# ASSIGNMENT

**Cryptography and Cyber Security**

Shino.V.Shibu

54,11032

# Encryption

Course Title: Encryption

Course Link: https://olympus.mygreatlearning.com/courses/66456

Encryption secures digital data using one or more mathematical techniques known as cryptography. The information input becomes unreadable through encryption as an algorithm converts the original text, known as plaintext, into an alternative form known as ciphertext. When an authorized user needs to read the data, they may decrypt the data using a binary key or password. This will convert ciphertext back to plaintext so that the user can access the original information.

Encryption is an important way for individuals and companies to protect sensitive information from hacking. For example, websites that transmit credit card and bank account numbers encrypt this information to prevent identity theft and fraud.

**Decryption** is the process of converting meaningless message (Ciphertext) into its original form (Plaintext). The major distinction between secret writing associated secret writing is that the conversion of a message into an unintelligible kind that's undecipherable unless decrypted. whereas secret writing is that the recovery of the first message from the encrypted information.

## Types of Encryption

There are many different types of encryption, each with its own benefit and use case.

- Symmetric Encryption

In this simple encryption method, only one secret key is used to both cipher and decipher information. While the oldest and best-known encryption technique, the main drawback is that both parties need to have the key used to encrypt the data before they can decrypt it. Symmetric encryption algorithms include AES-128, AES-192, and AES-256. Because it is less complex and executes faster, symmetric encryption is the preferred method for transmitting data in bulk.

- Asymmetric Encryption

Also known as public key cryptography, asymmetric encryption is a relatively new method that uses two different but related keys to encrypt and decrypt data. One key is secret and one key is public. The public key is used to encrypt data, and the private key is used to decrypt (and vice versa). Security of the public key is not needed because it is publicly available and can be shared over the internet.

Great Learning

# CERTIFICATE OF COMPLETION

Presented to

## Shino V Shibu INT MCA 2018-2023

For successfully completing a free online course

Encryption

Provided by

Great Learning Academy

(On October 2022)

To verify this certificate visit verify.mygreatlearning.com/XDHCVWRT