Week1 solution

Ans1

Cryptography is the science of securing communication and data from unauthorized access or alteration. It involves creating and analyzing protocols and algorithms to protect information. Here's a breakdown of the key concepts:

**Cryptanalysis** is the art and science of breaking cryptographic systems—essentially the opposite of cryptography. While cryptography aims to secure information, **cryptanalysis** tries to **find weaknesses** or flaws in those systems to **decrypt messages without knowing the key**.

**cryptographic attacks**, which are techniques used to break or weaken cryptographic systems.

**Encryption** is the process of converting readable data (**plaintext**) into an unreadable form (**ciphertext**) using a **key** and an **algorithm**, so that unauthorized people can’t understand it.

**Decryption** is the reverse process—transforming the ciphertext back into plaintext using the **correct key** and algorithm.

Plaintext The original readable message or data before encryption

|  |
| --- |
|  |

|  |
| --- |
| Ciphertext The encrypted (scrambled) version of the plaintext |
| A **key** is a piece of information that determines the output of a cryptographic algorithm. Without the key, you can’t decrypt the message properly.  Ans2  **. Caesar Cipher**   * **Type**: Monoalphabetic Substitution * **Mechanism**: Shifts each letter in the plaintext by a fixed number of positions (usually 3) in the alphabet. * **Example**:   + Plaintext: HELLO   + Key: 3   + Ciphertext: KHOOR   **2. Monoalphabetic Cipher**   * **Type**: Monoalphabetic Substitution * **Mechanism**: Each letter of the alphabet is replaced with another letter using a fixed mapping (substitution key). * **Example Key**: A → Q, B → W, C → E, etc. * **Example**:   + Plaintext: HELLO   + Ciphertext (with the key): ZEBBW * **Weakness**: Vulnerable to frequency analysis due to fixed substitution pattern.   **Playfair Cipher**   * **Type**: Digraph Substitution (encrypts pairs of letters) * **Mechanism**: Uses a 5x5 matrix constructed from a keyword (J usually combined with I). * **Rules**:   + Same row → shift right.   + Same column → shift down.   + Rectangle → swap columns. * **Example**:   + Key: MONARCHY   + Plaintext: BALLOON → divided as BA LL OO N → modified to BA LX LO ON   + Ciphertext: (depends on matrix)   **Hill Cipher**   * **Type**: Polyalphabetic Substitution using linear algebra * **Mechanism**: Plaintext is converted into vectors, multiplied by a key matrix (mod 26). * **Example**:   + Key Matrix (2x2): [[3, 3], [2, 5]]   + Plaintext: HI → vector [7, 8]   + Ciphertext: [3\*7 + 3\*8, 2\*7 + 5\*8] mod 26 = [45, 54] mod 26 = [19, 2] → TC * **Strength**: Requires linear algebra to break, but key matrix must be invertible mod 26.   **5. Polyalphabetic Cipher (Vigenère Cipher)**   * **Type**: Polyalphabetic Substitution * **Mechanism**: Uses a keyword to shift letters of the plaintext using Caesar Cipher with varying shifts. * **Example**:   + Plaintext: ATTACKATDAWN   + Key: LEMONLEMONLE   + Ciphertext: LXFOPVEFRNHR * **Strength**: Stronger than Caesar or monoalphabetic ciphers, but vulnerable to Kasiski and frequency analysis if key is reused.   **6. One Time Pad (OTP)**   * **Type**: Perfect Substitution * **Mechanism**: Uses a random key that is as long as the plaintext. Each letter is encrypted with a unique key value. * **Example**:   + Plaintext: HELLO   + Key: XMCKL   + Ciphertext: (by converting to numbers and adding mod 26) * **Security**: **Unbreakable** if key is truly random, used once, and kept secret. * **Weakness**: Key management is extremely difficult.   **1. Rail Fence Cipher**   * **Mechanism**: Writes the plaintext in a zig-zag pattern across multiple "rails" (rows) and reads it row by row. * **Example**:   + Plaintext: WEAREDISCOVEREDFLEEATONCE   + Key (number of rails): 3   + Writing:   Ans3  Code1 **. Caesar Cipher**  Code2 **Monoalphabetic Cipher** |