CRYPTOGRAPHY

By Anika, Christina, and Michelle

About Cryptography

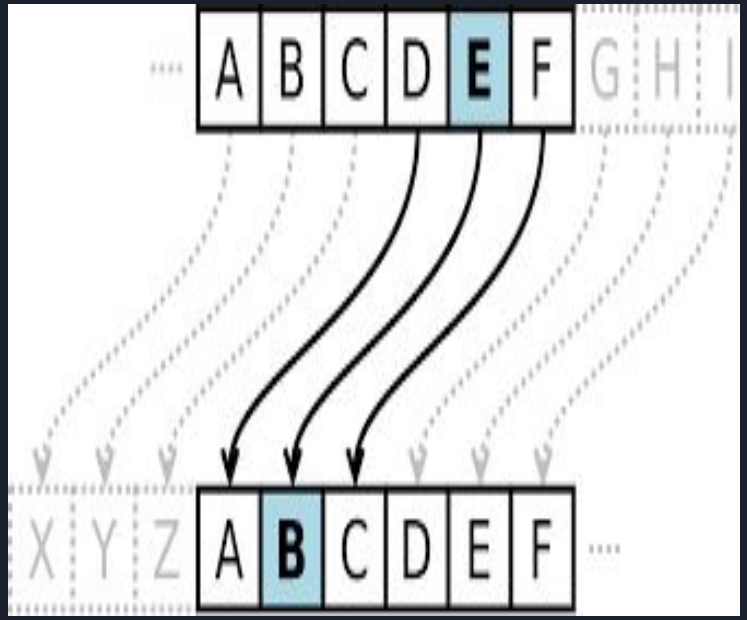
- Cryptography is the science of protecting information by transforming it into a secure format.
- Today, cryptography is used to protect digital data.
- It is a part of computer science that focuses on transforming data into formats that cannot be recognized by unauthorized users.

Basic Vocab

- Cryptography- the art of writing or solving codes
- Code- a system of words, letter, figures, or other symbols substituted for other words, letters, etc., for the purposes of secrecy
- Cipher- and method of encrypting text
- Plaintext- the message being shared, text as it is normally written
- Ciphertext- text that has been enciphered to prevent others from reading it
- Encode- to put a message into the form of code so that it can be kept as a secret
- Decode- to translate data or a message from code into the original language or form
- Encipher- to convert a message or a piece of text into coded form; encrypt
- Decipher- To convert a text written in code, or a coded signal, into normal language

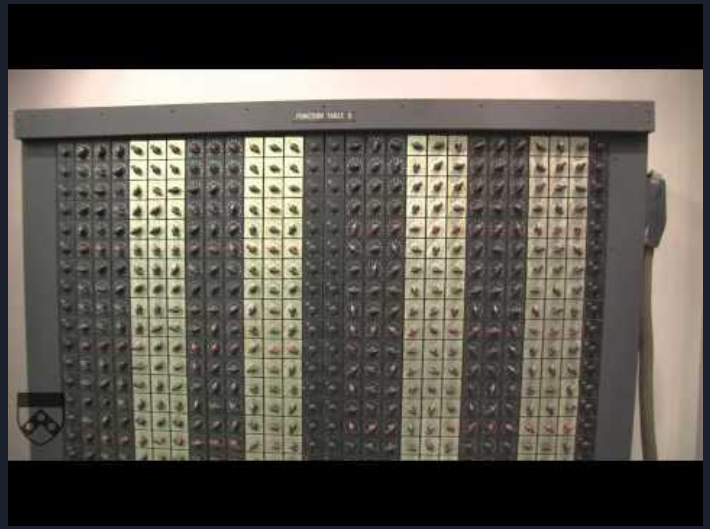
Classical Cryptography (cypher)

- In cryptography, a classical cipher is a type of cipher that was used historically but now has fallen, because of modern technology.
- In contrast to modern cryptographic algorithms, most classical ciphers can be practically computed and solved by hand.
- It is also known as Caesar cipher.



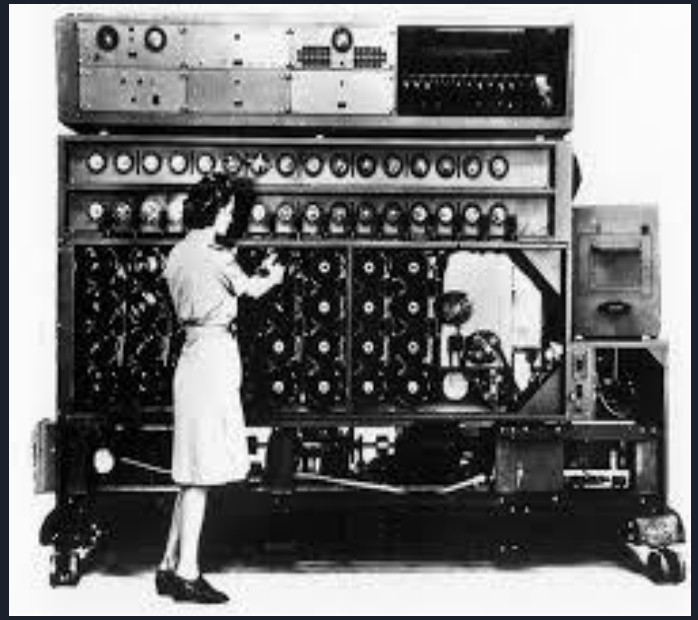
The Computer Era

- “Computers allowed for encryption of any kind of data representable in any binary format, unlike classical ciphers which only encrypted written language texts, this was new and significant.”
- The use of a quality cipher is very efficient (fast and requiring few resources, such as memory or CPU capability)
- Breaking this coding needs a great amount of effort, and much greater than that required to break a classical cipher
- What does CPU stand for?



Cryptography during World War II

- By World War II mechanical and electromechanical cryptographic cipher machines were in wide use.
- The Enigma machine is an encryption device developed and used in the early- to mid-20th century to protect commercial
- The most important codebreaking event of the war was the successful decryption by the Allies of the German "Enigma" Cipher.



Modern/Current Cryptography

- The first known evidence of cryptography can be traced to the use of 'hieroglyph' - a character of the ancient Egyptian writing system.
- Modern Cryptography - is used to provide secrecy and integrity to our data by mathematical equations.

Cryptography + Cyber Security

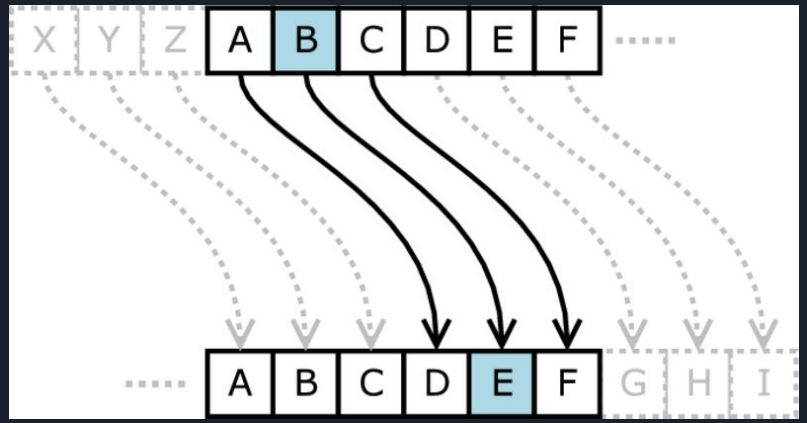
- ATM cards, computer passwords, electronic commerce, etc. all use cryptography for security
- Aspects in information security include data confidentiality, data integrity, authentication, etc.

Cryptography + Cyber Security (continued)

- Specific security requirements include authentication, authorization, confidentiality, integrity, and non-repudiation
  - Authentication/Identification- the process of verifying the identity of a user or process
  - Authorization - protects critical resources in a system by limiting access only to authorized users and their applications.
  - Confidentiality - ensures that no one but the intended receiver can read the message.
  - Integrity - assures that the intended receiver that the original message has not been changed in any way when it is received.
  - Non-repudiation - a mechanism that proves that the sender really sent the message.

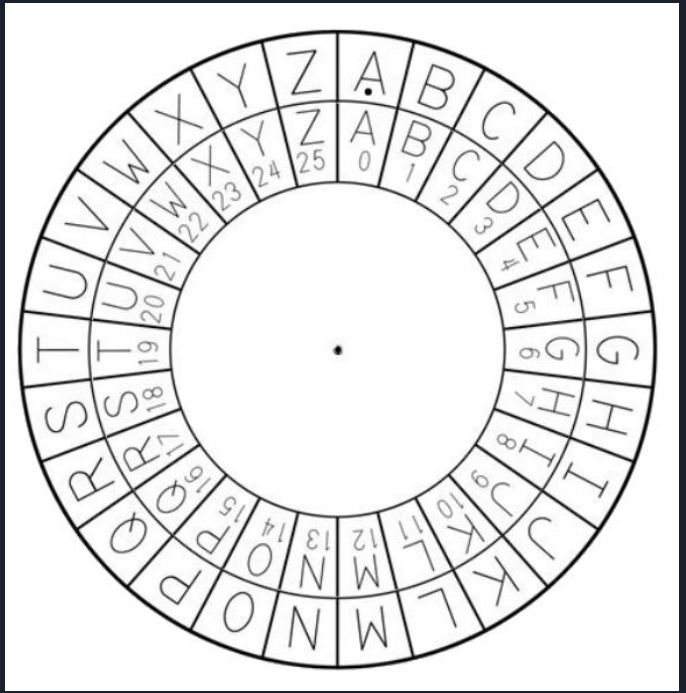
Caesar Cipher

- Also known as a shift cipher, Caesar's Code, or Caesar Shift
- Named after Julius Caesar, who used this method for secret military communications.
- This cipher substitutes each letter for another using displacement
- There are only 25 possible encryptions
- Was effective back then because many people were illiterate.



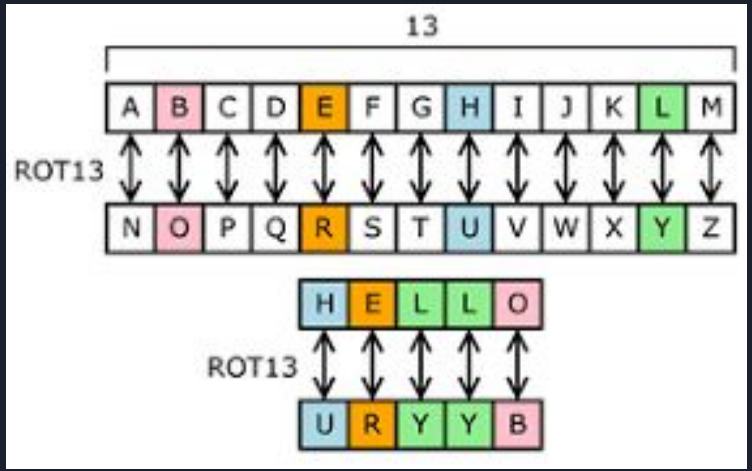
Caesar Cipher Practice

- Shifts in Caesar Cipher- How many letters or times were shifted to the left by moving the inner circle
- What is “A” with a shift of 10?
- What is “J” with the shift of K?
- What is “ARTEMIS” with a shift of 6?



Substitution Cipher

- More complex that the Caesar Cipher
- Each letter in the alphabet can be matched to any other letter
  - No pattern to mapping
- Best way to crack these code would be using frequency analysis
  - frequency analysis- the study of the frequency of letters or groups of letters in a ciphertext
  - In English, the letters E, T, and A are the most common while the letters Z and Q are the least common



Alan Turing

"The Imitation Game" The movie on how Alan Turing cracked the Enigma Code! (not free)

About Alan Turing

- Alan Turing credited as the father of computer science
- He was a British scientist and a pioneer in computer science.
- During World War II, he developed a machine that helped break the German Enigma code.
- He also laid the groundwork for modern computing and theorized about artificial intelligence.

The Enigma Code

- This was the code used in German naval communications, which were thought to be virtually unbreakable
- Turing cracked the system and regular decryption of German messages began in mid-1941.
- “To maintain progress on code-breaking, Turing introduced the use of electronic technology to gain higher speeds of mechanical working.”
- Turing became an valuable person Allies, successfully decoding many of Germany’s messages.

The Turing Test

- Alan Turing was also into philosophy he would debate over if computers could think like humans
- He created a test called the Turing test to answer the question. He reasoned that if a computer acted, reacted, and interacted like a sentient being, then it was sentient.
- In this simple test, an interrogator in isolation asks questions of another person and a computer. The questioner then must distinguish between the human and the computer-based on their replies to his questions.
- If the computer can "fool" the interrogator, it is intelligent. Today, the Turing Test is at the heart of discussions about artificial intelligence.

Fun Facts!!

The oldest encryption attempt known to mankind dates back to the kingdom of Egypt, around two thousand years before Christ. The ciphers are found on the tomb of Khnumhotep II. They may have been, however, a joke or an attempt to create a mystic atmosphere.

Julius Caesar used encryption in the days of the Roman Empire to cipher letters and messages. Generally, encryption played an important role in many wars and in military circles throughout the years.

The very word cryptography has Greek origins. “Kryptos” means hidden and “Graphein” – word.

PRACTICE!!

Online Caesar Cipher Link!!

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

What is I LOVE ICE CREAM with a shift of 4?

[redacted]

Decode NBSI JT GVO with a shift of 1 ?

[redacted]

What is ARTEMIS using the encoding alphabet above?

[redacted]

What is QUINOA?

[redacted]

What is SORBET?

[redacted]

SCOURCES

- Artemis Cryptography Presentation
- Google (definitions)
- IBM (cyber security)
- cs.mcgill.ca (caesar cipher)
- dcode.fr (substitution cipher)
- Wikipedia Cryptography
- About The Imitation Game
- Alan Turing