Университет ИТМО

Факультет программной инженерии и компьютерной техники

Информационная безопасность

Лабораторная работа 1.1

Выполнил:

Соловьев П.В.

Преподаватель:

Маркина Т.А.

Санкт-Петербург

2023

Содержание

1. Цель работы

Изучение основных принципов шифрования
информации, знакомство с широко известными алгоритмами шифрования, приобретение навыков их программной реализации

2. Задание

Реализовать в программе шифрование и дешифрацию файла с использованием аффинной криптосистемы. Провести частотный анализ зашифрованного файла, осуществляя проверку по файлу с набором ключевых слов.

3. Исходный код программы

utils.py

```
literal_ranges = [(1040, 1106), (32, 65), (91, 97), (123, 127), (9, 11)]

def init_alphabet():
    global literal_ranges

    alphabet = []
    literal_to_index = dict()

    for pair in literal_ranges:
        for i in range(pair[0], pair[1]):
            alphabet.append(chr(i))
            literal_to_index[chr(i)] = len(alphabet) - 1

    return alphabet, literal_to_index


def extended_gcd(a, b):
    old_r, r = a, b
    old_s, s = 1, 0
    old_t, t = 0, 1

    while r != 0:
        quotient = old_r // r
        old_r, r = r, old_r - quotient * r
        old_s, s = s, old_s - quotient * s
        old_t, t = t, old_t - quotient * t

    return old_s, old_t


if __name__ == "__main__":
    alphabet, literal_to_index = init_alphabet()

    print("Размер алфавита:", len(alphabet), "\n")
    print("--- Алфавит ---\n", " ".join(alphabet))
```

encrypt.py

```
import sys
from utils import init_alphabet
from math import gcd

def encrypt(msg, alphabet, literal_to_index, a, b):
    encrypted_msg = []
    for ch in msg:
        x = (a * literal_to_index[ch] + b) % len(alphabet)
        encrypted_msg.append(alphabet[x])

    return ''.join(encrypted_msg)


if __name__ == "__main__":
    alphabet, literal_to_index = init_alphabet()

    inp, out, a, b = sys.argv[1], sys.argv[2], int(sys.argv[3]), int(sys.argv[4])

    m = len(alphabet)
    if (gcd(a, m) != 1):
        raise RuntimeError("a и m должны быть взаимно простыми")

    with open(inp, encoding='utf-8') as f:
        msg = f.read()
        encrypted_msg = encrypt(msg, alphabet, literal_to_index, a, b)

    with open(out, 'w', encoding='utf-8') as f:
        f.write(encrypted_msg)
```

decrypt.py

```
import sys
from utils import extended_gcd, init_alphabet

def decrypt(msg, alphabet, literal_to_index, a, b):
    a1, _ = extended_gcd(a, len(alphabet))

    decrypted_msg = []
    for ch in msg:
        x = (a1 * (literal_to_index[ch] - b)) % len(alphabet)
        decrypted_msg.append(alphabet[x])

    return ''.join(decrypted_msg)


if __name__ == "__main__":
    alphabet, literal_to_index = init_alphabet()

    inp, out, a, b = sys.argv[1], sys.argv[2], int(sys.argv[3]), int(sys.argv[4])
```

```
with open(inp, encoding='utf-8') as f:
    msg = f.read()
    encrypted_msg = decrypt(msg, alphabet, literal_to_index, a, b)

with open(out, 'w', encoding='utf-8') as f:
    f.write(encrypted_msg)
```

freq_analysis.py

```
import sys
from collections import Counter

if __name__ == "__main__":
    with open(sys.argv[1], encoding='utf-8') as f:
        msg = f.read()
        stat = Counter(list(msg))

        for i in stat:
            ch = i
            if i == "\t":
                ch = "\\t"
            if i == "\n":
                ch = "\\n"

            print("{}: {}".format(ch, stat[ch]))
```

4. Результат исполнения программы

4.1. Исходный текст

```
[callmepedro@manjaro-linux-os information-security-1]$ cat text/msg
Учение, проповедующее равнодушие к богатству, к удобствам жизни, презрение к страдани
ям и смерти, совсем непонятно для громадного большинства, так как это большинство ник
огда не знало ни богатство, ни удобств в жизни; а презирать страдания значило бы для
него презирать самую жизнь, так как всё существо человека состоит из ощущений голода,
 холода, обид, потерь и гамлетовского страха перед смертью. В этих ощущениях вся жизн
ь; ею можно тяготиться, ненавидеть её, но не презирать.[callmepedro@manjaro-linux-os
information-security-1]$
```

4.2. Алфавит и его размер

```
information-security-1]$ python utils.py
Размер алфавита: 111

--- Алфавит ---
 А Б В Г Д Е Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я а б в г д е ж з и й
к л м н о п р с т у ф х ц ч ш щ ъ ы ь э ю я è ё   ! " # $ % & ' ( ) * + , - . / 0 1 2
 3 4 5 6 7 8 9 : ; < = > ? @ [ \ ] ^ _ ` { | } ~
```

4.3. Шифрование

```
[callmepedro@manjaro-linux-os information-security-1]$ python encrypt.py text/msg tex
t/decrypted 13 42
[callmepedro@manjaro-linux-os information-security-1]$ cat text/decrypted
!9-&3-щМ@А3@3и- з%Ж--МАОи&3 з`3-МбМЫ3хОЪНЪизщМбМз ЗЫНЪиОыМ:3{&3щМ@А-{А-&3-МбМНЪАО О&3
2ыМ3МНы-АЪ3щМН3иН-ыМ&-@3&2Ъ&3М о2МхА3ыО &3х3МЫ3он`3&НЪиОщМЪОбМбОбМъЪ3МЫ3он`3&НЪи3М&3б
3х ОМ&-М{&Оо3М&3МЫ3хОЪНЪи3щМ&3Мз ЗЫНЪиМиМ:3{&3ЮМОМ@А-{3АОЪнМНЪАО О&32М{&О93о3МЫаМ о2М
&-х3М@А-{3АОЪнМНОыз%М:3{&нщМЪОбМбОбМиН
МНзЖ-НЪи3М9-о3и-бОМН3НЪ33ЪМ3{М3ЖзЖ-&3ФМх3о3 ОщМё3о3 ОщМ3ЫЗ щМ@3Ъ-АнМ3МхОыо-Ъ3иНб3х3МН
ЬАОёОМ@-А- МНы-АЪн%1М"МъЪ3ёМ3ЖзЖ-&32ёМиН2М:3{&нЮМ-%Мы3:&3МЪ2х3Ъ3ЪнН2щМ&-&Оиз -ЪнМ-
щМ&3М&-М@А-{3АОЪн1[callmepedro@manjaro-linux-os information-security-1]$
```

4.4. Дешифрование

```
[callmepedro@manjaro-linux-os information-security-1]$ python decrypt.py text/decrypt
ed text/encrypted 13 42
[callmepedro@manjaro-linux-os information-security-1]$ cat text/encrypted
Учение, проповедующее равнодушие к богатству, к удобствам жизни, презрение к страдани
ям и смерти, совсем непонятно для громадного большинства, так как это большинство ник
огда не знало ни богатство, ни удобств в жизни; а презирать страдания значило бы для
него презирать самую жизнь, так как всё существо человека состоит из ощущений голода,
 холода, обид, потерь и гамлетовского страха перед смертью. В этих ощущениях вся жизн
ь; ею можно тяготиться, ненавидеть её, но не презирать.[callmepedro@manjaro-linux-os
```

4.5. Частотный анализ

Исходный текст	Зашифрованный текст
у: 1 ч: 3 е: 32 н: 29 и: 31 ,: 12 : 70 п: 9 р: 18 о: 41 в: 16 д: 15 у: 9 ю: 4 щ: 6 а: 29 ш: 3 к: 12 б: 8 г: 10 т: 30 с: 22 м: 9 ж: 5 з: 11 я: 9 л: 10 ь: 11 э: 2 ;: 2 ы: 1 ё: 2 й: 1 х: 4 .: 2 В: 1	!: 1 9: 3 -: 32 &: 29 З: 31 щ: 12 М: 70 @: 9 А: 18 З: 41 и: 16 : 15 з: 9 %: 4 ж: 6 О: 29 `: 3 б: 12 ы: 8 х: 10 ъ: 30 Н: 22 ы: 9 ::: 5 {: 11 2: 9 о: 10 н: 11 ъ: 2 Ю: 2 а: 1 \n: 0 ф: 1 ё: 4 1: 2 ": 1

5. Вывод

В ходе выполнения лабораторной работы я изучил принцип работы афинного шифра, реализовал набор программ для шифрования и дешифрования с помощью изученного метода, а также исследовал его криптографические свойства.