyspace:** Repeated or complex transpositions increase the security of the cipher.

# Symmetric Key Cryptography techniques

- Transposition Techniques

- **Strengths:**

- **Simple to implement** but effective in **obfuscating messages**.
- Can be combined with other encryption methods (like substitution) to increase security.

- **Weaknesses:**

- Simple transposition ciphers can be **vulnerable to pattern recognition and frequency analysis**, especially if the message is long.
- Cryptanalysis techniques can **often reverse the transposition by analyzing letter positions or testing various grid configurations**.

# Comparison between monoalphabetic and polyalphabetic

Feature	Monoalphabetic Cipher	Polyalphabetic Cipher
Definition	A substitution cipher that replaces each letter with a fixed corresponding letter.	A substitution cipher that uses multiple substitutions for letters, changing over time or based on the position.
Key Complexity	Typically uses a single key for substitution.	Uses a more complex key, often involving multiple keys or a key phrase.
Encryption Method	Each letter is replaced consistently throughout the message.	Each letter can be replaced by different letters based on the key.
Examples	Caesar cipher, Atbash cipher.	Vigenère cipher, Beaufort cipher.
Frequency Analysis	Vulnerable to frequency analysis; letter frequencies remain constant.	More resistant to frequency analysis due to varying substitutions.
Security Level	Generally less secure; easier to break.	More secure than monoalphabetic ciphers; harder to crack without the key.
Key Length	Key length is usually short (one alphabet).	Key length can be longer and varies; often based on the keyword length.
Use Cases	Simple encryption tasks, puzzles, or historical contexts.	More secure communication needs where stronger encryption is required.
Decryption Process	Straightforward, as the same key is used.	More complex due to the varying substitutions; requires the same key for decryption.

# Steganography

# Steganography

- Steganography is the **practice of hiding secret** information **within a non-secret medium** (such as an **image, video, or audio file**) in a way that conceals the existence of the hidden data.
- Unlike cryptography, which focuses on making the **content of the message unreadable to unauthorized users**,
- steganography **focuses on concealing the fact that a secret message exists at all**. The goal is for the hidden information to **remain undetectable to anyone who doesn't know** where or how to look for it.
- Steganography is the practice of concealing information within another message or physical object to avoid detection. Steganography can be used to hide virtually any type of digital content, including text, image, video, or audio content. That hidden data is then extracted at its destination

# Steganography

- **What is steganography?**
- Steganography is the practice of **concealing information within another message** or physical object to avoid detection. Steganography can be **used to hide virtually any type of digital content**, including text, image, video, or audio content. That hidden data is then **extracted at its destination**.
- Content concealed through steganography is sometimes encrypted **before being hidden** within another file format.
- If it isn't encrypted, then it may be processed in some way to make it harder to detect.

Source: <https://www.kaspersky.com/resource-center/definitions/what-is-steganography>

# Steganography

- **What is steganography?**
- As a form of covert communication, steganography is sometimes **compared to** [cryptography](#).
- However, the two are **not the same**
- since steganography **does not involve scrambling data** upon sending or using a key to decode it upon receipt.
- The term '**steganography**' comes from the Greek words '**steganos**' (which means **hidden** or covered) and 'graphein' (which means **writing**).
- Steganography has been practiced in various **forms for thousands of years** to keep communications private.
- For example, in ancient Greece, people would **carve messages on wood** and then use **wax to conceal them**. Romans used various forms of **invisible inks**, which could be deciphered **when heat or light** were applied.

Source: <https://www.kaspersky.com/resource-center/definitions/what-is-steganography>

# Steganography

- **What is steganography?**
- **Steganography is relevant** to cybersecurity because [ransomware](#) gangs and other threat actors often **hide information** when attacking a target.
- For example, they might **hide data, conceal a malicious tool, or send instructions** for command-and-control servers.
- They could place all this **information within innocuous-seeming image, video, sound, or text files.**

Source: <https://www.kaspersky.com/resource-center/definitions/what-is-steganography>



# Steganography

- **How steganography works**
- Steganography works by concealing information in a way that avoids suspicion. One of the most prevalent techniques is called **'least significant bit' (LSB) steganography**.
- This involves embedding the **secret information in the least significant bits of a media file**.
- For example:
  - In an **image file**, each **pixel is made up of three bytes** of data corresponding to the colors **red, green, and blue**.
  - Some image formats allocate an **additional fourth byte to transparency, or 'alpha'**.
  - **LSB steganography** alters the **last bit of each of those bytes to hide one bit of data**.
  - So, to hide **one megabyte** of data using this method, you would need an **eight-megabyte** image file.

Source: <https://www.kaspersky.com/resource-center/definitions/what-is-steganography>

# Steganography

- **How steganography works**
- For example:
  - Modifying the **last bit of the pixel value doesn't result in a visually perceptible change** to the picture,
  - which means that **anyone viewing the original** and the steganographically-modified images **won't be able to tell the difference**.

Source: <https://www.kaspersky.com/resource-center/definitions/what-is-steganography>

# Steganography

- **How steganography works**

1. The **same method** can be applied to **other digital media, such as audio and video**, where data is **hidden in parts** of the **file that result in the least change** to the audible or **visual output**.

Source: <https://www.kaspersky.com/resource-center/definitions/what-is-steganography>

# Steganography

- How steganography works

2. Another steganography technique is the use of **word or letter substitution**.

- This is where the sender of a **secret message conceals the text by distributing it inside a much larger text**, placing the **words at specific intervals**.
- While this substitution method is easy to use, it may also make the **text look strange and out of place since** the secret words might not fit logically within their target sentences.

3. Other steganography methods include hiding an **entire partition on a hard drive** or embedding **data in the header section of files and network packets**.

- The **effectiveness** of these methods depends on how much data they can hide and how easy they are to detect.

Source: <https://www.kaspersky.com/resource-center/definitions/what-is-steganography>

# Steganography

## Types of steganography

From a **digital perspective**, there are **five main types** of steganography. These are:

1. **Text** steganography
2. **Image** steganography
3. **Video** steganography
4. **Audio** steganography
5. **Network** steganography –so metimes known as **protocol steganography**, is the technique of **embedding information within network control protocols**

Source: <https://www.kaspersky.com/resource-center/definitions/what-is-steganography>

# Steganography

- **Difference Between Steganography and Cryptography:**
- **Steganography:** **Hides** the existence of the message. The hidden data is embedded in a carrier file without changing its apparent form.
- **Cryptography:** **Encodes the message** in a way that **makes it unreadable** to unauthorized users. The encrypted data is still **noticeable**, but its contents are protected.
- **Steganography vs. cryptography**
- Steganography and cryptography **share the same goal** – which is to **protect a message** or information from third parties – but they use different mechanisms to achieve it.
- Cryptography **changes the information** to ciphertext which can only be understood with a **decryption key**. This means that if someone intercepted this encrypted message, they could easily see that some form of encryption has been applied.
- By contrast, steganography **doesn't change the format** of the information but **instead conceals** the existence of the message.



# Steganography

- **Steganography vs. cryptography**

Feature	Cryptography	Steganography
Definition	The practice of securing information by transforming it into an unreadable format.	The technique of hiding information within another medium.
Purpose	To protect the confidentiality, integrity, and authenticity of data.	To conceal the existence of the information.
Visibility	The existence of encrypted data is obvious.	The presence of hidden data is not apparent.
Method	Uses algorithms and keys to encrypt/decrypt data.	Embeds data in files (e.g., images, audio, text).
Examples	AES, RSA, DES, and symmetric/asymmetric encryption.	Hiding text in images (LSB technique), or in audio files.
Security	Secures data even if the encryption method is known; relies on key secrecy.	Security relies on the secrecy of the hidden message and the carrier.
Use Cases	Secure communications, data protection, digital signatures.	Covert communication, watermarking, and digital rights management.
Detectability	Can be detected through analysis of encrypted data.	Harder to detect unless specific methods are used to uncover hidden data.
Strength	Strength depends on algorithm complexity and key length.	Strength relies on the medium used and the method of embedding.

# Steganography



Interesting information

## How steganography is used to deliver attacks

From a **cybersecurity perspective**, threat actors can use **steganography to embed malicious** data within seemingly innocuous files. Since steganography requires significant effort and nuance to get right, its use often involves **advanced threat actors** with specific targets in mind. Here are some ways in which attacks can be delivered via steganography:

### Concealing malicious payloads in digital media files

Digital images can be prime targets because they contain a lot of redundant data that can be manipulated without noticeably altering how the image appears. Since their use is so widespread within the digital landscape, image files tend not to raise red flags about malicious intent. Videos, documents, audio files and even email signatures also offer potential alternative mediums for the use of steganography to plant malicious payloads.

# Steganography



Interesting information

## Ransomware and data exfiltration

Ransomware gangs have also learned that using steganography can help them carry out their attacks. Steganography can also be used in the **data exfiltration stage** of a cyberattack. By **hiding sensitive data** within legitimate communications, steganography provides a means to **extract data without being detected**. With many threat actors now viewing data exfiltration as the primary objective for cyberattacks, security specialists are getting better at implementing measures to detect when data is being extracted, often by monitoring encrypted network traffic.

## Hiding commands in web pages

Threat actors may hide commands for their implants in web pages with whitespace and within debug logs posted to forums, covertly upload stolen data in images, and maintain persistence by storing encrypted code within specific locations.

## Malvertising

Threat actors conducting malvertising campaigns can take advantage of steganography. They can embed malicious code inside online banner ads which, when loaded, extract malicious code and redirect users to an exploit kit landing page.

# Steganography



Interesting information

## Examples of steganography used in cyber attacks

### E-commerce skimming

In 2020, Dutch e-commerce security platform Sansec published research which showed that threat actors had embedded skimming malware inside Scalable Vector Graphics (SVG) on e-commerce checkout pages. The attacks involved a concealed malicious payload inside SVG images and a decoder hidden separately on other parts of the webpages.

Users who entered their details on the compromised checkout pages didn't notice anything suspicious because the images were simple logos from well-known companies. Because the payload was contained within what appeared to be the correct use of SVG element syntax, standard security scanners searching for invalid syntax did not detect the malicious activity.

### SolarWinds

Also in 2020, a group of hackers hid malware inside a legitimate software update from SolarWinds, maker of a popular IT infrastructure management platform. The hackers [successfully breached](#) Microsoft, Intel and Cisco, in addition to various US government agencies. Then, they used steganography to disguise the information they were stealing as seemingly benign XML files served in HTTP response bodies from control servers. The command data within those files was disguised as different strings of text.

# Steganography



Interesting information

## Examples of steganography used in cyber attacks

### Industrial enterprises

Again in 2020, businesses in the United Kingdom, Germany, Italy, and Japan were hit by a campaign using steganographic documents. Hackers **avoided detection** by using a steganographic image uploaded on reputable image platforms, like Imgur, to infect an Excel document. Mimikatz, a malware that steals Windows passwords, was downloaded via a secret script included in the picture.

# Steganography



Interesting information

## How to detect steganography

The practice of detecting steganography is called '**steganalysis**'.

There are various **tools** that can detect the **presence of hidden data**, including StegExpose and StegAlyze.

Analysts may use other general analysis tools such as **hex viewers** to **detect anomalies in files**.

However, **finding files that have been modified through steganography is a challenge** – not least because **knowing where to start looking** for hidden data in the **millions of images** being uploaded on social media every day is **virtually impossible**.

# Steganography

- Various other techniques have been used historically; some examples are the
- **Character marking:** Selected letters of printed or typewritten text are overwritten in pencil. The marks are ordinarily not visible unless the paper is held at an angle to bright light.
- **Invisible ink:** A number of substances can be used for writing but leave no visible trace until heat or some chemical is applied to the paper.
- **Pin punctures:** Small pin punctures on selected letters are ordinarily not visible unless the paper is held up in front of a light.
- **Typewriter correction ribbon:** Used between lines typed with a black ribbon, the results of typing with the correction tape are visible only under a strong light.



**Thank You**

