MIT World Peace University

Information and Cybersecurity
Second Year B. Tech, Semester 1

Classical Cryptographic Techniques
"Ceasar Cipher"

Lab Assignment 1

Prepared By

Krishnaraj Thadesar
Cyber Security and Forensics
Batch A1, PA 20

February 19, 2023

Contents

1 Aim

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

2 Objectives

To conceal the context of some message from all accept the sender and recipient.

3 Theory

3.1 Cryptography

Cryptography is the practice and study of techniques for secure communication in the presence of third parties called adversaries. More generally, cryptography is about constructing and analyzing protocols that prevent third parties or the public from reading private messages; various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation are central to modern cryptography.

3.2 Types of Cryptography

3.2.1 Classical Cryptography

Classical cryptography is the study of cryptography before the advent of modern computers. The classical ciphers are those ciphers that were in use before the advent of computers.

Some Classical Cryptographic Techniques are:

1. *Caesar Cipher* - A Caesar cipher is a type of substitution cipher in which each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet. For example, with a left shift of 3, D would be replaced by A, E would become B, and so on. The method is named after Julius Caesar, who used it in his private correspondence.

   ```
   Example:
   Plain Text: ABCDEFGHIJKLMNOPQRSTUVWXYZ
   Key: 3
   Cipher Text: DEFGHIJKLMNOPQRSTUVWXYZABC
   ```

2. *Vigenere Cipher* - A Vigenère cipher is a method of encrypting alphabetic text by using a series of interwoven Caesar ciphers, based on the letters of a keyword. It employs a form of polyalphabetic substitution.

   ```
   Example:
   Input : Plaintext :   GEEKSFORGEEKS
   Keyword :  AYUSH
   Output : Ciphertext :  GCYCZFMLYLEIM
   ```

3. *Hill Cipher* - The Hill cipher is a polygraphic substitution cipher based on linear algebra. Invented by Lester S. Hill in 1929, it was the first polygraphic cipher in which it was practical (though barely) to operate on more than three symbols at once. The matrix used for encryption is known as a key matrix.

```
Example of Hill Cipher:
Input  : Plaintext: ACT
Key: GYBNQKURP
Output : Ciphertext: POH
```

4. *Playfair Cipher* - The Playfair cipher is a manual symmetric encryption technique and was the first literal digram substitution cipher. The scheme was invented in 1854 by Charles Wheatstone, but was named after Lord Playfair for promoting its use.

   ```
   Example:
   Key text: Monarchy
   Plain text: instruments
   Cipher text: gatlmzclrqtx
   ```

5. *Affine Cipher* - In cryptography, an affine cipher is a type of monoalphabetic substitution cipher, wherein each letter in an alphabet is mapped to its numeric equivalent, encrypted using a simple mathematical function, and converted back to a letter. The formula used means that each letter encrypts to one other letter, and back again, meaning the cipher is essentially a standard substitution cipher with a rule governing which letter goes to which. As such, it has the weaknesses of all substitution ciphers. Each letter is enciphered with the function (ax + b) mod 26, where b is the magnitude of the shift.

   ```
   Example:
   Encrypted Message is : UBBAHK CAPJKX
   Decrypted Message is: AFFINE CIPHER
   Key: a = 17, b = 20
   ```

6. *DES* - The Data Encryption Standard (DES) is a symmetric-key algorithm for the encryption of electronic data. Although its short key length of 56 bits makes it too insecure for most current applications, it has been highly influential in the advancement of modern cryptography.

7. *AES* - The Advanced Encryption Standard (AES), also known by its original name Rijndael is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001. AES is based on the Rijndael cipher developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen, who submitted a proposal to NIST during the AES selection process. AES is a subset of Rijndael designed by Daemen and Rijmen to be easy to implement in hardware and software. The AES standard has been adopted by the U.S. government and is now used worldwide to protect classified and sensitive but unclassified information.

8. *Substitution Ciphers* - In cryptography, a substitution cipher is a method of encoding by which units of plaintext are replaced with ciphertext, according to a fixed system; the "units" may be single letters (the most common), pairs of letters, triplets of letters, mixtures of the above, and so forth. The receiver deciphers the text by performing an inverse substitution.

   A substitution cipher is a method of encoding by which units of plaintext are replaced with ciphertext, according to a fixed system; the "units" may be single letters (the most common),

pairs of letters, triplets of letters, mixtures of the above, and so forth. The receiver deciphers the text by performing an inverse substitution.

9. *Transposition Ciphers* - In cryptography, a transposition cipher is a method of encryption by which the positions held by units of plaintext (which are commonly characters or groups of characters) are shifted according to a regular system, so that the ciphertext constitutes a permutation of the plaintext. That is, the plaintext is written out in a certain order, then the ciphertext is formed by reading down the columns going left to right.

3.2.2 Modern Cryptography

Modern cryptography exists at the intersection of the disciplines of mathematics, computer science, electrical engineering, communication science, and physics. Applications of cryptography include electronic commerce, chip-based payment cards, digital currencies, computer passwords, and military communications.

Some Modern Cryptographic Techniques are:

1. *Diffie-Hellman Key Exchange* - In cryptography, the Diffie Hellman key exchange is a method of securely exchanging cryptographic keys over a public channel and was one of the first public-key protocols as originally conceived by Whitfield Diffie and Martin Hellman. It is one of the earliest practical examples of public key exchange implemented within the field of cryptography. It was the first public key exchange protocol that did not rely on trusted third parties and was the first public key protocol for which polynomial-time algorithms were found. It is also the first public key protocol for which a practical attack was found.

2. *ElGamal Encryption* - In cryptography, ElGamal encryption is an asymmetric key encryption algorithm based on the Diffie Hellman key exchange. It is named after Taher ElGamal, who published it in 1985. ElGamal encryption is a public-key encryption scheme, meaning that a pair of keys, one public and one private, are used. The public key may be known to everyone, while the private key is kept secret. The scheme is based on the difficulty of the discrete logarithm problem in a finite field.

3. *RSA* - RSA is an algorithm used by modern computers to encrypt and decrypt messages. It is an asymmetric cryptographic algorithm. Asymmetric means that there are two different keys. This is also called public key cryptography, because one of the keys can be given to anyone. The other key must be kept private. The algorithm is based on the fact that finding the factors of a large composite number is difficult: when the factors are prime numbers, the problem is called prime factorization. It is also a key pair (public and private) generator.

4. *Digital Signature* - A digital signature is a mathematical scheme for verifying the authenticity of digital messages or documents. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, the message has not been altered in transit, and the sender cannot deny having sent the message. Digital signatures are a common method of authentication and data integrity in computer systems and communications.

5. *Hashing* - In cryptography, a hash function is any function that can be used to map data of arbitrary size to data of fixed size. The values returned by a hash function are called hash values, hash codes

4 Platform

Operating System: Arch Linux x86-64
IDEs or Text Editors Used: Visual Studio Code
Compilers or Interpreters : Python 3.10.1

5 Pseudo Code or Algorithm

```
// Pseudo Code for Ceasar Cipher
// Input : String, Key
// Output : Ciphered String
// Function to Cipher the String

def Cipher(String, Key):
  Ciphered_String = ""
  for i in String:
    if i.isupper():
      Ciphered_String += chr((ord(i) + Key - 65) % 26 + 65)
    else:
      Ciphered_String += chr((ord(i) + Key - 97) % 26 + 97)
  return Ciphered_String
```

6 Input and Output

```
Welcome to Assignment 1 in Information and CyberSecurity, working with Ceasar Ciphers.
Enter the string that you want to Cipher.
Assignments of Information and Cybersecurity
Enter the key : 9
Applying the Ceasar Cipher to it.
jBBRPWVNWCB XO rWOXAVJCRXW JWM lHKNABNLDARCH
```

7 Code

```
# Assignment 1
# Ceaser Cipher


def get_ascii(some_char):
    if some_char.islower():
        return ord(some_char) - 97
    elif some_char.isupper():
        return ord(some_char) - 65
    else:
        return -1


def ceaser_cipher(plain_text, key):
    cipher_letter = ""
    cipher = []
    for i in plain_text:
```

```
        if i == " ":
            cipher.append(" ")
            continue
        if i.islower():
            cipher_letter = chr(((get_ascii(i) + key) % 26) + 97).upper()
        else:
            cipher_letter = chr(((get_ascii(i) + key) % 26) + 65).lower()

        cipher.append(cipher_letter)
    return cipher


def is_valid(plain_text):
    for i in plain_text.split(" "):
        if not i.isalpha():
            return False
    return True


def main():
    plain_text = "1"
    key = -1

    print(
        "Welcome to Assignment 1 in Information and CyberSecurity, working with Ceaser Ciphers. "
    )
    print("Enter the string that you want to Cipher. ")

    # take inputs from the user.
    plain_text = input()

    while not is_valid(plain_text):
        print("Invalid input, try again!")
        plain_text = input()

    key = int(input("Enter the key : "))

    while key <= 0 or key >= 26:
        print("Key input, try again!")
        key = int(input("Enter the key : "))

    print("Applying the Ceaser Cipher to it. ")
    cipher_text = ceaser_cipher(plain_text, key)
    print("".join(cipher_text))
    return


main()
```

Listing 1: "Ceasar Cipher"

```
import math

ADDED_CHAR = "*"


def rail_transportation(plain_text, key):
    number_of_cols = math.ceil(len(plain_text) / key)
```

```
    matrix = []

    for i in range(number_of_cols * key - len(plain_text)):
        plain_text += "*"

    for _ in range(key):
        col_matrix = []
        for j in range(number_of_cols):
            col_matrix.append(plain_text[j * key + _])
        matrix.append(col_matrix)

    cipher_text = [j for i in matrix for j in i]

    return "".join(cipher_text)


def main():
    # plain_text = input("Enter the Plain text: ")
    # key = int(input("Enter the number of rows as the key:" ))
    plain_text = "GYANENDR"
    key = 3
    if key <= 1:
        print("The key length is smaller than 1, it must be greater! Run again.")
        return

    print("The Plain Text you entered is: ", plain_text)
    print("The key you entered is: ", key)

    cipher_text = rail_transportation(plain_text, key)
    print("The Ciphered Text is: ", cipher_text)

    print("Decrypting now!")

    plain_text = rail_transportation(cipher_text, key)

    plain_text = plain_text.replace(ADDED_CHAR, "")

    print("The Decrypted Plain Text is: ", plain_text)


main()
```

Listing 2: "Rail Transportation Cipher"

8 Conclusion

Thus, learnt about the different kinds of ciphers, classical cryptographic techniques, and how to implement some of them in python.

9 FAQ

1. **What are various classical ciphers?**
   Answer: There are many different kinds of ciphers, some of them are:
   (a) *Caesar Cipher*
   (b) *Vigenere Cipher*
   (c) *Rail Transportation Cipher*
   (d) *Hill Cipher*
   (e) *Playfair Cipher*
   (f) *Autokey Cipher*
   (g) *Columnar Transposition Cipher*
   (h) *Affine Cipher*
   (i) *Monoalphabetic Cipher*
   (j) *Polyalphabetic Cipher*
   (k) *Transposition Cipher*
   (l) *Substitution Cipher*

2. **Compare steganography and Cryptography**

   Answer: **Steganography** is the practice of concealing a file, message, image, or video within another file, message, image, or video.

   Cryptography is the practice and study of techniques for secure communication in the presence of third parties called adversaries. More generally, cryptography is about constructing and analyzing protocols that prevent third parties or the public from reading private messages; various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation are central to modern cryptography. Modern cryptography exists at the intersection of the disciplines of mathematics, computer science, electrical engineering, communication science, and physics. Applications of cryptography include electronic commerce, chip-based payment cards, digital currencies, computer passwords, and military communications.

   Steganogrphy is a type of cryptography.

   Steganography comes from the words steganos (meaning covered or hidden) and graphein (meaning writing). It is the practice of concealing a file, message, image, or video within another file, message, image, or video.

   Cryptography however, comes from the Greek words kryptos (meaning hidden) and graphein (meaning writing). It is the practice and study of techniques for secure communication in the presence of third parties called adversaries.

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

(a) *Electronic Commerce* - Cryptography is used to protect the privacy of credit card numbers, bank account numbers, and other sensitive information exchanged over the Internet.

(b) *Chip-based Payment Cards* - Cryptography is used to protect the privacy of credit card numbers, bank account numbers, and other sensitive information exchanged over the Internet.

(c) *Digital Currencies* - Cryptography is used to protect the privacy of credit card numbers, bank account numbers, and other sensitive information exchanged over the Internet.

(d) *Computer Passwords* - Cryptography is used to protect the privacy of credit card numbers, bank account numbers, and other sensitive information exchanged over the Internet.

(e) *Military Communications* - Cryptography is used to protect the privacy of credit card numbers, bank account numbers, and other sensitive information exchanged over the Internet.

4. **How can Caesar cipher be cracked?**

Answer:

(a) *Frequency Analysis* - Frequency analysis is a method of analyzing the frequency of each letter in a message. The frequency of each letter is compared to the frequency of letters in the English language. If the frequency of a letter in the message is close to the frequency of that letter in the English language, then it is likely that the letter is an English letter. This method is not very effective because it is possible to create a message that has the same frequency of letters as the English language.

(b) *Brute Force* - Brute force is a method of trying every possible key until the correct key is found. This method is very effective, but it is very time consuming.

(c) *Cryptanalysis* - Cryptanalysis is a method of analyzing the cipher to find a weakness in the cipher. This method is very effective, but it is very difficult to find a weakness in a cipher.