CYBERSECURITY TRAINING (WEEK 2 - Day 5)

1.1 Introduction to cryptography

Cryptography is the science and art of securing information by transforming it into a form that is unreadable to unauthorized users. It enables **confidentiality**, **integrity**, **authentication**, and **non-repudiation** of data.

- **History of cryptography**

1. Caesar Cipher (Rome, ~100 BCE):

   Replaces each letter by a fixed number of positions in the alphabet. Example: A → D (Shift of 3).

2. Substitution & Transposition Ciphers:

   Letters are replaced or rearranged. Used by ancient Greeks (Scytale cipher) and Arab scholars.

3. Post-Quantum & Future Cryptography

   Research on cryptography that can resist attacks from **quantum computers**.
   Lattice-based cryptography, multivariate cryptography, etc.

1.2 Introduction to steganography

Steganography is the practice of hiding secret information **within** ordinary, non-secret data or media (like an image, audio, or video) in such a way that the

presence of the hidden information is **not obvious**.

- **History of steganography**

1. Invisible Inks (Middle Ages):
   Using lemon juice or milk, visible only with heat.
2. Shrinking secret messages to the size of a dot and hiding them in a document.
3. Most common. Hides data in **pixels**, often using **Least Significant Bit (LSB)**.
4. Hides data in sound waves by modifying frequency or amplitude.