UMM AL-QURA UNIVERSITY

Project: Implementing a Basic Cryptosystem

Cybersecurity department

Applied cryptography | SEC 2213

lecturer: Dr.Shrouq Alansari.

Team members :

Student name	Student ID
رتاج باعقيل	
رزان المالكي	
مرح المقاطي	
وفاء العواضي	
صباح العنزي	

Binary Flip Cipher

design and implementation:

I.   encryption:

The system is based on bit-by-bit transforming cipher. We transform plane text to an *ascii* code then take this ascii output and transform it into *decimal* a value and lastly take the decimal value and transform it to a *binary one's-complement* value which mean each one is turned into a zero and vis vars.

I. Transforming the plan-text to ASCII:
Let's take "hello" as an example. will be to transforming each letter into an ascii value.
- h=104
- e=101
- l=108
- l=108
- o=111

II. transforming ascii to binary:
- h=104→1101000
- e=101→1100101
- l=108 →1101100
- l=108 →1101100
- o=111→1101111

Now do the one's-complement:
- 1101000→ 0010111
- 1100101→ 0011010
- 1101100→ 0010011
- 1101100→ 0010011
- 1101111→ 0010000

III. transform the binary to decimal:
- h= 119
- e= 122
- l= 115
- l= 115
- o= 112

IV. now transform the decimal value into characters:
- h=119 →w
- e=122 →z
- l= 115 →s
- l= 115 →s
- o=112 →p

and now we reach the cipher text which is **:wzssp**

Binary Flip Cipher

II. *decrypting:*

the same method is used except that we start from the bottom this time, so we go like:

decimal→binary→binary one's-complement→ascii→ thin we reach the decrypted character.

Character: w

- Flipped Decimal: 119
- Flipped Binary: 1110111
- Binary: 0001000
- ASCII Value: 104
- Decrypted Character: h

Character: z

- Flipped Decimal: 122
- Flipped Binary: 1111010
- Binary: 0000101
- ASCII Value: 101
- Decrypted Character: e

Character: s

- Flipped Decimal: 115
- Flipped Binary: 1110011
- Binary: 0001100
- ASCII Value: 108
- Decrypted Character: l

Character: s

- Flipped Decimal: 115
- Flipped Binary: 1110011
- Binary: 0001100
- ASCII Value: 108
- Decrypted Character: l

Character: p

- Flipped Decimal: 112
- Flipped Binary: 1110000
- Binary: 0001111
- ASCII Value: 111
- Decrypted Character: o

Decrypted Text: hello

Binary Flip Cipher

- **short version of the pseudocode for the Binary Flip Cipher class.**

```
FUNCTION encodeMessage(plaintext):

  encodedMessage = ""

  FOR EACH character IN plaintext:

    encodedMessage = encodedMessage +
flipBits(convertToBinary(convertToASCII(character)
))

  RETURN encodedMessage


FUNCTION decodeMessage(encodedMessage):

  decodedMessage = ""

  FOR EACH character IN encodedMessage:

    decodedMessage = decodedMessage +
convertToCharacter(convertToDecimal(flipBits(con
vertToBinary(convertToASCII(character)))))

  RETURN decodedMessage
```

```
FUNCTION convertToASCII(character):

  RETURN ASCII value of character


FUNCTION convertToBinary(decimalValue):

  RETURN binary representation of decimalValue


FUNCTION flipBits(binaryValue):

  RETURN flipped binaryValue


FUNCTION convertToDecimal(binaryValue):

  RETURN decimal representation of binaryValue


FUNCTION convertToCharacter(decimalValue):

  RETURN character corresponding to
decimalValue
```

III. *what type of attack can be detected on this encryption and decryption method:*

In our Encryption/Decryption method each character in the plaintext is converted to its ASCII value, and then its binary representation is flipped (0s become 1s and 1s become 0s) as it's called the COMPLEMENT . The flipped binary is then converted back to decimal and mapped to a character.

This Encryption/Decryption method it might be not secure against modern cryptographic attacks like :

- Frequency Analysis: The binary flip cipher does not change the frequency distribution of characters in the plaintext. An attacker can analyze the frequency of characters in the encrypted message and compare it to the expected frequency distribution of characters in the language being used. This can provide clues about the original message and help break the encryption.

- Brute Force Attack: the binary flip cipher only about flipping the binary representation of each character, an attacker can try all possible combinations of flipping and mapping it to decrypt the message.

Binary Flip Cipher

V. *what is the strong and week point in provided method ?*
Since the method based on the binary flip cipher has both
strong and weak points we will discuss it in the team opinion:

• Strong Points:
1. Non-reversible:
   The encryption process in the binary flip cipher is nonreversible without
   knowledge of the specific flipping operation. This can provide a minimal level of
   confidentiality against the attacker, by using our Encryption/Decryption method
   we can say that we make the life harder for the attackers.

2. Simplicity:
   The binary flip cipher is a straightforward encryption method that is easy to
   understand and implement.

3. Obscurity:
   The flipping operation in the binary flip cipher adds an extra layer of obscurity to
   the ciphertext.

4. Speed:
   the binary flip cipher can encrypt and decrypt messages relatively quickly. It does
   not involve complex calculations, making it efficient in terms of runtime.
   However, The encryption and decryption processes have linear complexity $O(n)$,
   where n is the length of the input message.

• Weak Points:
1. Limited Character Set:
   The binary flip cipher only works with characters in the ASCII range, which
   limits its usability and applicability in scenarios where a broader range of
   characters, such as non-English alphabets or special characters, is required.

VI. Reference:
- https://www.freecodecamp.org/news/big-o-notation-why-it-matters-and-why-it-doesnt-1674cfa8a23c/

VII. Task distribution:

	Code writing	Document editing	Presentation
وفاء العواضي	●		
رزان المالكي	●		
رتاج باعقيل		●	
صباح العنزي		●	
مرح المقاطي			●