МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
Кафедра кібербезпеки

Дисципліна “Системи та засоби криптоаналізу”

Звіт до лабораторної роботи № 7-8

на тему **“ Поліграмний шифр Хілла і дослідження методів його криптоаналізу. Частина 1-2. ”**

Студент	Борщ Д.О.
Варіант	№ 1
Група	КБ-01
Перевірила	Лаврик Т.В

Суми 2023

ЗВІТ

Завдання (10 б.). Здійснити шифрування і розшифрування тексту, використовуючи шифр Хілла.

Для шифрування вибрати самостійно україномовний текст/

У якості ключа взяти власне прізвище та ім’я (довжина має бути кратна числу 3), m = 3 .

У звіті подати детально всі дії, що виконуються під час шифрування та розшифрування. Результат може супроводжуватися програмною реалізацією.

Результати роботи

Частина 1. Зашифрувати текст, використовуючи шифр Хілла для m=3.

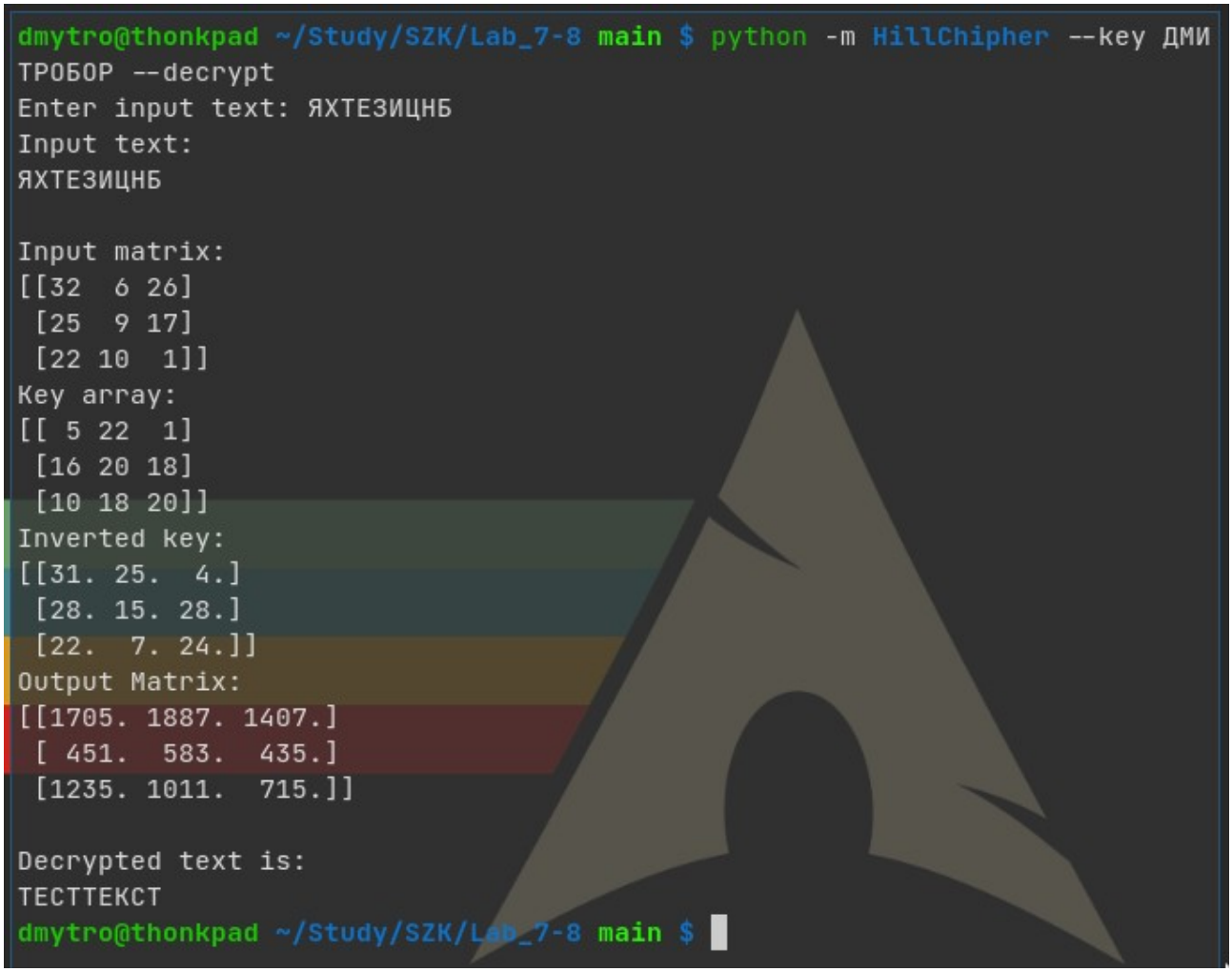
```
dmytro@thonkpad ~/Study/SZK/Lab_7-8 main $ python -m HillChipher --key ДМИ
ТРОБОР --encrypt
Enter input text: ТЕСТТЕКСТ
Input text:
ТЕСТТЕКСТ

Input matrix:
[[22 22 14]
 [ 6 22 21]
 [21  6 22]]
Key array:
[[ 5 22  1]
 [16 20 18]
 [10 18 20]]
Output Matrix:
[[ 263  850  748]
 [ 600  900  736]
 [ 554 1040  958]]

Encrypted text is:
ЯХТЕЗИЦНБ
dmytro@thonkpad ~/Study/SZK/Lab_7-8 main $
```

Результат шифрування

Частина 2. Розшифрувати текст, використовуючи шифр Хілла для m=3.



Приклад роботи з великим текстом: