ACTIVITY 4.

1. **True or False Activity:** Read the following statements and decide if they are True (T) or False (F).

- Symmetric encryption uses the same key for both encrypting and decrypting data.
- Plaintext is the unreadable format of the data after encryption.
- Symmetric encryption is not suitable for large amounts of data like videos or databases.
- Key sharing is one of the challenges of symmetric encryption.
- AES (Advanced Encryption Standard) is faster and more secure than DES.
- Symmetric encryption cannot protect data during transfer.
- Financial transactions in online banking often use symmetric encryption.
- 3DES is a slower and more secure version of DES.
- Managing a large number of encryption keys is simple with symmetric encryption.
- Symmetric encryption plays a vital role in ensuring confidentiality and privacy in digital communication.

2. **KEYWORDS**

Encryption: A security method that scrambles data so it is only read by using a key

Blocks of data: a sequence of data in bits or bytes that are usually transferred as a whole.

Bit: A bit is the smallest unit of digital information that can be processed by a computer, consisting of either a 0 or 1.

Pseudorandom: a sequence of numbers or data that appears random but is generated by a deterministic algorithm

Cipher text: is encrypted text transformed from plaintext using an encryption algorithm.

Plain text: text that is not computationally tagged, specially formatted, or written in code.

Decryption: is the process of transforming data that has been rendered unreadable through encryption back to its unencrypted form

Web traffic: the volume of users visiting a website.

HTTPS: Hypertext transfer protocol secure (HTTPS) is the secure version of HTTP, which is the primary protocol used to send data between a web browser and a website.