TEACHENGINEERING.ORG

Cybersecurity

Encryption Using Shift Ciphers

U.S. National Science Foundation

Engineering & Applied Science
UNIVERSITY OF COLORADO BOULDER

Pre-Assessment

Please complete the pre-assessment questions.

Warm-Up

🧩 Try it: Decode this message:

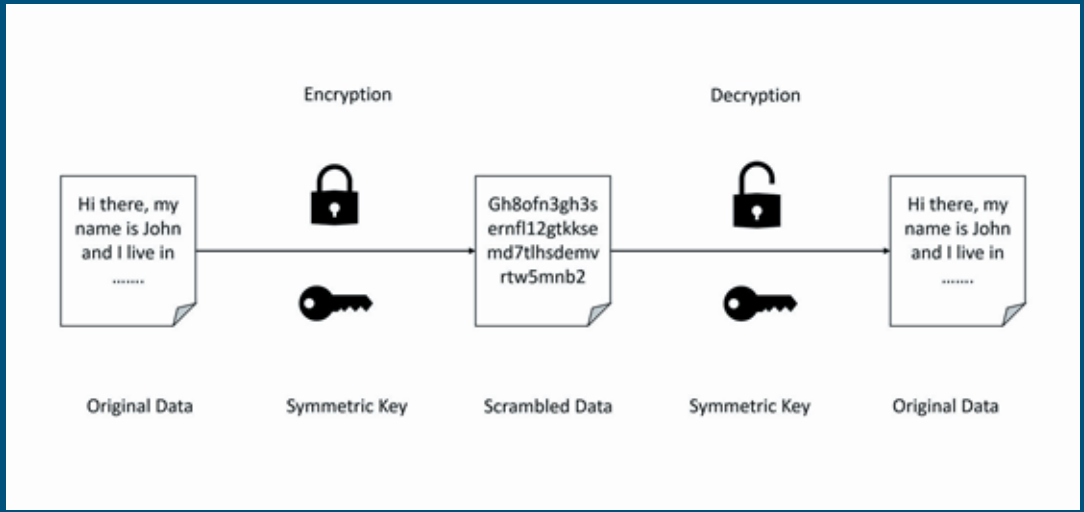
Wklv lv d whvw phvvdjh.

Discussion:

- What do you think is happening here?
- Have you ever tried to keep a message secret?
- What does the word ‘encryption’ mean to you?

What Is Encryption?

The encoding of information to make it unreadable



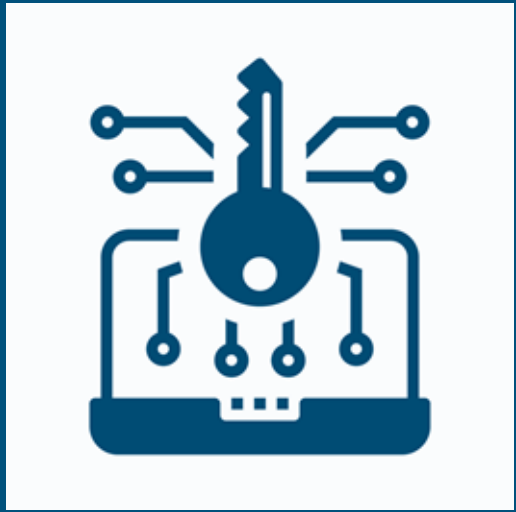
What Is Cryptography?

A technique that transforms data and prevents it from being read.

Uses algorithms to encode information.

Examples:

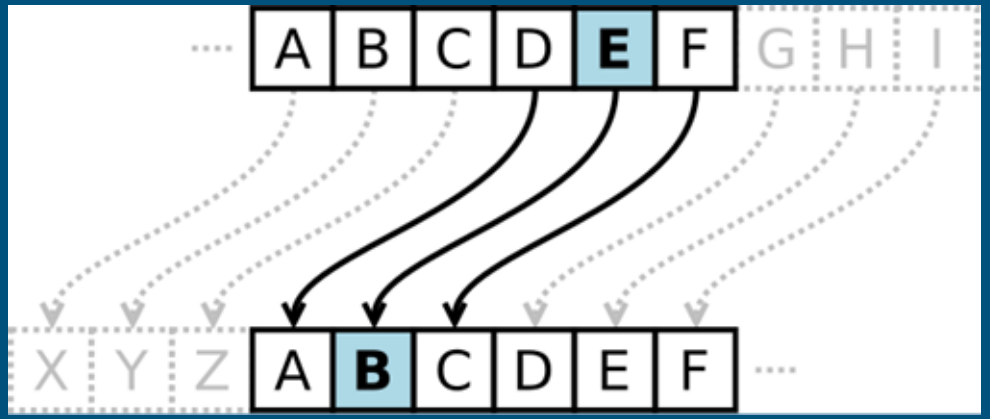
- Digital signatures
- Block ciphers
- Random bit generation
- Caesar ciphers



What Is a Caesar Cipher?

Caesar cipher: a substitution cipher where each letter is shifted a fixed number of spaces.

A simple example:
D→ A (shift of -3), E → B, etc.



Fun Fact!

Caesar Cipher

Caesar ciphers were used 2,000 years ago as a way to protect information throughout the Roman Empire from enemy spies.

Caesar Cipher!

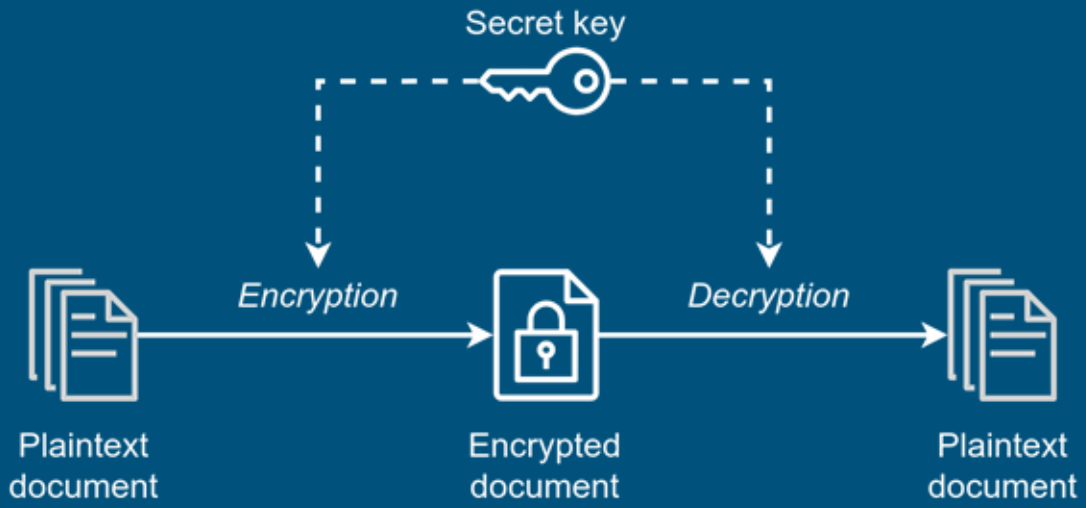
At the peak of the Roman Empire's power,the civilization was often at war with other empires. Spies, enemy soldiers, and thieves would often try to intercept messages from messengers. To keep anyone from discovering top secret information, it was often the practice of military leaders to encode messages using a cipher. This cipher was also known as a shift cipher. The person to whom the message was sent would use a special tool to decipher the message and read what it had to say.

Jura lbh jvfu hcba n fgne Znxrf ab qvssrerapr jub lbh ner

Nalguvat lbhe urneg qrfverf Jvyy pbzr gb lbh

Symmetric Encryption

- Symmetric encryption uses a single key.
- Less secure , but more efficient.



Asymmetric Encryption

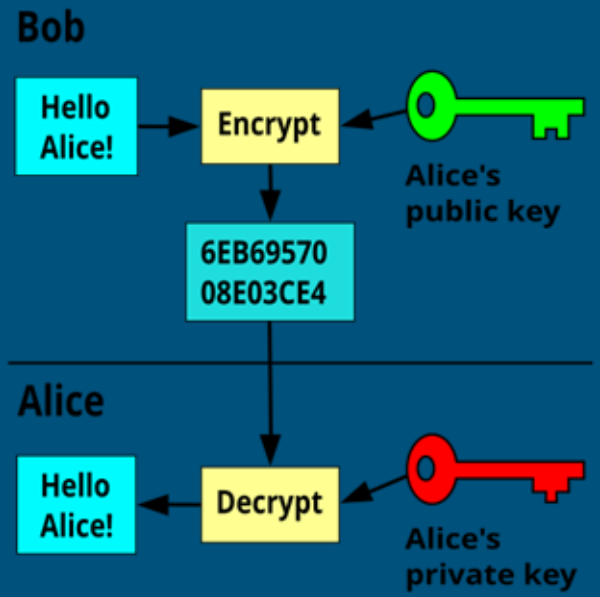
Asymmetric encryption uses two keys—a public key and a private key—to encrypt and decrypt data

Public Key

Shared openly

Encrypts data

Verifies digital signatures



Private Key

Never shared

Decrypts data

Creates digital signatures

Hands-On Activities

Activity 1: Create Your own decoder wheel or shift chart using blank handouts.

Activity 2: Encode your name or a short phrase using a Caesar shift of your choice. Exchange encrypted messages with a classmate and decode each other's messages.

Activity 3: Decrypt encoded messages in the Encoding/Decoding Practice Sheet.

How Does This Relate to Cybersecurity

Discussion Questions:
Why is encryption important today?
How is Caesar's idea still used in modern technology?

<Think-Pair-Share> - Discuss ideas (10 mins)

Simple ciphers are not very secure.
They lay the foundation for stronger algorithms.
Modern encryption: HTTPS, end-to-end encryption, etc.

Digital Extension

Caesar Cipher

Use an online Caesar cipher tool to try encrypting and decrypting messages faster.
https://www.dcode.fr/caesar-cipher

Challenge: Try brute-forcing a Caesar cipher by checking all 25 possible shifts.

Symmetric and Asymmetric Keys

Go to: https://www.kerryveenstra.com/cryptosystem.html

Post-Assessment

Please complete the post-assessment.

 Assessment / Exit Ticket:

- Encode this sentence with a Caesar cipher using shift 5:
  “Cybersecurity is important.”

- Write 1–2 sentences explaining why encryption matters in cybersecurity.

References

https://www.ibm.com/think/topics/cryptography

https://www.ibm.com/think/topics/asymmetric-encryption

https://www.ibm.com/think/topics/symmetric-encryption

https://www.ibm.com/docs/en/sia?topic=osdc-private-keys-public-keys-digital-certificates-27