CLASSICAL CRYPTOGRAPHY

FOR TODAY...

01 CAESAR CIPHER

02 VIGENÈRE CIPHER

03 PLAYFAIR CIPHER

04 RAIL FENCE CIPHER

Content Curated by Pollux M. Rey

WHY DO WE NEED TO STUDY CLASSICAL CRYPTOGRAPHY?

Summary

Before the introduction of computers ushered in modern cryptography, breaking many codes was impossible using just pencil and paper. Although computing made many of the old, classical ciphers vulnerable to attack, they're still fun to learn about. Writing cryptanalysis programs that crack these ciphers is a great way to learn how to program.

In Chapter 1, we'll start with some basic cryptography tools to encrypt and decrypt messages without the aid of computers.

Let's get hacking.

WHY DO WE NEED TO STUDY CLASSICAL CRYPTOGRAPHY?

MAKING PAPER CRYPTOGRAPHY TOOLS

"The encryption genie is out of the bottle."
—Jan Koum, WhatsApp founder

Before we start writing cipher programs, let's look at the process of encrypting and decrypting with just pencil and paper. This will help you understand how ciphers work and the math that goes into producing their secret messages. In this chapter, you'll learn what we mean by cryptography and how codes are different from ciphers. Then you'll use a simple cipher called the Caesar cipher to encrypt and decrypt messages using paper and pencil.

01

CAESAR CIPHER

Content Curated by Pollux M. Rey

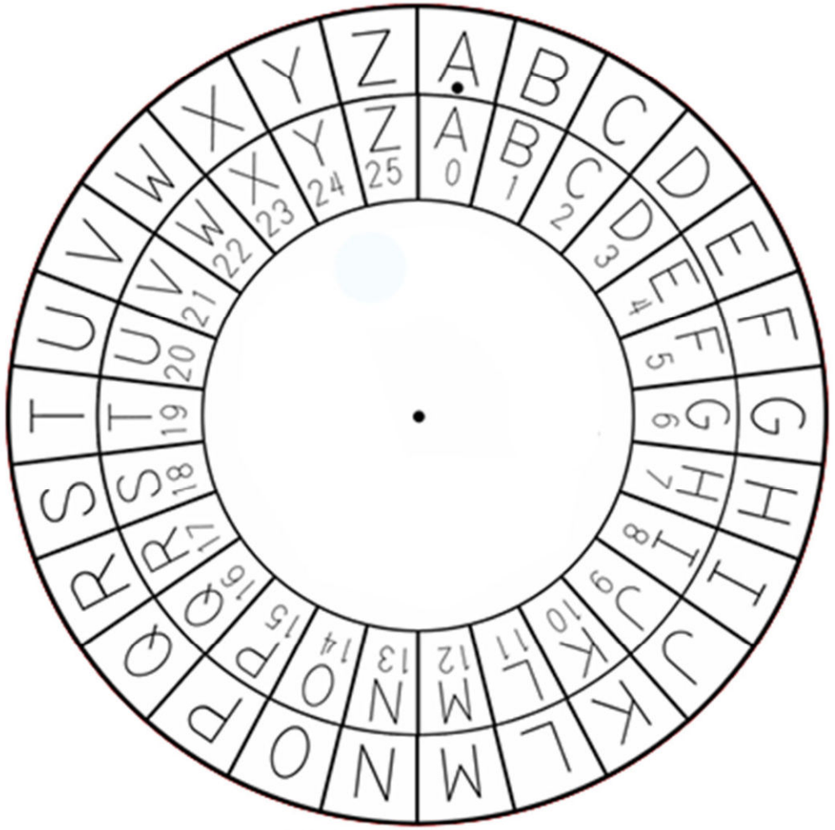
CAESAR CIPHER

- Named after **Julius Caesar** who used it 2000 years ago.
- He **shifted letters by three positions** in the alphabet to encrypt his messages.
- **Monoalphabetic substitution cipher**

Content Curated by Pollux M. Rey

Cracking Codes with Python, Al Sweigart

CAESAR CIPHER



Click wheel to rotate.

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	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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

CAESAR CIPHER

$$(p + k) \bmod n$$

Encryption Algorithm

https://crypto.interactive-maths.com/caesar-shift-cipher.html

CAESAR CIPHER

$$(c - k) \bmod n$$

Decryption Algorithm

CAESAR CIPHER

$$(c - k) \bmod n$$

Decryption Algorithm

https://crypto.interactive-maths.com/caesar-shift-cipher.html

MODULO

The **remainder** after dividing one number by another.

https://www.mathsisfun.com/numbers/modulo.html

MODULO

What is **100 mod 9**?

What is $-100 \bmod 9$?

CAESAR CIPHER

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

CAESAR CIPHER

$$(p + k) \bmod n$$

Encryption Algorithm

CAESAR CIPHER

$$(p + k) \bmod 26$$

Encryption Algorithm

CAESAR CIPHER

$$(c - k) \bmod 26$$

Decryption Algorithm

CAESAR CIPHER

Encrypt
"HELLO WORLD"
using the **first letter of your name** as the key.

CAESAR CIPHER

Decrypt
"**MKOCKB**"
using "L" as the key.

02

VIGENÈRE CIPHER

Content Curated by Pollux M. Rey

VIGENÈRE CIPHER

- Named after the French diplomat **Blaise de Vigenère.**
- First described in **1553**.
- Known as the "indecipherable cipher," it remained unbroken until Charles Babbage broke it in the **19th century.**

Content Curated by Pollux M. Rey

Cracking Codes with Python, Al Sweigart

VIGENÈRE CIPHER

- Polyalphabetic substitution cipher

Content Curated by Pollux M. Rey

Cracking Codes with Python, Al Sweigart

VIGENÈRE CIPHER

The Vigenère key is a **series of letters, such as a single English word,** that is **split into multiple single-letter subkeys** that encrypt letters in the plaintext.

Cracking Codes with Python, Al Sweigart

VIGENÈRE CIPHER

Using the Vigenère cipher is the same as using **multiple Caesar ciphers.**

VIGENÈRE CIPHER

Instead of encrypting the whole plaintext with one Caesar cipher, we **apply a different Caesar cipher to each letter of the plaintext.**

VIGENÈRE CIPHER

Encrypt
"HELLO WORLD"
using the **"CICS"** as the key.

Cracking Codes with Python, Al Sweigart

VIGENÈRE CIPHER

Decrypt
"EZAHVWIJCXJQ"
using **"CICS"** as the key.

03

PLAYFAIR CIPHER

Content Curated by Pollux M. Rey

PLAYFAIR CIPHER

- Named after **Lord Playfair**, who heavily promoted the use of the cipher to the military.
- **Digraph Substitution Cipher**

Content Curated by Pollux M. Rey

Cracking Codes with Python, Al Sweigart

PLAYFAIR CIPHER

Encrypt
"HELLO WORLD"
using **"PLAYFAIR"**
as the key.

Cracking Codes with Python, Al Sweigart

PLAYFAIR CIPHER

Generate a Polybius square

1. Create an empty 5x5 grid.
2. Write the letters of the key in the grid, row by row, skipping any repeated letters.
3. Treat "I" and "J" as the same letter.
4. Fill the rest of the grid with the remaining unused letters of the alphabet, in order.

PLAYFAIR CIPHER

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

PLAYFAIR CIPHER

Split the plaintext up into digraphs

1. If the digraph has the same letter twice (or one letter remains at the end), insert "X" between them or at the end, then proceed.
2. If the letters are in the same row, replace each with the one to its right (wrap around if needed).
3. If the letters are in the same column, replace each with the one below it (wrap around if needed).
4. If neither, form a rectangle with the letters as opposite corners, and replace each with the letter in the same row at the other corner.

PLAYFAIR CIPHER

HELLO WORLD

PLAYFAIR CIPHER

HE LL OW OR LD

PLAYFAIR CIPHER

HE LL OW OR LD

PLAYFAIR CIPHER

HE LX LO WO RL D

PLAYFAIR CIPHER

HE LX LO WO RL D

PLAYFAIR CIPHER

HE LX LO WO RL DX

PLAYFAIR CIPHER

HE LX LO WO RL DX

PLAYFAIR CIPHER

HE LX LO WO RL DX

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

PLAYFAIR CIPHER

KG YV RV VQ GR CZ

PLAYFAIR CIPHER

Encrypt **"BALLOON"**
using **"NETWORKING"**
as the key.

PLAYFAIR CIPHER

Decrypt "**BALLOON**" using "**NETWORKING**" as the key.

04

RAIL FENCE CIPHER

Content Curated by Pollux M. Rey

RAIL FENCE CIPHER

- **Transposition cipher**
- Also known as **Zigzag cipher.**

Content Curated by Pollux M. Rey

https://crypto.interactive-maths.com/rail-fence-cipher.html

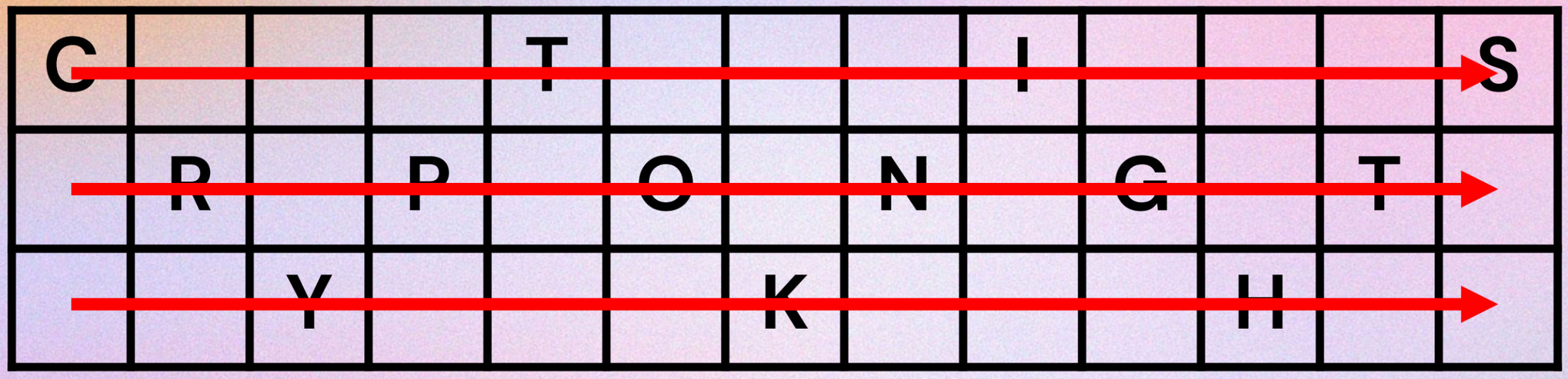
RAIL FENCE CIPHER

Encrypt "**CRYPTOKNIGHTS**" using **4** as the key.

RAIL FENCE CIPHER

C				T				I				S
	R		P		O		N		G		T	
		Y				K				H		

RAIL FENCE CIPHER



RAIL FENCE CIPHER

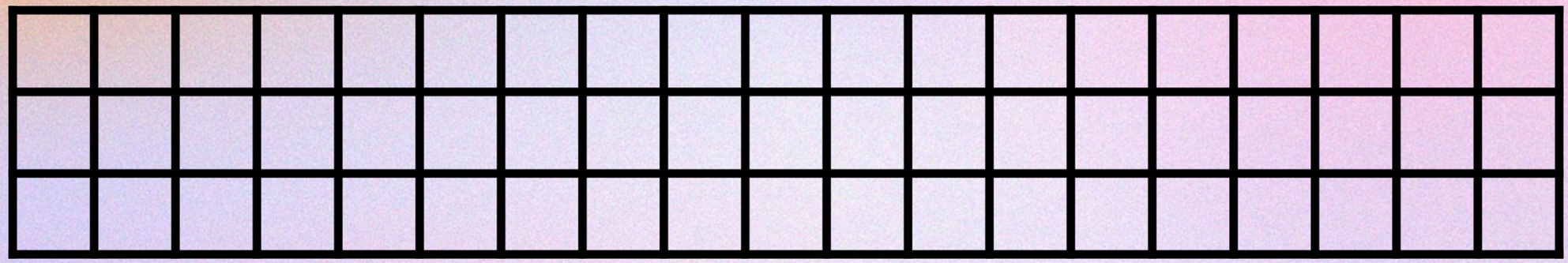
Ciphertext:

CTISRPONGTYKH

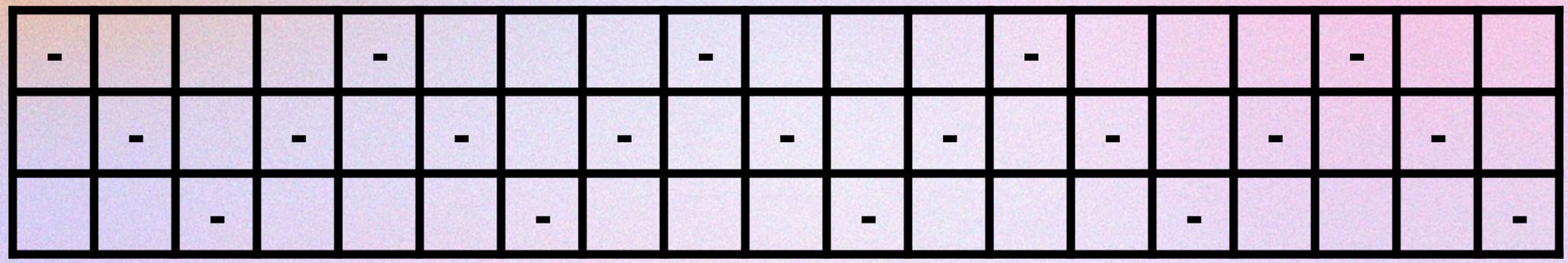
RAIL FENCE CIPHER

Decrypt
"DNETLEEDHESWLXFTAAX"
using **3** as the key.

RAIL FENCE CIPHER



RAIL FENCE CIPHER



RAIL FENCE CIPHER

D				N				E				T				L		
	E		E		D		H		E		S		W		L		X	
		F				T				A				A				X

RAIL FENCE CIPHER

Plaintext:

DEFEND THE EAST WALL XX

RAIL FENCE CIPHER

Plaintext:

DEFEND THE EAST WALL

ACTIVITY

1. Decrypt **"IIVDVRTOUT"** using **"HACK"** as the key with **Vigenère cipher.**
2. Decrypt **"IPSYYTSWWMOS"** using **"HACK"** as the key with **Playfair cipher.**
3. Decrypt **"IAENMTTCFRINHOO"** using **4** as the key with **Rail Fence cipher.**

THANK YOU!

Content Curated by Pollux M. Rey