ASSIGNMENT-2

[CRYPTOGRAPHY & CYBERSECURITY]

SUBMITTED TO:

Ms. SONA MARIA SEBASTIAN

SUBMITTED BY:

ADHILA ISMAIL

INTMCA S9

Course Documentation on Introduction to Cryptography

Cryptography plays a crucial role in securing information and communication in the digital realm, acting as the locks and keys of the cyberworld. It is like the superhero of the digital world, using special math tricks to keep our information safe. It's the reason your messages and data stay private when you send them online. Imagine it as putting your secrets in a magic box and only letting the person with the right key open it. This magical process also makes sure nobody messes with your information while it's being sent or stored. Cryptography acts like a guardian, making sure only the right people can access and understand what you're sending, kind of like a secret code for the internet. It's the superhero that protects our online world from bad guys who might try to spy on our conversations or mess with our data. . It involves the use of mathematical techniques to secure information, ensuring that only authorized parties can access it while protecting it from unauthorized access or manipulation.

History

1. Hieroglyphs:

Definition: Hieroglyphs are a system of writing in ancient Egypt, consisting of pictorial symbols.

Cryptography Connection: In the context of cryptography, hieroglyphs could refer to using symbols or characters as part of a substitution cipher.

2. Scytale:

Definition: A scytale is an ancient cryptographic tool used by the Spartans. It involves wrapping a strip of parchment around a rod to write a message, and the message is only revealed when the strip is unwound from the rod of the same diameter.

Cryptography Connection: Scytale is an early example of a transposition cipher, where the order of letters is rearranged.

3. Transposition/Substitution Ciphers:

Transposition Cipher: Involves rearranging the order of letters in a message without changing the actual letters.

Substitution Cipher: Involves replacing letters with other letters or symbols.

4. Kautiliyam/Mulavediya/Caesar Shift:

Kautiliyam: Possibly a reference to Chanakya, also known as Kautilya, an ancient Indian teacher, philosopher, economist, and royal advisor.

Mulavediya: Not clear without additional context.

Caesar Shift: A type of substitution cipher where each letter in the plaintext is shifted a certain number of places down or up the alphabet.

5. Polyalphabetic - Alberti, Vigenère Cipher:

Alberti Cipher: Invented by Leon Battista Alberti, it involves the use of two concentric disks, each with an alphabet, to encrypt messages.

Vigenère Cipher: A method of encrypting alphabetic text using a simple form of polyalphabetic substitution.

6. Cryptanalysis - Mid 19th Century:

Cryptanalysis: The study of techniques for attempting to defeat cryptographic techniques and gain access to the information being protected.

Mid 19th Century: This period saw the development of more systematic and mathematical approaches to cryptanalysis, especially with the advent of frequency analysis.

In 1976, super-smart people created a cool way to keep online secrets safe. They made two special keys: one for everyone to use (public key) and one secret key just for you. If someone wants to send you a secret message, they use the public key. But only you, with your secret key, can actually read it. It's like having a magical lock and key for the internet, so you can chat and do stuff without worrying about sneaky eavesdroppers. This idea made online shopping and talking super secure.

Great Learning

CERTIFICATE OF COMPLETION

Presented to

Adhila Ismail

For successfully completing a free online course

Introduction to Cryptography

Provided by

Great Learning Academy

(On September 2023)