MIT World Peace University

Information and Cyber Security

Assignment 1

Naman Soni Roll No. 10

Contents

1 Aim

Write a program using JAVA or Python or C++ to implement any classical cryptographic technique.

2 Objective

To conceal the context of some message from all accept the sender and recipient (Privacy or secrecy)

3 Theory

3.1 *Cryptography*

Cryptography is the practice of securing communication by converting plain text into a coded or scrambled format to prevent unauthorized access or interception. It involves the use of mathematical algorithms and techniques to encrypt and decrypt data.

The main goal of cryptography is to ensure the confidentiality, integrity, and authenticity of information. Confidentiality refers to keeping information secret from unauthorized parties, integrity means that the data remains unaltered during transmission or storage, and authenticity means verifying that the information comes from a trusted source.

Cryptography has been used for centuries to protect important information, including military secrets, financial transactions, and personal data. Today, cryptography plays a crucial role in securing online communications, including email, banking transactions, e-commerce, and messaging apps.

There are several types of cryptographic techniques, including symmetric key cryptography, asymmetric key cryptography, and hashing. Symmetric key cryptography uses the same key for both encryption and decryption, while asymmetric key cryptography uses a public key for encryption and a private key for decryption. Hashing creates a fixed-size output, called a hash, from any input data and is commonly used for verifying the integrity of data.

3.2 *Substitution Cypher*

A substitution cipher is a type of cryptographic technique that involves replacing each letter of the original plaintext message with another letter or symbol. This technique is based on the principle of replacing one entity with another.

In a simple substitution cipher, each letter of the alphabet is replaced with a different letter. For example, the letter "A" might be replaced with the letter "D", "B" with "E", and so on. This creates a new message that is unreadable to anyone who doesn't know the substitution key.

There are many different types of substitution ciphers, including the Caesar cipher, which involves shifting each letter of the alphabet a fixed number of positions. For example, if the key is "3", then "A" would be replaced with "D", "B" with "E", and so on.

Substitution ciphers are relatively easy to use and understand, but they are also easy to break. Cryptanalysts can use frequency analysis to identify common patterns in the ciphertext and guess the substitution key. As a result, substitution ciphers are typically used as a basic form of encryption or as part of a more complex cryptographic system.

3.3 *Transposition Cypher*

A transposition cipher is a type of cryptographic technique that involves rearranging the letters or symbols of a message without changing the actual letters or symbols themselves. This technique is based on the

principle of rearranging the order of entities in a message.

In a simple transposition cipher, the letters of the original message are rearranged according to a specific pattern. For example, the letters could be rearranged in reverse order, or every second letter could be switched with the letter next to it. This creates a new message that is unreadable to anyone who doesn't know the transposition key.

There are many different types of transposition ciphers, including rail fence ciphers, columnar transposition ciphers, and route ciphers. Rail fence ciphers involve writing the message out in a zigzag pattern across a set number of rows and then reading the message horizontally. Columnar transposition ciphers involve rearranging the letters of the message according to a specific columnar pattern, while route ciphers involve reading the message in a specific order by following a predetermined path through a grid of letters.

Transposition ciphers can be more secure than substitution ciphers because they are less susceptible to frequency analysis. However, they can still be vulnerable to cryptanalysis if the pattern used for the transposition is predictable. As a result, transposition ciphers are typically used as a basic form of encryption or as part of a more complex cryptographic system.

4 Code

```
import java.util.Scanner;

public class caeser_cipher {

  public static void main(String[] args) {

    Scanner sc = new Scanner(System.in);

    System.out.print("Enter a message: ");
    String message = sc.nextLine();

    System.out.print("Enter the shift key (1-25): ");
    int shift = sc.nextInt();

    String cipherText = encrypt(message, shift);
    System.out.println("Encrypted message: " + cipherText);

    String plainText = decrypt(cipherText, shift);
    System.out.println("Decrypted message: " + plainText);

    sc.close();
  }

  public static String encrypt(String message, int shift) {
    StringBuilder cipherText = new StringBuilder();

    for (int i = 0; i < message.length(); i++) {
      char c = message.charAt(i);

      if (Character.isLetter(c)) {
        c = (char) (c + shift);

        if (Character.isLowerCase(message.charAt(i)) && c > 'z') {
          c = (char) (c - 26);
        } else if (Character.isUpperCase(message.charAt(i)) && c > 'Z') {
          c = (char) (c - 26);
        }
      }

      cipherText.append(c);
    }

```

```
43        return cipherText.toString();
44      }
45
46      public static String decrypt(String cipherText, int shift) {
47        return encrypt(cipherText, -shift);
48      }
49    }
50
```

Listing 1: Input

```
1   Enter a message: hey how are you
2   Enter the shift key (1-25): 23
3   Encrypted message: ebv elt xob vlr
4   Decrypted message: NK_ NU] aXK _U[
5
```

Listing 2: Output

5 Conclusion

Thus, we learnt about classical cryptography

6 FAQ's

1. What are various classical ciphers?

   Ans. Classical ciphers are encryption techniques that were used before the development of modern cryptographic systems. These ciphers were typically based on simple mathematical operations and substitutions and were often used to protect military, diplomatic, or personal communications. Here are some examples of classical ciphers:

   - Caesar Cipher: This is a type of substitution cipher in which each letter of the plaintext message is shifted a fixed number of positions down the alphabet. For example, a key of 3 would shift "A" to "D", "B" to "E", and so on.
   - Vigenère Cipher: This is a type of polyalphabetic substitution cipher in which multiple Caesar ciphers are used with different shift values based on a repeating keyword.
   - Playfair Cipher: This is a type of substitution cipher that uses a 5x5 grid of letters to encrypt plaintext. The letters of the message are paired up and replaced by other letters in the same grid according to a specific rule.
   - Rail Fence Cipher: This is a type of transposition cipher in which the plaintext message is written out diagonally on a set number of rails, and then read off in a specific order.
   - Polybius Square: This is a type of substitution cipher that uses a 5x5 grid of letters or numbers to encrypt plaintext. Each letter or number is represented by its coordinates in the grid.
   - Atbash Cipher: This is a type of substitution cipher in which each letter of the plaintext message is replaced by the corresponding letter in the opposite position in the alphabet. For example, "A" is replaced by "Z", "B" by "Y", and so on.

   These are just a few examples of classical ciphers. While these ciphers are relatively simple and easy to understand, they are also easy to break using modern cryptanalysis techniques. As a result, they are generally not considered secure for modern communication purposes.

2. Compare steganography and Cryptography?

Ans. Steganography and cryptography are two different techniques used to protect information and maintain its confidentiality. While they share some similarities, they differ in their approach and purpose.

Cryptography is the practice of converting plain text into a coded or scrambled format to prevent unauthorized access or interception. It involves the use of mathematical algorithms and techniques to encrypt and decrypt data. The main goal of cryptography is to ensure the confidentiality, integrity, and authenticity of information.

Steganography, on the other hand, is the practice of hiding a message within another message or file. It involves concealing the existence of a message by embedding it within an innocuous-looking cover object, such as an image or audio file. The main goal of steganography is to keep the existence of the message secret, rather than to keep its contents secret.

While both cryptography and steganography are used to protect information, cryptography is more commonly used for secure communication, such as in email or online transactions. Steganography is often used for covert communication, such as in espionage or other secret activities.

Another key difference between the two techniques is that cryptography alters the message itself, while steganography does not. Cryptography converts the original message into a different, coded format that cannot be understood without the proper decryption key. Steganography, on the other hand, hides the existence of the message within another object, but does not alter the original message itself.

In summary, cryptography and steganography are two different techniques used for protecting information. Cryptography converts the original message into a coded format to prevent unauthorized access, while steganography hides the existence of the message within another object.

3. What are the few major applications of cryptography in the modern world?

Ans. Cryptography has many applications in the modern world, ranging from securing communications to protecting financial transactions. Here are a few major applications of cryptography:

- Secure Communication: Cryptography is used to secure communication between two parties, such as in online transactions, email, and instant messaging. Cryptography ensures that only the intended recipient can read the message by encrypting it using a secret key.
- Secure Communication: Cryptography is used to secure communication between two parties, such as in online transactions, email, and instant messaging. Cryptography ensures that only the intended recipient can read the message by encrypting it using a secret key.
- Data Protection: Cryptography is used to protect sensitive data, such as passwords, credit card numbers, and other personal information. This is achieved by encrypting the data before it is stored or transmitted, so that only authorized users with the decryption key can access it.
- Authentication: Cryptography is used to authenticate the identity of users and devices, such as in digital signatures, authentication protocols, and access control systems. Cryptography ensures that only authorized users can access a system or resource by verifying their identity using digital signatures or other authentication mechanisms.
- Blockchain: Cryptography is used in blockchain technology to secure transactions and prevent fraud. The integrity of the blockchain is maintained through a distributed network of computers that use complex cryptographic algorithms to validate transactions and ensure that they are not tampered with.
- Password Storage: Cryptography is used to store passwords securely by hashing them using a one-way algorithm. This ensures that even if the password database is compromised, the passwords cannot be easily decrypted or reversed.

- Digital Rights Management: Cryptography is used in digital rights management (DRM) systems to protect copyrighted content, such as movies, music, and software. Cryptography is used to encrypt the content so that only authorized users with the decryption key can access it.

These are just a few examples of the many applications of cryptography in the modern world. Cryptography plays a critical role in protecting sensitive information and ensuring the integrity and authenticity of digital communication and transactions.

4. How can the Caesar cipher be cracked?

Ans. The Caesar cipher is a simple substitution cipher that involves shifting the letters of the plaintext message by a fixed number of positions down the alphabet. While the Caesar cipher was once considered a secure encryption method, it can now be easily cracked using modern cryptanalysis techniques. Here are a few methods to crack the Caesar cipher:

- Brute Force Attack: In a brute force attack, the attacker tries every possible shift value until the correct plaintext is obtained. Since there are only 26 possible shift values in the Caesar cipher, this method can be easily automated and can be done quickly using a computer.
- Frequency Analysis: Another way to crack the Caesar cipher is to use frequency analysis. In this method, the attacker analyzes the frequency of letters in the ciphertext and compares it to the frequency of letters in the English language. Since certain letters, such as "E", "T", and "A", are more common in English than others, the attacker can determine the most likely shift value by analyzing the frequency of letters in the ciphertext.
- Known Plaintext Attack: In a known plaintext attack, the attacker has access to both the plaintext and the ciphertext. By analyzing the relationship between the plaintext and ciphertext, the attacker can determine the shift value used in the encryption.
- Crib Dragging: Crib dragging is a manual method that involves comparing the ciphertext to known plaintext, such as common phrases or words. By looking for patterns and matching the ciphertext to the known plaintext, the attacker can determine the shift value used in the encryption.

In summary, while the Caesar cipher is a simple encryption method, it can be easily cracked using modern cryptanalysis techniques. To ensure the security of encrypted messages, it is recommended to use more secure encryption methods, such as the Advanced Encryption Standard (AES) or the RSA algorithm.