**CS409 ETHICAL HACKING**

**HOMEWORK 4**

1. **What is a cryptosystem? Explain the five types of cryptanalytic attacks.**

It functions by encrypting plain text at the sender's end using some encryption technique, and decrypting ciphertext at the receiver's end. Confidentiality, integrity, authenticity, and non-repudiation are all provided by cryptography.

* Cyphertext only: In this kind of attack, the attacker only has access to a small amount of ciphertext and must search for the associated encryption key and plaintext. Since only ciphertext is needed, it is the most difficult to implement but also the most likely attack.
* Known Plaintext: Some plaintext-ciphertext pairings used in this kind of attack are already well-known. To locate the encryption key, the attacker maps them. Due to the abundance of already-available information, this approach is simpler to use.
* Chosen plaintext: This kind of attack involves the attacker selecting random plaintexts, obtaining the accompanying ciphertexts, and attempting to decipher the encryption key. Like KPA, it is easy to install, but it has low success rates.
* Chosen ciphertext: To attack cipher, choose ciphertext and get plaintext.
* Chosen text: To encrypt or decrypt an attack cipher, choose either ciphertext or plaintext.

1. **What is Rail Fence cipher? Convert the following plaintext into ciphertext using Rail Fence Cipher. ILOVECYBERSECURITY**

The Rail fence cipher is a simple transposition cipher that quickly and conveniently shuffles the letters in a message. In order to make it a little bit more difficult to crack, it also has the security of a key.

You must write your message in zigzag lines across the paper and then read off each row to encrypt it using the Rail Fence Cipher. In order to decrypt a message, you must first have a key, which for this cipher is the number of rows you intend to have. You then begin writing the plaintext letters diagonally down to the right until you reach the number of rows provided by the key. When you reach the first row once more, you bounce back up diagonally. This keeps on until the plaintext is finished.

As the key(for the depth) has not been mentioned, I had used 3 to encode as submitted in the attachment for the solution (Filename: RailFenceCipher)

1. **Convert the following plaintext into ciphertext using Playfair Cipher. Key: MONARCHY Plaintext: INSTRUMENTS**

Please find the solution in the attachment for filename: Playfair

1. **Explain frequency attack on a substitution cipher.**

Frequency analysis in cryptography is the study of the frequency of individual letters or groups of letters in a ciphertext. The technique is employed to help break substitution ciphers.

Each letter in a text is counted for frequency analysis purposes. The basis for frequency analysis is the fact that specific letters and letter combinations appear in texts with varied frequencies. For instance, in the English language, the letters E, T, A, and O are most frequently used, while Z, Q, and X used less frequently.

1. **Convert the following plaintext into ciphertext using Vernam Cipher (One-Time Pad). Key: HELLO Plaintext: WORLD**

Please find the solution in the attachment for filename: Vernam

1. **What is steganography? Mention some techniques of doing steganography.**

Steganography is the practice of enclosing information in another message or physical item in a way that prevents human inspection from revealing its presence. Steganography encloses hidden communications in a cover message so that only the sender and the intended receiver are aware of their presence.

Text Steganography: Information is being concealed through text steganography in the text files. To create understandable texts, it may be necessary to alter the format of already existing text, change the words inside a text, create random letter sequences, or use context-free grammar. There are many ways to conceal the data in the text, including:

Format-Based Approach

Linguistic Method

Random and Statistical Generation

Audio/ Video/ Image/ Network steganography are some other techniques.