Cryptography

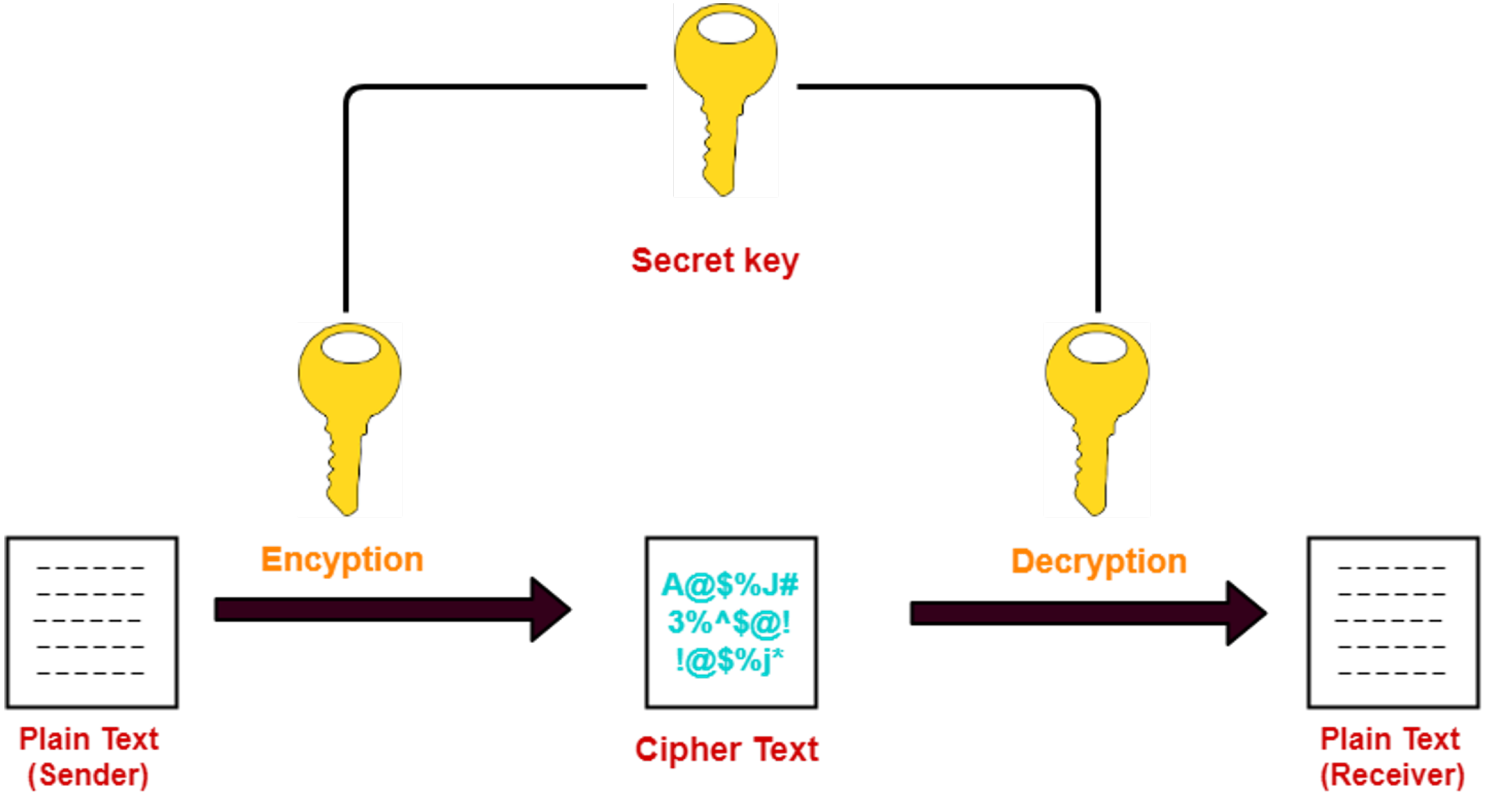
Por Kevin Ortiz

Cryptography

- The prefix "crypt-" means "hidden" and the suffix "-graphy" stands for "writing."
- It’s method of protecting information and communications using codes.
- So that only those for whom the information is intended can read and process it.
- Classical Ciphers: *Caesar, Rail Fence, Vigenere, and Playfair.*

Key Terms

- **Cryptography:** Cryptography is the art of coding messages so only the intended people have access to the information.
- **Plaintext:** The original message or data that is used as input for the cipher algorithm.
- **Ciphertext:** The encrypted message received as output from a cryptographic algorithm.
- **Encryption:** The process of converting from plaintext to ciphertext.
- **Decryption:** the process of converting from ciphertext to plaintext.
- **Key:** A value, keyword, or parameter that determines the output of a cryptographic algorithm.

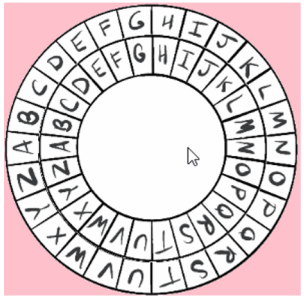


Symmetric Key Cryptography

CAESAR CIPHER

The Caesar cipher is one of the earliest known examples of a substitution cipher. Said to have been used by Julius Caesar to secretly communicate with his army. It involves “shifting” the letters of the alphabet.

The key to the Caesar cipher determines the number of times the letters “shift” on the alphabet to perform an encryption or decryption.



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

KEY 1

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
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

KEY 4

Example #1

- Plaintext: defend the east
- Ciphertext: efgfoe uif fbtu

- Key: 1
- Plain: abcdefghijklmnopqrstuvwxyz
- Cipher: bcdefghijklmnopqrstuvwxyza

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

Example #2

- Ciphertext: m lezi xli tewwasvh
- Plaintext: i have the password

- Key: 4
- Plain: abcdefghijklmnopqrstuvwxyz
- Cipher: efghijklmnopqrstuvwxyzabcd

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
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

RAIL FENCE CIPHER

The Rail Fence cypher is an easy transposition cypher that mixes the order of a plaintext. It also uses a key, making it harder to decrypt as one same message can be mixed in different ways depending on the key.

Its name comes from the patterns it forms on tables once its methods are applied in the encryption or decryption of a text. Since the text is written diagonally on successive rails of an imaginary fence.

R				**O**				**H**				**S**
	U		**T**		**T**		**E**		**E**		**L**	
		N				**H**				**E**		

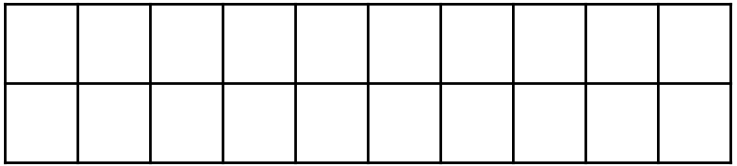
Key: 3

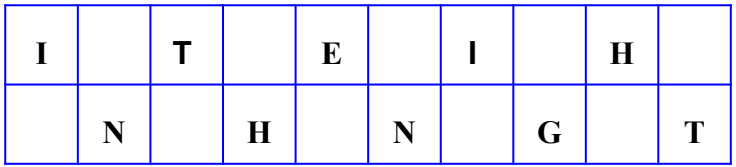
Plaintext: Run to the heels

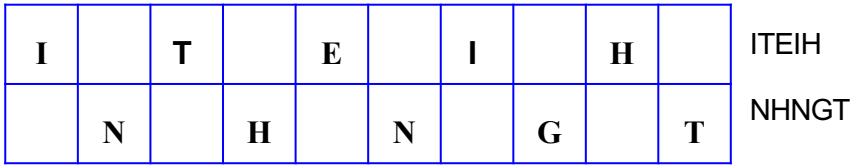
Ciphertext: rohsutteelnhe

Example #1

- Key: 2
- Plaintext: in the night
- Ciphertext: iteihnhngt







Example #2

- Key: 4
- Ciphertext: TEHDIDEOSECR
- Plaintext: THE CODE IS RED

*						*					
	*				*		*				*
		*		*				*		*	
			*						*		

T						E					
	H				D		I				D
		E		O				S		E	
			C						R		

POLYBIUS CIPHER

- The Polybius cipher is a substitution cipher that employs a 5x5 table containing the *key word*. The letters can't repeat, and they go in successive order after the key.
- To encrypt or decrypt substitute the letter for the value of the column and row.

	1	2	3	4	5
1	**L**	**A**	**P**	**T**	**O**
2	**B**	**C**	**D**	**E**	**F**
3	**G**	**H**	**I/J**	**K**	**M**
4	**N**	**Q**	**R**	**S**	**U**
5	**V**	**W**	**X**	**Y**	**Z**

Key: Laptop

Plaintext: Science

Ciphertext: 44 22 33 42 14 22 42

	1	2	3	4	5
1	**S**	**C**	**I/J**	**E**	**N**
2	**A**	**B**	**D**	**F**	**G**
3	**G**	**H**	**K**	**L**	**M**
4	**O**	**P**	**Q**	**R**	**T**
5	**U**	**V**	**W**	**Y**	**Z**

Example #1

- Key: saturday
- Plaintext: computer
- Ciphertext: 42 54 34 15 41 31 52 51

	1	2	3	4	5
1	S	A	T	U	R
2	D	Y			
3					
4					
5					

	1	2	3	4	5
1	S	A	T	U	R
2	D	Y	B	C	E
3	F	G	H	I/J	K
4	K	L	M	N	O
5	P	Q	V	W	Z

42	54	34	15	41	31	52	51
c	o	m	p	u	t	e	r

Example #2

- Key: internet
- Ciphertext: 52 54 31 54 51 41
- Plaintext: future

	1	2	3	4	5
1	I/J	N	T	E	R
2					
3					
4					
5					

	1	2	3	4	5
1	I/J	N	T	E	R
2	A	B	C	D	F
3	G	H	K	L	M
4	O	P	Q	S	U
5	V	W	X	Y	Z

52	54	31	54	51	41
f	u	t	u	r	e

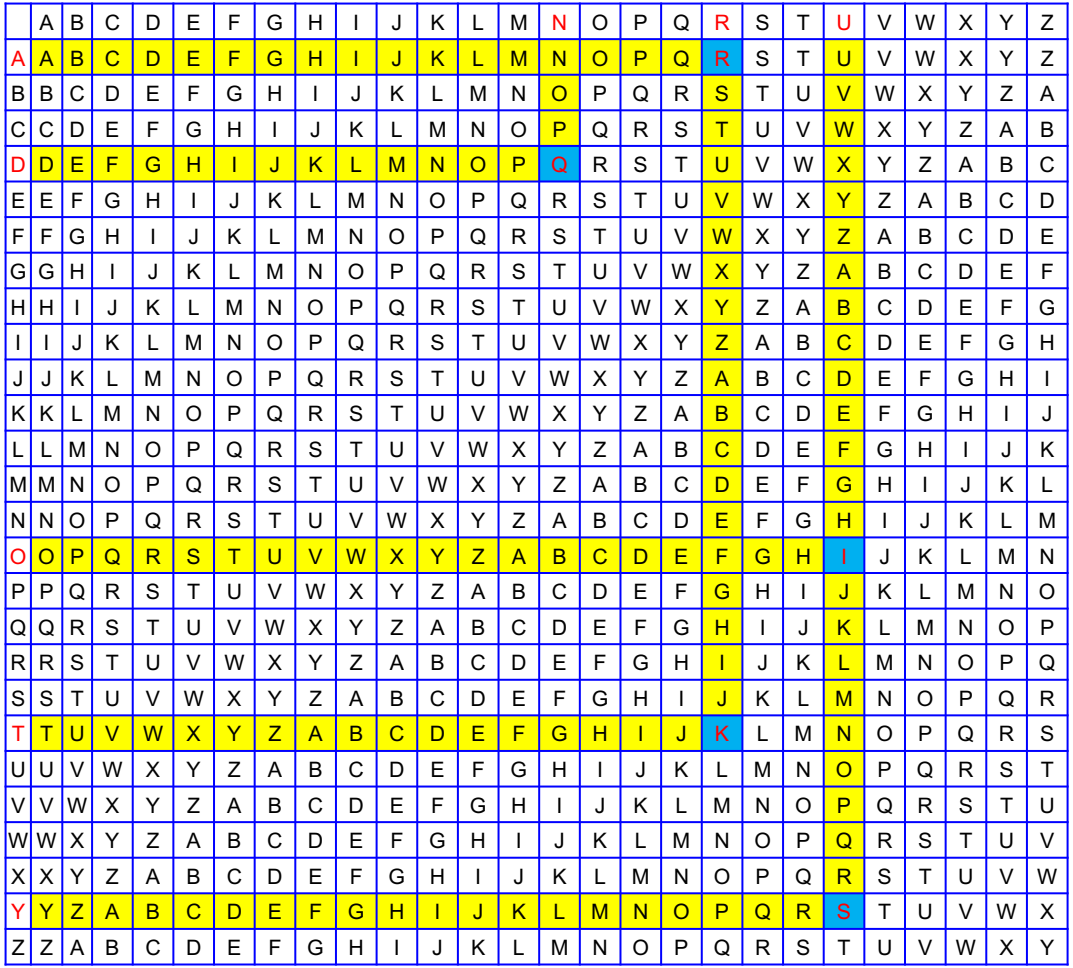
VIGENERE CIPHER

- The Vigenere cipher is a polyalphabetic substitution cipher.
- The top row of the Vigenere Square corresponds to the Key.
- While the outermost left column corresponds to the plaintext.
- The letter that connects the row and column is the ciphertext.

	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

VIGENERE CIPHER

Key: run
Plaintext: today
Ciphertext: kiqrs



PLAYFAIR CIPHER

- The Playfair cipher is a polygraphic substitution cipher that employs a 5x5 table (matrix) like the **Polybius** containing the *key word.*

C	O	M	P	U
T	E	R		

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

PLAYFAIR CIPHER

Plaintext **Ciphertext**

Same Column

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

G – M R – W

Same Row

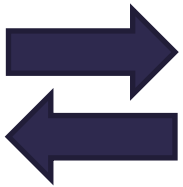
A	B	C	D	E
F	G	H	I/J	K
L	M	N	O	P
Q	R	S	T	U
V	W	X	Y	Z

B – C E – A

Different Row and Column

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 – C S – Q



PLAYFAIR CIPHER

Ciphertext **Plaintext**

Same Column

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

G – M W – R

Same Row

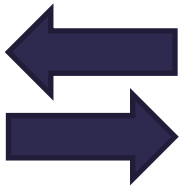
A	B	C	D	E
F	G	H	I/J	K
L	M	N	O	P
Q	R	S	T	U
V	W	X	Y	Z

C – B A – E

Different Row and Column

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

C – A Q – S



PLAYFAIR CIPHER