# **Лабораторна робота № 3**

##### **Використання шифрування у програмних засобах**

##### **захисту інформаційних систем.**

**Мета роботи:** ознайомити студента з основними підходами до організації інформаційної безпеки, з основними методами шифрування інформації. Набути знань із реалізації методів шифрування інформації у вигляді програмних модулів.

**Завдання:** Освоїти основні методи шифрування інформації, сформувати структуру та реалізувати модуль шифрування для захисту інформаційної системи використовуючи шифр Цезаря та XOR

**1.** **Опис методу реалізації завдання**

**Шифр Цезаря** — симетричний алгоритм шифрування підстановками. Використовувався римським імператором Юлієм Цезарем для приватного листування. Принцип дії полягає в тому, щоб циклічно зсунути алфавіт, а ключ — це кількість літер, на які робиться зсув.

Шифр Цезаря має замало ключів — на одиницю менше, ніж літер в абетці. Тому перебрати усі ключі не складає особливої роботи. Дешифрування з одним з ключів дасть нам вірний відкритий текст.

**Шифр XOR** — алгоритм шифрування, який як ключ використовує ключове слово та може бути записаний формулою Ci = Pi XOR Kj. де Kj - j-та літера ключового слова представлена в кодуванні ASCII. XOR — логічна та бітова операція, що приймає значення "істина" тоді і лише тоді коли значення «істина» має рівно один з її операндів.

**2.** **Алгоритм реалізації завдання**

**Шифр Цезаря** Якщо зіставити кожному символу алфавіту його порядковий номер (нумеруючи з 0), то шифрування і дешифрування можна виразити формулами:



  
де x — порядковий номер символу відкритого тексту, y — порядковий номер символу шифрованого тексту, n — потужність алфавіту, а k— ключ.

**Шифр XOR** використовує ключове слово та може бути записаний формулою Ci = Pi XOR Kj. де Kj - j-та літера ключового слова представлена в кодуванні ASCII.

##### **3. Лістинг програми**

Лістинг 1. Шифр Цезаря

class Caesar

attr\_reader :offset

LOW\_RU\_ALPHABET = Array('а'..'я')

UP\_RU\_ALPHABET = Array('А'..'Я')

LOW\_EN\_ALPHABET = Array('a'..'z')

UP\_EN\_ALPHABET = Array('A'..'Z')

def initialize(offset = 8)

@offset = offset

@encryptor = create\_encryption\_table(offset)

@decryptor = create\_encryption\_table(-offset)

end

def offset=(offset)

@offset = offset

@encryptor = create\_encryption\_table(offset)

@decryptor = create\_encryption\_table(-offset)

end

def encode(text)

text.chars.map { |c| @encryptor.fetch(c, c) }.join

end

def decode(text)

text.chars.map { |c| @decryptor.fetch(c, c) }.join

end

private

def create\_encryption\_table(offset)

[

Hash[LOW\_RU\_ALPHABET.zip(LOW\_RU\_ALPHABET.rotate(offset))],

Hash[UP\_RU\_ALPHABET.zip(UP\_RU\_ALPHABET.rotate(offset))],

Hash[LOW\_EN\_ALPHABET.zip(LOW\_EN\_ALPHABET.rotate(offset))],

Hash[UP\_EN\_ALPHABET.zip(UP\_EN\_ALPHABET.rotate(offset))]

].inject(&:merge)

end

end

Лістинг 2. Шифрування XOR

class XOR

attr\_accessor :key

def initialize(key)

@key = key.codepoints

end

def encrypt(text)

text.codepoints.map.with\_index do |c, i|

(c ^ @key[i % @key.size]).chr

end.join

end

end

##### **4. Результати виконання програми**

##### Рис 1. Шифр Цезаря

##### 

##### Рис 2. Шифр XOR

##### 

##### **5. Висновок**

В даній лабораторній роботі я ознайомився з основними підходами до організації інформаційної безпеки, з основними методами шифрування інформації. Набув знань із реалізації методів шифрування інформації у вигляді програмних модулів.

Освоїв основні методи шифрування інформації, на прикладі алгоритму шифрів Цезаря та XOR, сформував структуру та реалізував модулі шифрування для вищезгаданих алгоритмів.