ASSIGNMENT

(RLMCA305 - Cryptography and Cyber Security)

Submitted by;

Rohith Santhosh

INT MCA S9

Roll no: 48

Submitted to;

Miss. Sona Maria Sebastian

Course Title: Introduction to Cryptography

Course Summary:

This comprehensive course offered by MyGreatLearning Academy takes a deep dive into the world of cryptography, covering a wide range of topics, including its historical development and its role in securing information and communication in today's adversarial digital landscape.

Introduction:

Cryptography and Its History:

The course commences with an exploration of the origins of cryptography. It traces its roots to ancient civilizations, highlighting:

- **Hieroglyphs**: Hieroglyphs are one of the earliest forms of cryptography used by ancient Egyptians to encode messages. I gained insights into how symbols and pictorial representations were employed for secrecy.
- **Scytale**: The Scytale, an ancient Spartan cryptographic tool, is examined. This device involved wrapping a strip of parchment around a cylinder to encrypt messages. The course delves into its use and significance.

Locks and Keys of the Cyberworld:

The course bridges the gap between the physical and digital realms, emphasizing the parallels between physical locks and keys and their digital counterparts. It explores how encryption serves as the "locks" for securing digital information, and cryptographic keys are the "keys" to unlocking and protecting that data.

Sending a Physical Object vs. Sending Information:

This section of the course draws a clear distinction between the logistics of sending physical objects and transmitting digital information. It sheds light on the unique challenges associated with securing the transfer of data in the digital realm, where information can be intercepted and manipulated by malicious actors.

Cryptography in the Face of Adversarial Behavior:

One of the core themes of the course is the concept of cryptography as a defense against adversarial behavior. It provides an in-depth understanding of how cryptographic techniques

are employed to safeguard sensitive information and communications in the presence of adversaries who seek to compromise or intercept them.

Transposition/Substitution Ciphers and Cryptanalysis:

The course delves into classical cryptographic techniques, including:

- **Transposition Ciphers**: These involve rearranging the order of characters in a message. I learned about methods such as the Kautilyam, Mulavediya, and Caesar Shift, which rely on various transposition principles.
- **Substitution Ciphers**: The course covers substitution ciphers, including the famous Caesar Shift, where letters are replaced by others based on a fixed shift value.
- **Cryptanalysis**: I explored the art of cryptanalysis, which involves deciphering encrypted messages without the knowledge of the key. The course introduces cryptanalysis techniques that have evolved over time.

World Wars I and II and Public-Key Cryptography:

The course highlights the pivotal role of cryptography during the World Wars, with a particular focus on:

- **Enigma Machine**: The Enigma machine, used by the Germans during World War II, is discussed in detail. I gained insight into how Allied cryptanalysts successfully cracked the Enigma code, significantly impacting the course of the war.
- **1976: Public-Key Cryptography**: The course concludes with a critical milestone in the history of cryptography—public-key cryptography. This breakthrough development, which occurred in 1976, revolutionized the field by introducing a new way of securely exchanging cryptographic keys without prior communication.

By the end of this course, I have a profound understanding of the historical evolution of cryptography, its significance in securing information, and the fundamental principles and techniques that underpin modern cryptographic systems. This knowledge is invaluable for those interested in cybersecurity, information security, and the history of encryption.

Course Certificate: