МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

Кафедра кібербезпеки

**Дисципліна “Системи та засоби криптоаналізу”**

**Звіт до лабораторної роботи №1**

на тему “Дослідження криптоаналітичних атак на шифр Цезаря. Частина 1**”**

Студент Борщ Дмитро Олександрович

Варіант № 1

Група КБ-01

Перевірила Лаврик Т.В

**Суми 2022**

**ЗВІТ**

1. (5 б.) Програмний код, який шифрує введену з клавіатури *українською мовою* інформацію за допомогою шифру Цезаря:

Текст програми

alphabet = [

'а', 'б', 'в', 'г', 'ґ', 'д', 'е', 'є', 'ж', 'з', 'и', 'і', 'ї', 'й',

'к', 'л', 'м', 'н', 'о', 'п', 'р', 'с', 'т', 'у', 'ф', 'х', 'ц', 'ч',

'ш', 'щ', 'ь', 'ю', 'я', ' '

]

def caesar(string, key):

output = ""

for i in string:

index = (alphabet.index(i)+key)%len(alphabet)

output += alphabet[index]

return output

Подана вище функція реалізовує шифрування алгоритмом Цезаря з використанням вказаного алфавіту. Також було створено головну функцію програми, яка обробляє отримані аргументи.

def main(args=sys.argv):

# Using file as input source

if "--file" in args:

try:

fileName = args[args.index("--file")+1]

except:

print("ERROR, no file specified!")

return 0

try:

f = open(fileName, "r")

inputText = ''.join(f.read())

except:

print("ERROR, can`t open file!")

return 0

# Using plain text as input source

else:

inputText = input("Enter input text: ")

# Taking key from args

try:

key = int(args[args.index("--key")+1])

except:

if "--brute" not in args:

print("ERROR, no key specified!")

return 0

else: pass

# Choosing an option

if "--encrypt" in args:

print(f"Encrypted text is:\n{caesar(inputText, key)}")

elif "--decrypt" in args:

print(f"Decrypted text is:\n{uncaesar(inputText, key)}")

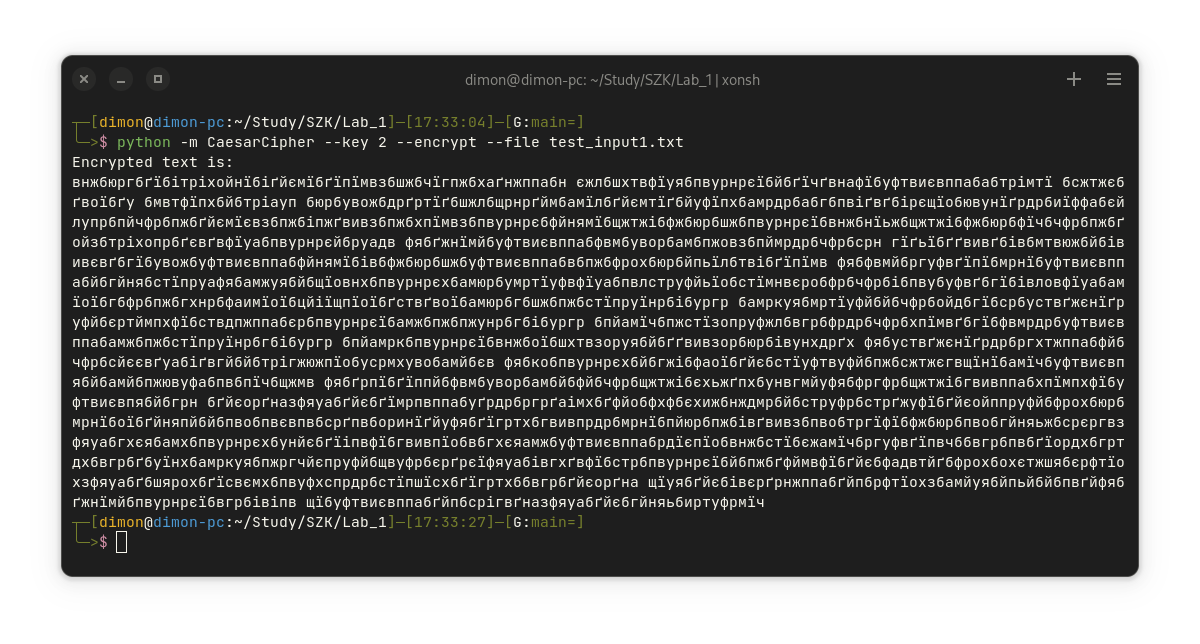
elif "--brute" in args:

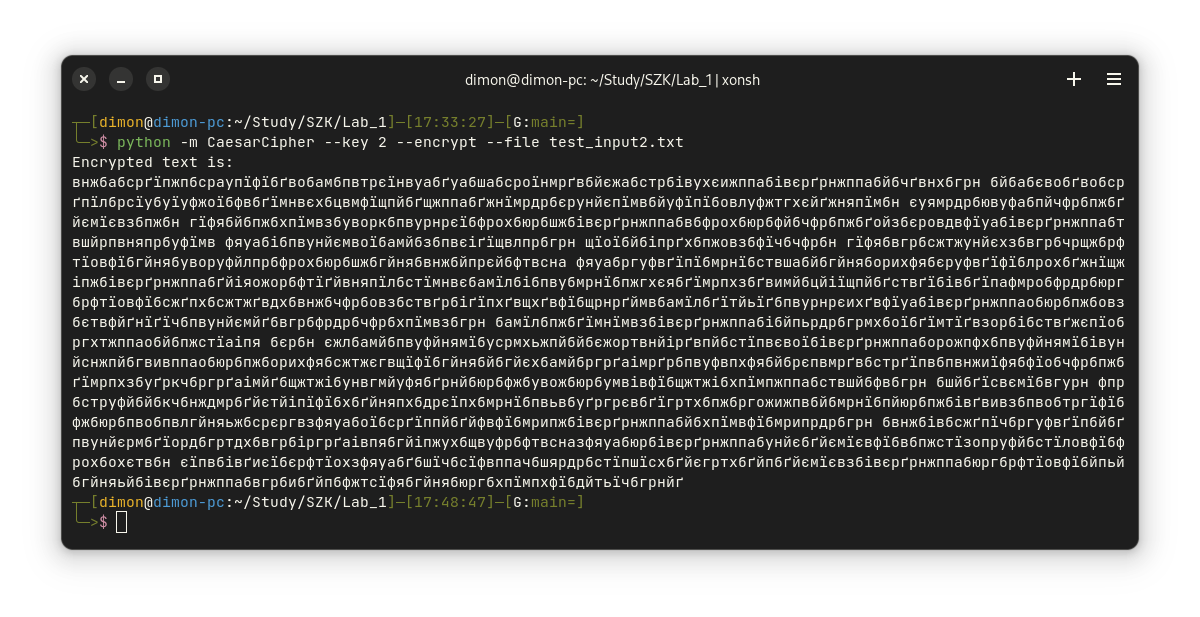
print("Brute forced variants are:\n")

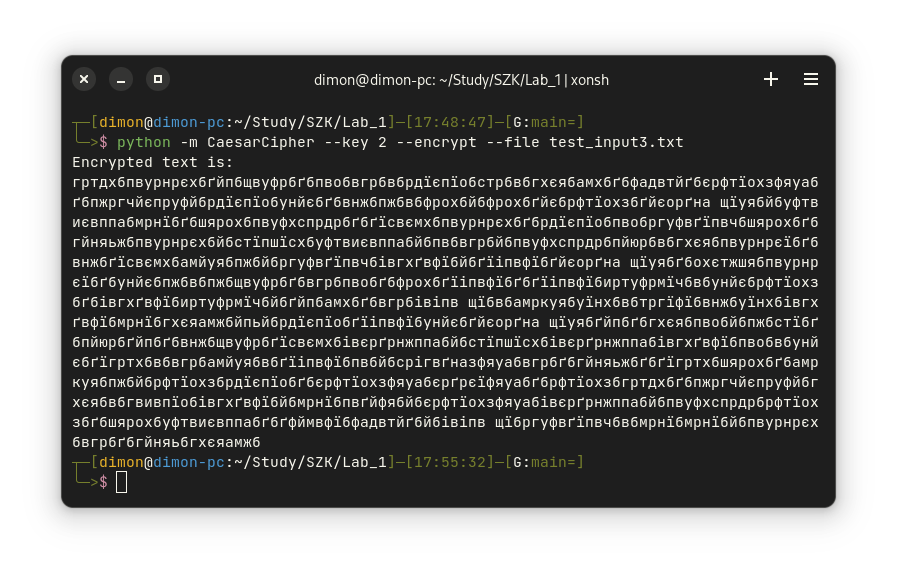
bruteForce(inputText)

return 0

Скріншоти з результатами роботи програми (мінімум 3 різні тексти)

Рис. 1 — Перший приклад роботи програми.

Рис. 2 — Другий приклад роботи програми.

Рис. 3 — Третій приклад роботи програми.

1. (3 б.) Блок-схема алгоритму реалізації методу повного перебору:

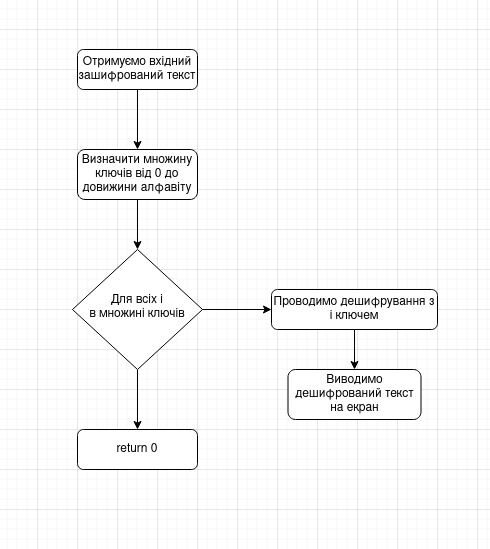


Рис. 4 — Блок-схема алгоритму повного перебору.

1. (5 б.) Програмний код методу повного перебору.

def uncaesar(string, key):

output = ""

for i in string:

index = alphabet.index(i)-key

while index < 0: index += len(alphabet)

output += alphabet[index]

return output

def bruteForce(string):

for key in range(len(alphabet)):

print(

f"Result with key {key}\n\n",

uncaesar(string, key),

"\n"

)

Скріншоти з результатами роботи програми (мінімум 3 різні шифротексти)



Рис. 5 — Перший приклад повного перебору.

Рис. 6 — Другий приклад повного перебору.

Рис. 7 — Третій приклад повного перебору.