Experiment 1: Breaking the Mono-alphabetic Substitution Cipher using Frequency analysis method

Question: What is the principle behind frequency analysis?

Answer: Frequency analysis is a technique used to analyze the frequency distribution of characters in a ciphertext. The assumption is that the frequency of characters in the ciphertext will correspond to the frequency of characters in the plaintext language.

Question: How does frequency analysis help in breaking mono-alphabetic substitution ciphers?

Answer: By comparing the frequency distribution of characters in the ciphertext to the known frequency distribution of characters in the plaintext language, we can make educated guesses about the substitution of characters. This can be used to create a substitution table and decrypt the ciphertext.

Question: What are the limitations of frequency analysis?

Answer: Frequency analysis is effective for short ciphertexts, but it becomes less effective for longer ciphertexts or if the plaintext language is not well-known or if the ciphertext has been modified to obscure the frequency distribution.

Question: Can frequency analysis be used to break polyalphabetic substitution ciphers?

Answer: No, frequency analysis is not effective for breaking polyalphabetic substitution ciphers because the frequency distribution of characters in the ciphertext will not correspond to the frequency distribution of characters in the plaintext language.

Experiment 2: Cryptanalysis or decoding Playfair cipher

Question: Explain the Playfair cipher.

Answer: The Playfair cipher is a digraphic substitution cipher that substitutes pairs of characters instead of individual characters. A 5x5 grid is used to represent the alphabet, and pairs of characters are substituted based on their positions in the grid.

Question: How can you identify a Playfair cipher?

Answer: A Playfair cipher can be identified by the fact that it substitutes pairs of characters and that the substitution pattern is based on a 5x5 grid.

Question: What are the common techniques used to crack Playfair ciphers?

Answer: Common techniques used to crack Playfair ciphers include frequency analysis (based on digraphs), pattern recognition, and known plaintext attacks.

Question: Can you demonstrate the steps involved in decoding a Playfair cipher?

Answer: Yes, I can demonstrate the steps involved in decoding a Playfair cipher. This would involve creating a 5x5 grid based on the key, analyzing the ciphertext for patterns, and using known plaintext or frequency analysis to determine the substitution pairs.

Experiment 3: Cryptanalysis or decoding Vigenère cipher

Question: What is the Vigenère cipher?

Answer: The Vigenère cipher is a polyalphabetic substitution cipher that uses a keyword to select which alphabet to use for each letter of the plaintext.

Question: How does the Vigenère cipher differ from the mono-alphabetic substitution cipher?

Answer: The Vigenère cipher uses multiple substitution alphabets, while the mono-alphabetic substitution cipher uses only one.

Question: What is the Kasiski examination method?

Answer: The Kasiski examination method is a technique used to determine the length of the keyword in a Vigenère cipher by looking for repeated sequences of letters in the ciphertext.

Question: How can you determine the length of the key in a Vigenère cipher?

Answer: The length of the key can be determined using the Kasiski examination method or by analyzing the frequency distribution of characters in different parts of the ciphertext.

Experiment 4: Encrypt and Decrypt short messages using Hill Cipher

Question: Explain the Hill cipher.

Answer: The Hill cipher is a polyalphabetic substitution cipher that uses matrix multiplication to encrypt and decrypt messages. The key is a square matrix of numbers.

Question: What is the mathematical basis of the Hill cipher?

Answer: The Hill cipher is based on matrix multiplication and linear algebra.

Question: How do you find the inverse of a matrix in the Hill cipher?

Answer: The inverse of a matrix can be found using the adjoint method or Gaussian elimination.

Question: What are the limitations of the Hill cipher?

Answer: The Hill cipher is vulnerable to attacks if the key matrix is not invertible or if the plaintext is short.

Experiment 5: Encrypt long messages using various modes of operation using AES

Question: What is AES?

Answer: AES (Advanced Encryption Standard) is a symmetric-key encryption algorithm that is widely used for secure communication.

Question: Explain the different modes of operation used in AES.

Answer: The different modes of operation used in AES include Electronic Codebook (ECB), Cipher Block Chaining (CBC), Counter (CTR), Cipher Feedback (CFB), and Output Feedback (OFB).

Question: How does each mode of operation ensure security?

Answer: Each mode of operation has its own strengths and weaknesses, but they all aim to provide security by preventing attacks such as frequency analysis and known plaintext attacks.

Question: When would you choose one mode of operation over another?

Answer: The choice of mode of operation depends on the specific requirements of the application, such as the need for confidentiality, integrity, or authenticity.

Experiment 6: Encrypt long messages using various modes of operation using DES

Question: What is DES?

Answer: DES (Data Encryption Standard) is a symmetric-key encryption algorithm that was widely used in the past, but is now considered to be insecure due to its small key size.

Question: How does DES differ from AES?

Answer: DES uses a smaller key size (64 bits) than AES (128, 192, or 256 bits) and has a simpler structure.

Question: Explain the different modes of operation used in DES.

Answer: The different modes of operation used in DES include Electronic Codebook (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB), and Output Feedback (OFB).

Question: What are the security concerns associated with DES?

Answer: DES is now considered to be insecure due to its small key size, which can be easily brute-forced.

Experiment 7: Cryptographic Hash Functions and Applications (HMAC)

Question: What is a cryptographic hash function?

Answer: A cryptographic hash function is a mathematical function that takes an input of arbitrary size and produces a fixed-size output, known as a hash value.

Question: What are the properties of a good cryptographic hash function?

Answer: A good cryptographic hash function should be:

- **Pre-image resistant:** It should be difficult to find an input that produces a given hash value.
- **Second pre-image resistant:** It should be difficult to find two different inputs that produce the same hash value.
- **Collision resistant:** It should be difficult to find two different inputs that produce the same hash value.

Question: Explain the concept of HMAC.

Answer: HMAC (Hash-based Message Authentication Code) is a message authentication code that uses a cryptographic hash function and a secret key to ensure the integrity and authenticity of a message.

Question: How is HMAC used to ensure message integrity?

Answer: HMAC is used to ensure message integrity by calculating a hash value of the message and a secret key. If the calculated hash value matches the hash value that was sent with the message, then the message is likely to be intact and unmodified.

Experiment 8: Implementation and analysis of RSA cryptosystem and Digital signature scheme using RSA

Question: Explain the RSA algorithm.

Answer: RSA is a public-key encryption algorithm that uses a pair of keys: a public key and a private key. The public key is used to encrypt messages, while the private key is used to decrypt them.

Question: How are the public and private keys generated in RSA?

Answer: The public and private keys in RSA are generated using a mathematical process that involves large prime numbers and modular arithmetic.

Question: How does RSA work for encryption and decryption?

Answer: In RSA, the plaintext is encrypted using the public key and the resulting ciphertext is decrypted using the private key.

Question: What is a digital signature? How is RSA used for digital signatures?

Answer: A digital signature is a cryptographic technique that is used to verify the authenticity and integrity of a message. In RSA, a digital signature is created by using the private key to encrypt a hash value of the message. The recipient can then verify the signature by using the public key to decrypt the hash value and comparing it to the hash value of the message.

Experiment 9: Study the Keyloggers and its functionality

Question: What is a keylogger?

Answer: A keylogger is a type of malware that records keystrokes entered on a computer.

Question: How do keyloggers work?

Answer: Keyloggers can be installed on a computer without the user's knowledge and can record all keystrokes, including passwords, credit card numbers, and other sensitive information.

Question: What are the potential risks of keyloggers?

Answer: Keyloggers can be used to steal personal information, financial data, and other sensitive information.

Question: How can you detect and prevent keylogger attacks?

Answer: Keylogger attacks can be detected by using antivirus software, monitoring network traffic, and being aware of unusual behavior on the computer. To prevent keylogger attacks, it is important to use strong passwords, avoid clicking on suspicious links, and keep software up to date.

Experiment 10: Study of packet sniffer tools Wireshark

Question: What is a packet sniffer?

Answer: A packet sniffer