

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

“КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ

імені ІГОРЯ СІКОРСЬКОГО”

Факультет прикладної математики

Кафедра програмного забезпечення комп’ютерних систем

**Лабораторна робота №** 1

з дисципліни “ Програмні засоби захисту інформації ”

тема “Загальні принципи побудови симетричних криптосистем. Шифр Лестера Хілла.”

| Виконав  студент 4 курсу  групи КП-91  Власюк Сергій Петрович  (*прізвище, ім’я, по батькові*)  варіант №3 |  | Зарахована  “05” “квітня” 2023 р.  викладачем Онай Микола Володимирович (*прізвище, ім’я, по батькові*) |
| --- | --- | --- |

| Штрафні бали:   | **Термін здачі (01.11.2018)** | **Оформлення звіту (–2)** | | --- | --- | |  |  | | Нараховані бали:   | **Відповіді на теор. питання + коректність (3+3)** | **Відповіді на прогр. питання (4)** | | --- | --- | |  |  | | Сумарний бал:   |  | | --- | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

Київ 2018

**Мета роботи** – опанувати методи шифрування даних за допомогою

моноалфавітних та поліалфавітних шифрів заміни.

**Завдання для виконання**

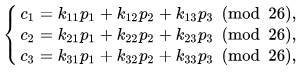
Розробити програму на будь-якій мові програмування, яка буде

реалізувати шифрування та дешифрування даних за допомогою алгоритму Лестера Хілла.

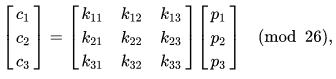
**Математичне підґрунтя**

Шифр Хілла є поліграмним шифром, який може використовувати більші блоки за допомогою лінійної алгебри. Кожна буква алфавіту містить число за модулем 26. Для латинського алфавіту часто використовується простейша схема: A = 0, B = 1, …, Z = 25, але це не є суттєвою властивістю шифру. Блок з n букв розглядається як n-вимірний вектор і множиться по модулю 26 на матрицю розміром n×n. Якщо в якості основи модуля використовується число більше, ніж 26, то можна використовувати іншу числову схему для розміщення букв чисел і додати пробіли та знаки пунктуації. Елементи матриці є ключем. Матрица повинна бути оборотна, щоб була можлива операція розшифрування.

Для n = 3 систем може бути описано так:



або в матричній формі:



У загальному випадку алгоритм шифрування може бути виражений у наступному вигляді

Шифрування: 

Дешифрування: 

**Код програми**

import numpy

def create\_matrix\_from(key):

m=[[0] \* 3 for i in range(3)]

for i in range(3):

for j in range(3):

m[i][j] = ord(key[3\*i+j]) % 65

return m

def create\_matrix():

m=[[17, 17, 5], [21, 18, 21], [2, 2, 19]]

return m

def encrypt(P, K):

C=[0,0,0]

C[0] = (K[0][0]\*P[0] + K[0][1]\*P[1] + K[0][2]\*P[2]) % 26

C[1] = (K[1][0]\*P[0] + K[1][1]\*P[1] + K[1][2]\*P[2]) % 26

C[2] = (K[2][0]\*P[0] + K[2][1]\*P[1] + K[2][2]\*P[2]) % 26

return C

def Hill(message, K):

cipher\_text = []

for i in range(int(len(message) / 3)):

P=[0, 0, 0]

for j in range(3):

P[j] = ord(message[j]) % 65

message = message[3:]

#Encript three letters

C = encrypt(P,K)

for j in range(3):

cipher\_text.append(chr(C[j] + 65))

return "".join(cipher\_text)

def MatrixInverse(K):

det = int(numpy.linalg.det(K))

det\_multiplicative\_inverse = pow(det, -1, 26)

K\_inv = [[0] \* 3 for i in range(3)]

for i in range(3):

for j in range(3):

Dji = K

Dji = numpy.delete(Dji, (j), axis=0)

Dji = numpy.delete(Dji, (i), axis=1)

det = Dji[0][0]\*Dji[1][1] - Dji[0][1]\*Dji[1][0]

K\_inv[i][j] = (det\_multiplicative\_inverse \* pow(-1,i+j) \* det) % 26

return K\_inv

if \_\_name\_\_ == "\_\_main\_\_":

message = "MYSECRETMESSAGE"

key = "RRFVSVACT"

K = create\_matrix\_from(key)

print(K)

# C = P \* K mod 26

cipher\_text = Hill(message, K)

print ('Cipher text: ', cipher\_text)

# P = C \* K^-1 mod 26

K\_inv = MatrixInverse(K)

plain\_text = Hill(cipher\_text, K\_inv)

print ('Plain text: ', plain\_text)

**Результати роботи програми**

****

Де перший рядок це матриця ключ.