Classic Ciphers

CЯ4CK1NG-THΞ-C0D3

Today’s Roadmap

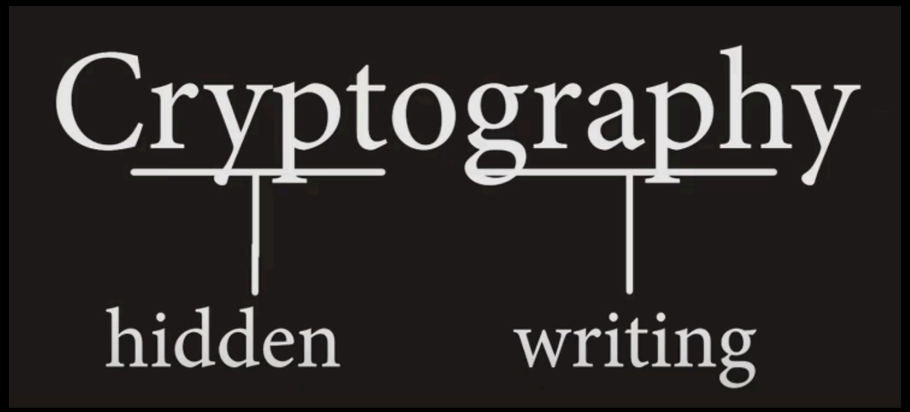
- History of Cryptography: Caesar ➜ Enigma ➜ RSA
- CIA Triad: Confidentiality • Integrity • Availability
- Hands-on with Classical Ciphers (Caesar, Vigenère, ROT13)

What is cryptography?

- The modern study of cryptography investigates techniques for facilitating interactions between distrustful entities.
- In this course we introduce some of the fundamental concepts of this study.
- We will Emphasise on the foundations of cryptography and in particular on precise definitions and techniques deployed for the same

Lets define cryptography

“Cryptography is the art of private communication in a public environment”



Note:
That definition leaves out the word “encryption.”
Some cryptographic techniques merely conceal the message without actually converting it into ciphertext.

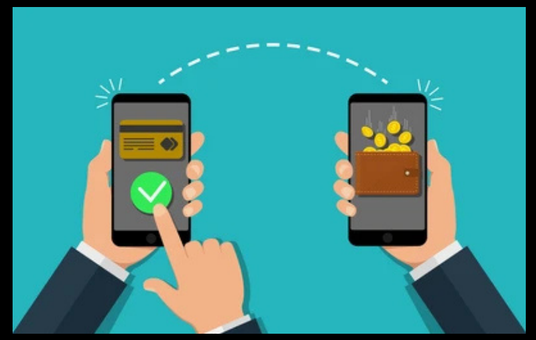
History of cryptography

- In the past, cryptography’s main purpose was to keep messages private.
- People have been using forms of encryption for millennia—Egyptian scribes, for example, hid messages in hieroglyphs, and many other ancient cultures developed their own secret methods.
- Today, cryptography goes far beyond secrecy: it secures authentication, verifies data integrity, enables digital signatures, powers online gambling, supports cryptocurrencies like Bitcoin, and more.

Applications

Encryption/Decryption in email

Electronic Money



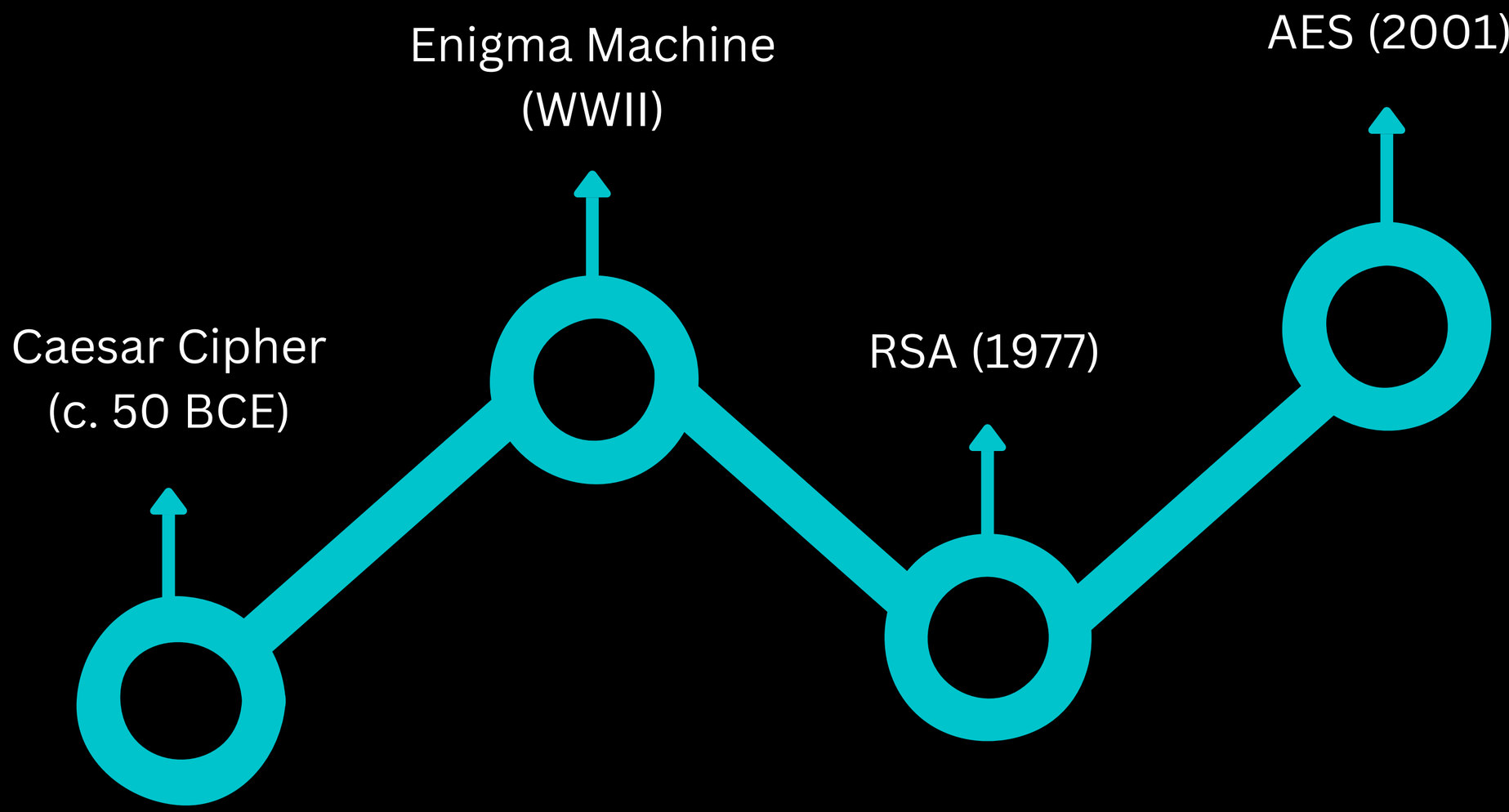
Encryption in WhatsApp

Sim card Authentication

The CIA Triad - Core Security Principles

- ☞ Confidentiality - Data Confidentiality and Privacy
- ☞ Integrity - Data Integrity and System Integrity
- ☞ Availability

A Quick Timeline of Encryption

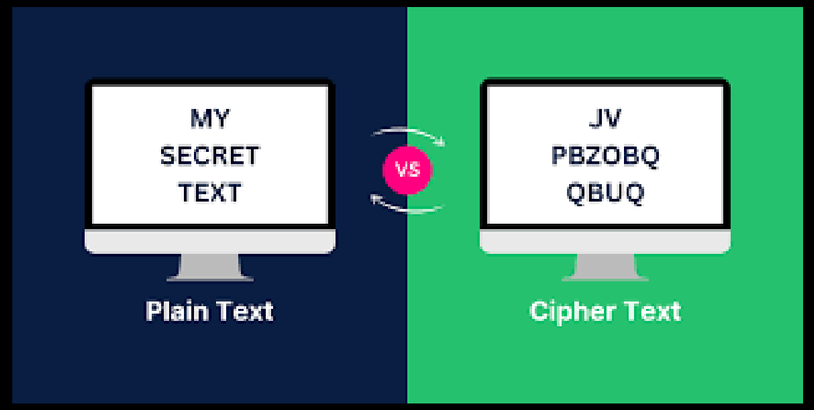


Basic Terminologies

Plaintext vs. Ciphertext

• Plaintext (or Cleartext): The original, human-readable message.

• Ciphertext: The encrypted, non-human-readable form of the message.



Encryption (Encipherment)

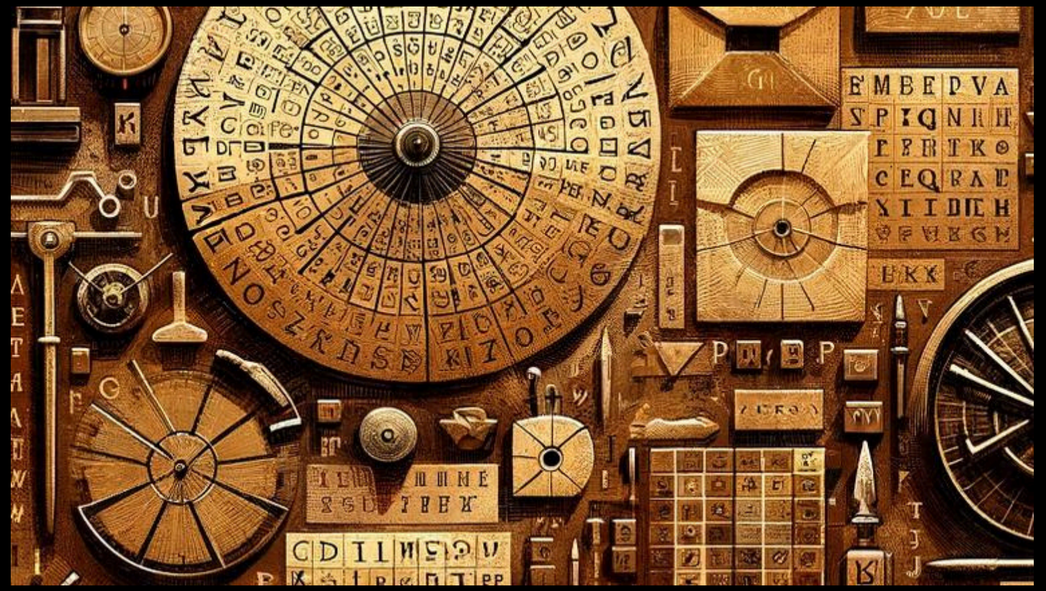
• The process of converting plaintext into ciphertext so that it cannot be understood without the key.

Decryption (Decipherment)

• The process of converting ciphertext back into its original plaintext form, restoring readability.

Classical Ciphers

- The classical algorithms are those invented pre-computer up until around the 1950's - Mainly:
  - Substitution ciphers
  - Transposition cipher
  - Combined



Substitution Ciphers

- Three types:
  - Monoalphabetic cipher
  - Polyalphabetic cipher
  - Polygraphic cipher
- An example of it is Caesar Cipher

1. Letter Coding

If SUN is written as RTO, how is MOON written?

a) LPPM

b) NQPP

c) LNNM

d) LOPP

2. Substitution Puzzle

If rose is called lily, lily is called tulip, tulip is called jasmine, and jasmine is called orchid, which flower is known as the queen of flowers?


The Caesar cipher | Journey into cryptography | Computer Science | Khan Acade...
Copy link
The
Caesar cipher
Khan Academy
Watch on YouTube

The Caesar Cipher

- Origin: The Caesar cipher is one of the oldest known encryption methods, dating back over 2,000 years.
- Inventor: Named after Julius Caesar, who used it to secure military communications.
- Method: It is a substitution cipher where each letter in the message is shifted by a fixed number of positions in the alphabet.
- Purpose: Allowed Caesar to send secret orders that only recipients who knew the shift could decode.

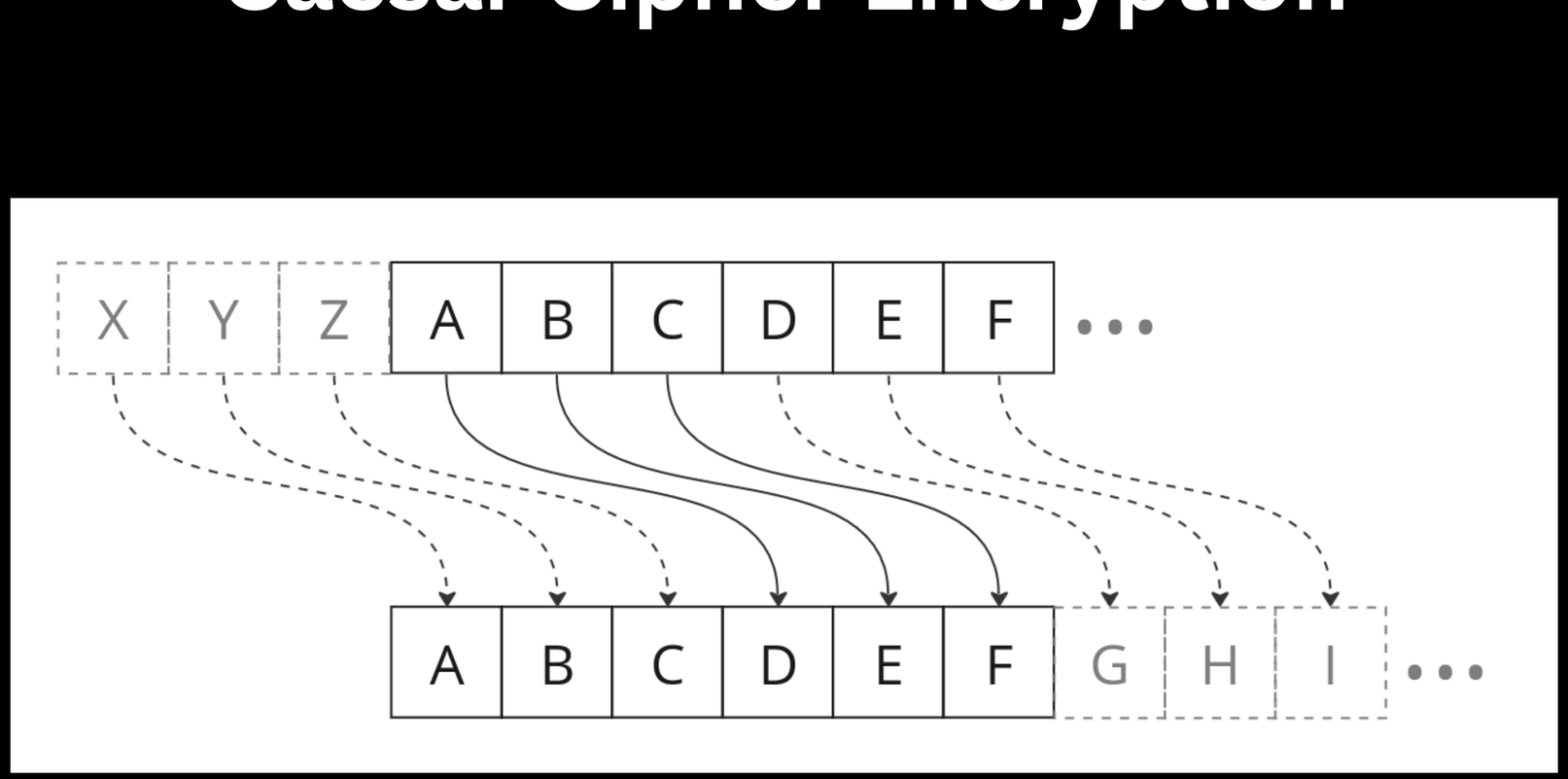
Ceasar Cipher Wheel

- A Caesar cipher wheel is a circular disk with two concentric alphabets - one fixed (outer ring) and one movable (inner ring).

- Outer Wheel: Contains the normal alphabet A–Z in order.
- Inner Wheel: Also has A–Z but can be rotated to set the shift key.

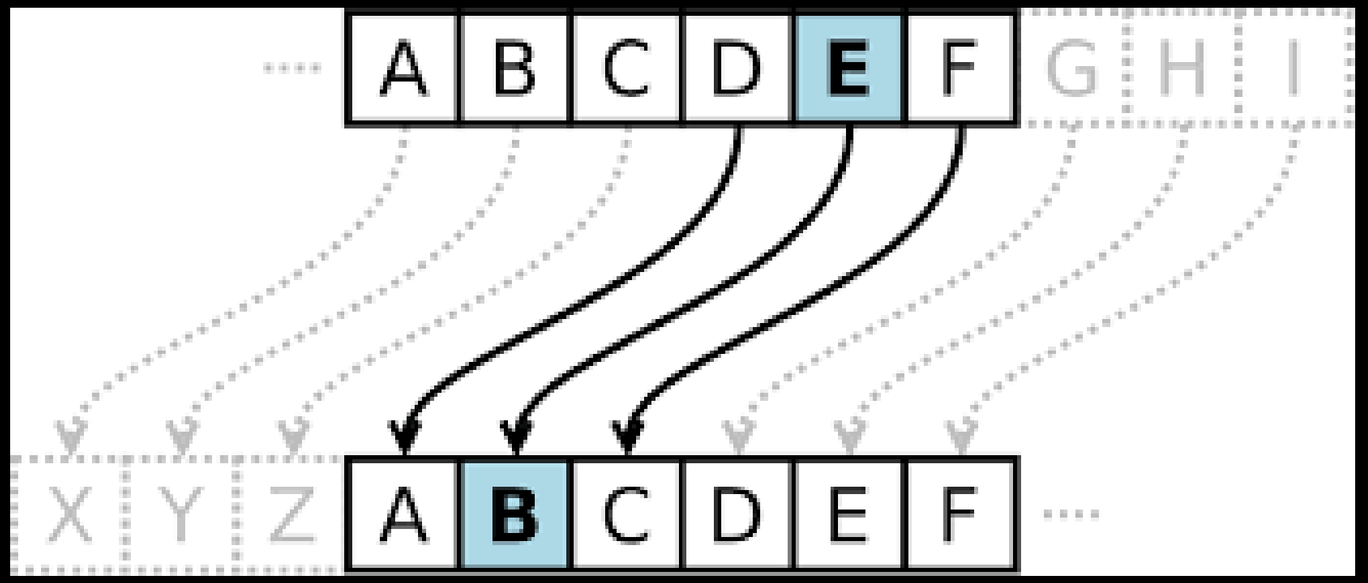
- The wheel provides a quick, visual way to encode and decode messages without doing mental arithmetic for each letter.

Caesar Cipher Encryption



Here K=3 (Shift Key)

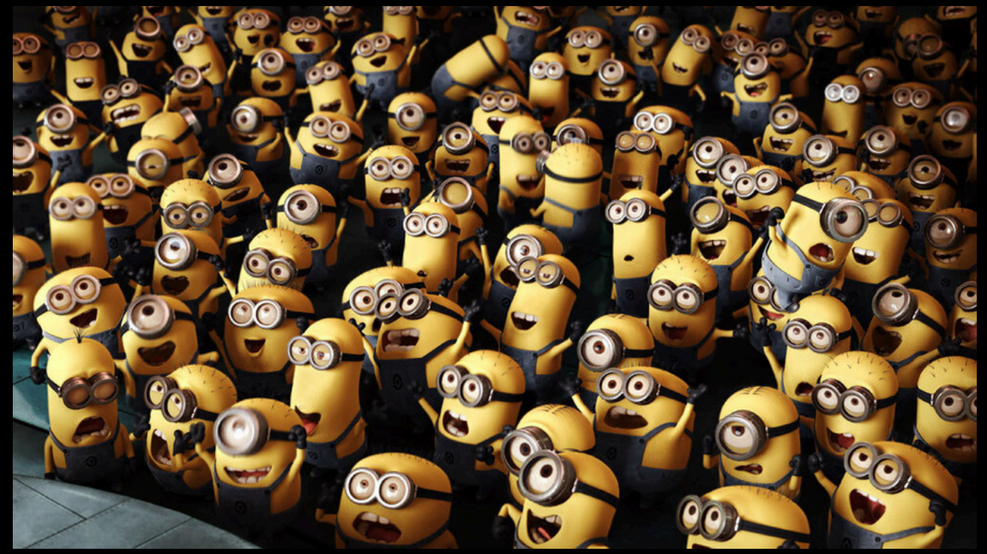
Caesar Cipher Decryption



Here K=3 (Shift Key)

Question

- Use the Caesar cipher with shift of 3 to encrypt the message:
- “WE STEAL THE MOON”



Question

- Decrypt the message GFSFSF KZS YNRJ if it was encrypted using a shift cipher with shift of 5

Think about it

Suppose you intercept a message, and you know the sender is using a Caesar cipher, but do not know the shift being used. The message begins EQZP.

How hard would it be to decrypt this message?

Hint: Can you bruteforce it?

Think about it

Shift	Message	Shift	Message	Shift	Message	Shift	Message
1	DPYO	7	XJSI	13	RDMC	19	LXGW
2	COXN	8	WIRH	14	QCLB	20	KWFV
3	BNWM	9	VHQG	15	PBKA	21	JVEU
4	AMVL	10	UGPF	16	OAJZ	22	IUDT
5	ZLUK	11	TFOE	17	NZIY	23	HTCS
6	YKTJ	**12**	**SEND**	18	MYHX	24	GSBR
						25	FRAQ

The Vinegar Cipher

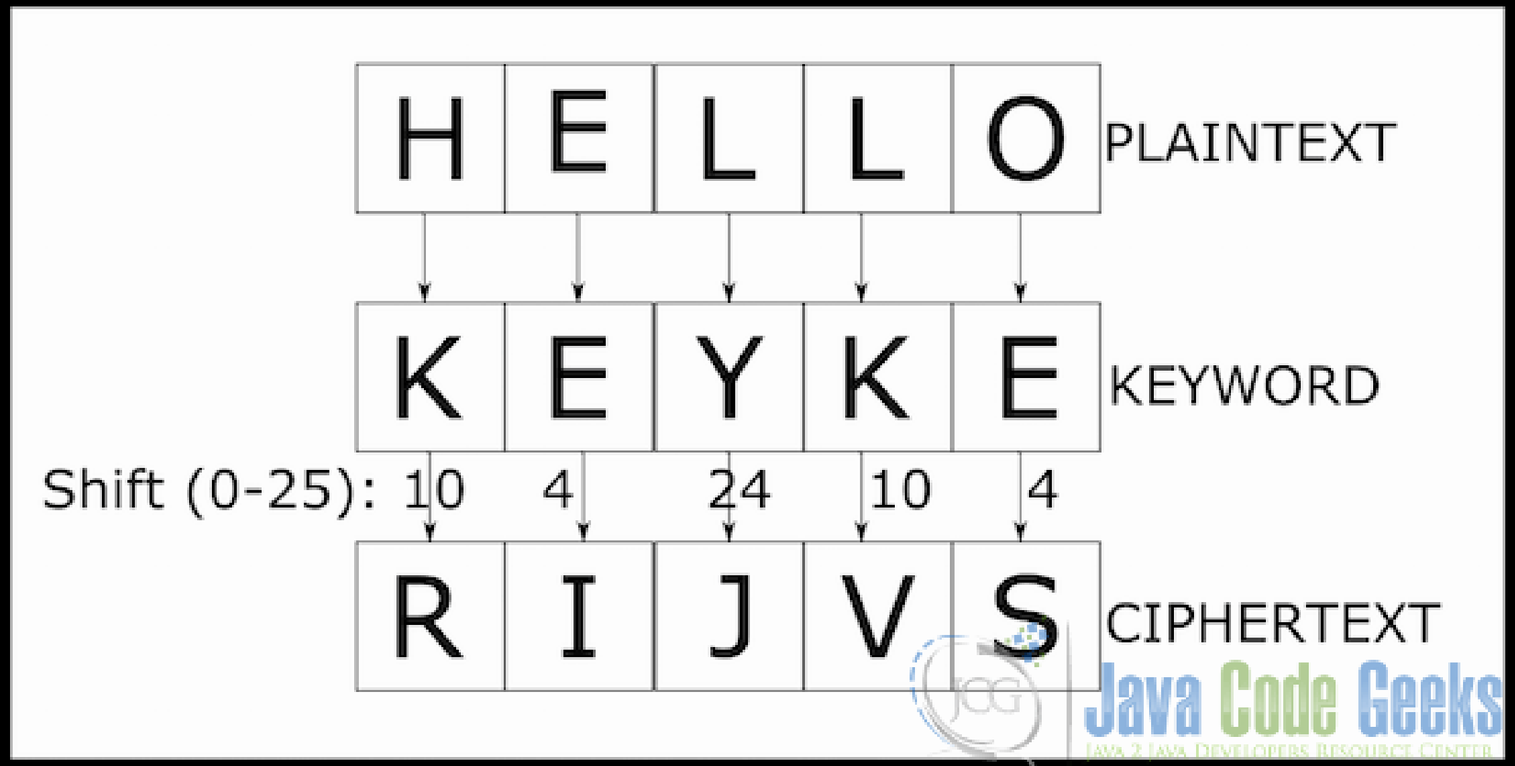
.....

commonly mistaken and thought of-

The Vigenere Cipher

- Origin: A historic encryption method, first described in the 16th century.
- Inventor: Blaise de Vigenère, who created it as a stronger alternative to simple substitution ciphers.
- Method: A polyalphabetic substitution cipher where each letter is shifted based on a repeating key word or phrase instead of a fixed number.
- Purpose: Enables messages to be encrypted with varying shifts, making it harder for unauthorized recipients to decode without the key.

Vigenere Cipher Encryption



Here K is different for each character

Note: Alphabets are always 0 indexed

Question

- Message: "MINIONS LOVE BANANAS"
- Keyword: "YELLOW"
- Task: Encrypt the message using the Vigenère cipher.

Hands on for implementing the same

Read carefully:

Among the endless symbols a secret lies,
digits of earth and sky disguise.
In the poster’s maze where @’s and &’s roam,
seek the numbers that point you home.
Two parts—north and west—form a pair;
enter them together and the flag waits there.

The poster you’ve been seeing all this while is not just art—it’s a cipher.
Find the numbers hidden inside, piece them into coordinates, and enter them on our website.