МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний університет «Чернігівська політехніка»

Навчально-науковий інститут електроних та інформаційних технологій

Кафедра кібербезпеки та математичного моделювання

**ЗВІТ**

про виконання лабораторної роботи

з дисципліни «Основи криптографічного захисту інформації»

Виконав: здобувач 3 курсу, групи КБ-221 Регент Анастасія

Перевірив: Шелест Михайло Євгенович

НУ «Чернігівська політехніка» 2024

Лабораторна робота № 1

Класичні шифри

Мета: ознайомитися з різними класичними шифрами (підстановки, перестановки), їх властивостями та методами дешифрування.

Теоретичні відомості

Хід роботи

Завдання № 1

Дешифруйте повідомлення, зашифроване варіацією шифру Цезаря. Користуйтеся операцією ROT13 з [CyberChef](https://gchq.github.io/CyberChef) для швидкого перебору можливих ключів шифру Цезаря.

Шифртекст:

CDBCGT DIOZGGDBZIO DIYDQDYPVGN DIOZMZNOZY DI XDXVYV OCDMOT OCMZZ UZMJ JIZ

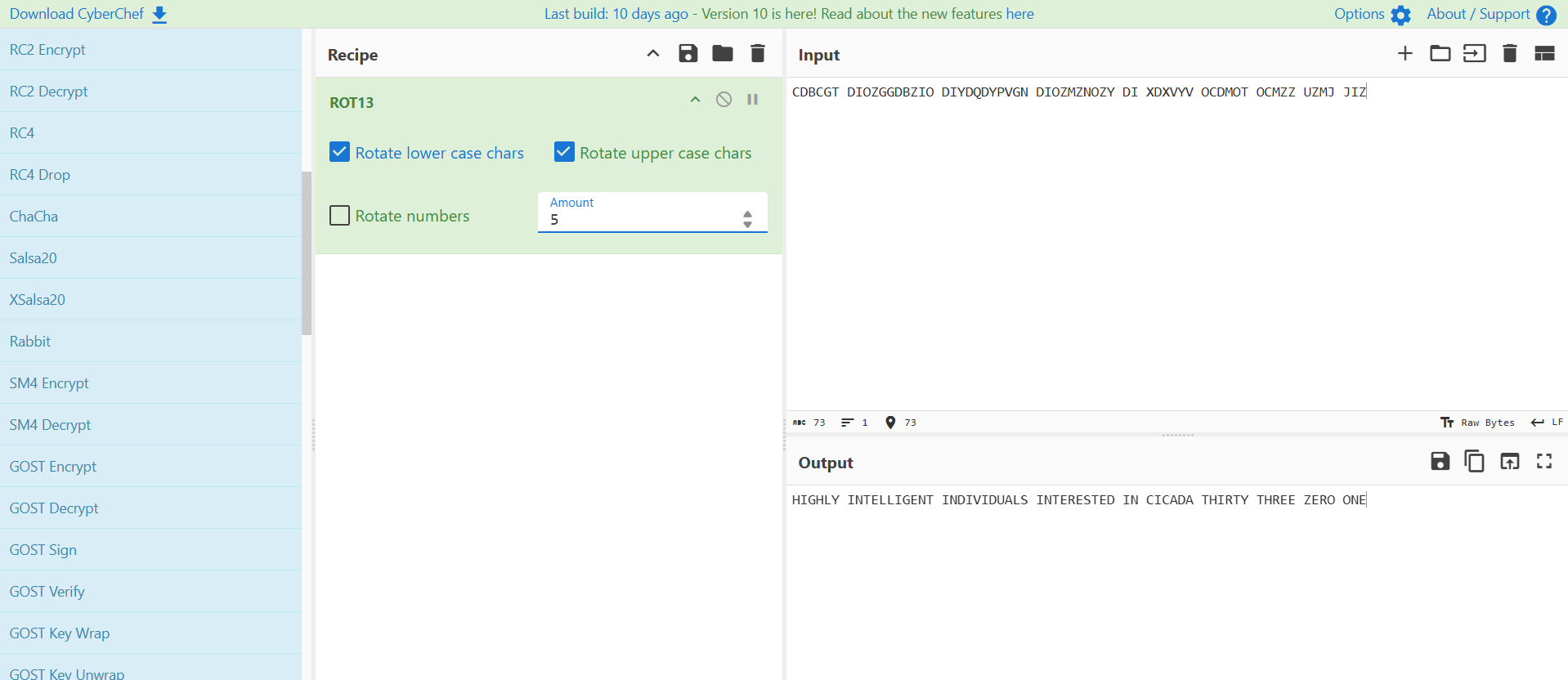


Рисунок 1 – Результат завдання № 1

Завдання № 2

Розшифруйте повідомлення з шифрмашини Енігми моделі М3 (3 ротори). Повідомлення було зашифроване 23-го числа згідно з кодовою книгою, без використання індивідуального ключа (message key). Для зашифрування повідомлення використовувалася третя ключова група цього дня.

Шифртекст:

GOKDM GVDYY ZOCOQ DUAFE QVXCC HCQTW UHXLG GOBGX BXSNZ FZEYX RSTXZ BPZVI LTG

Для роботи можна скористатися моделлю за посиланням: <https://cryptii.com/>

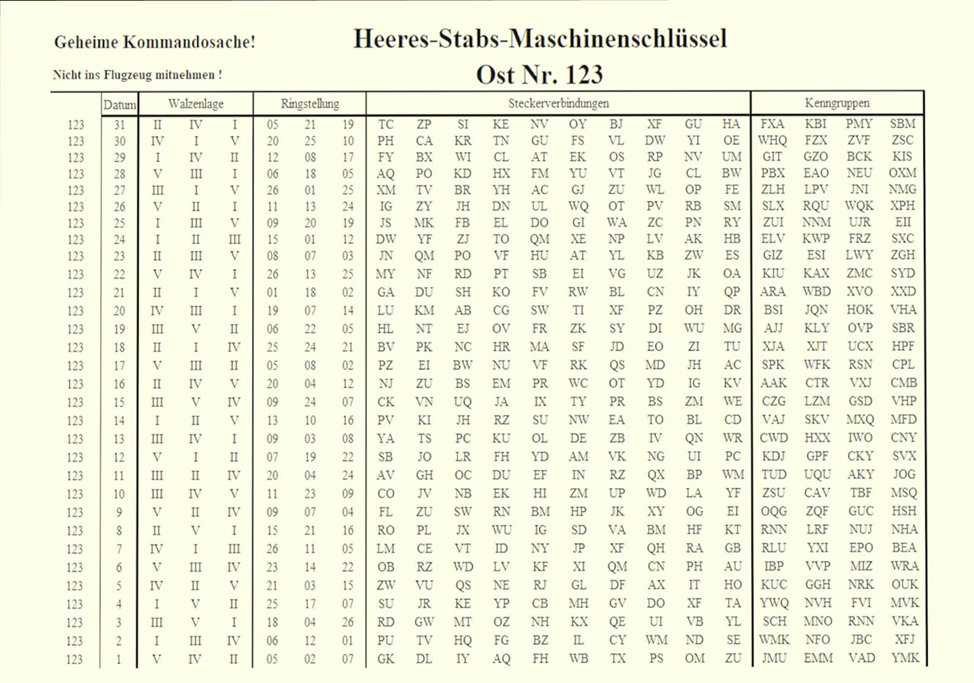


Рисунок 2 – Кодовий лист

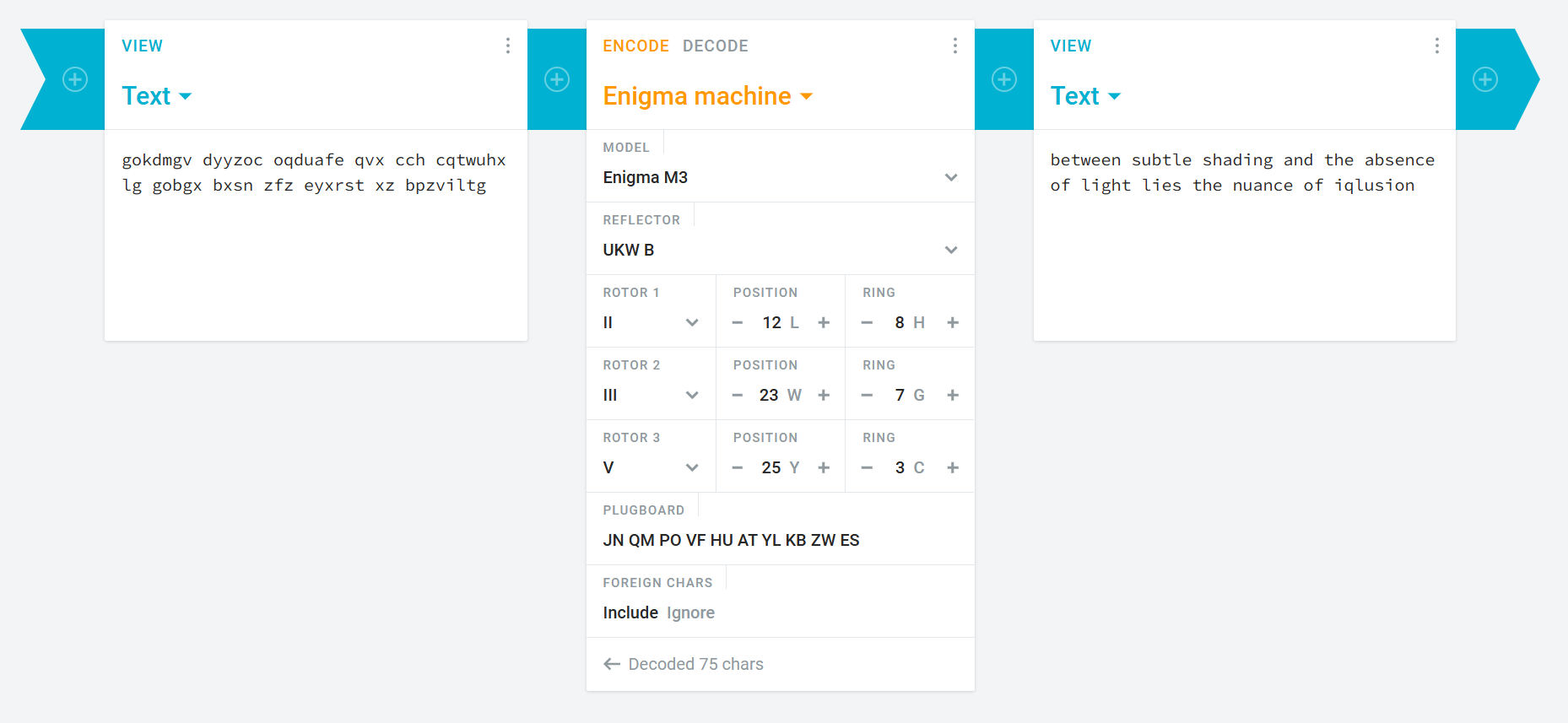


Рисунок 3 – Результат

Завдання № 3

Дешифруйте повідомлення зашифроване шифром Віженера. Ключем є назва об'єкту, на якому зображено повідомлення із завдання 2 (якщо не впевненні, запитайте Джима Санборна або Вільяма Вебстера :) ).

Шифртекст:

SK UPL HGDRJAR WFFZQXUZW RFUH MVSD GMHLWTVV ? RWXM MCVB IAS WKIRWL ASQECIBQ XSVJS Q HZO ZLUHFEKKGDG KSC XYIASJOU YCW HJKEQBBHLOU SCWSJQISJGR LY RL JGYFYNL AHQSDZMC Q RGOJ JPGUDOP ICHK SLFSI MVAC ? KFTR GZYLJS BHK LLPXXR GEK RWXFW CFKTPVWBV V LAC CXFUH MVW OOYRM ZGMRRXHB ? GXCW LP HZSJ UPL VAC CYHM AWCJYVX L LRZPIR SAQYR SXUJOVQ UBTLI JCKXB ESESIXG KSO NDBBL PZTT LSUYEBH GCJDY QTOSFDP QTOSF NVEGXSK OZEWM AAXLRTL TGBKW UHIJ CVADGRK GVQI Q ZSIVP IPC

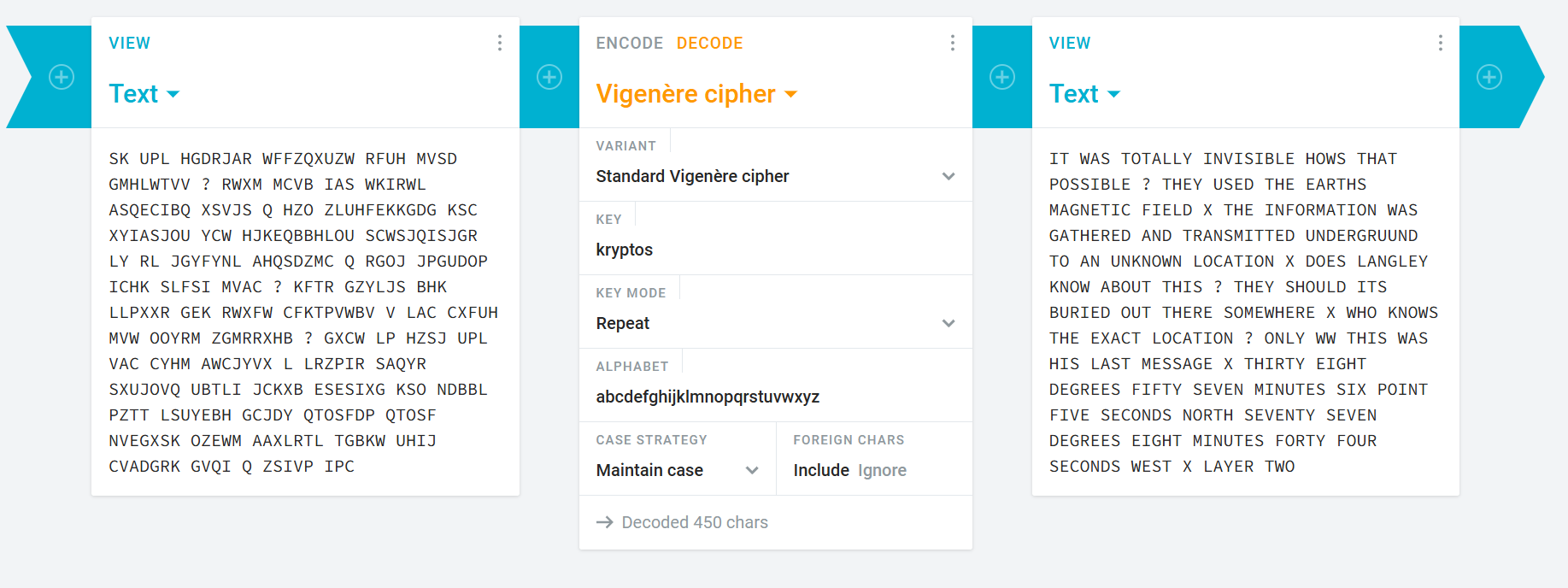


Рисунок 4 – Результат

Завдання № 4

Зашифруйте текст шифрами простої заміни, вертикальною та горизонтальною перестановками, а потім побудуйте гістограми літер. Проаналізуйте відмінність. Дайте числові оцінки отриманим гістограмам (наприклад, хи-квадрат).

Для завдання я обрала італійську фразу: «La vita e bella».

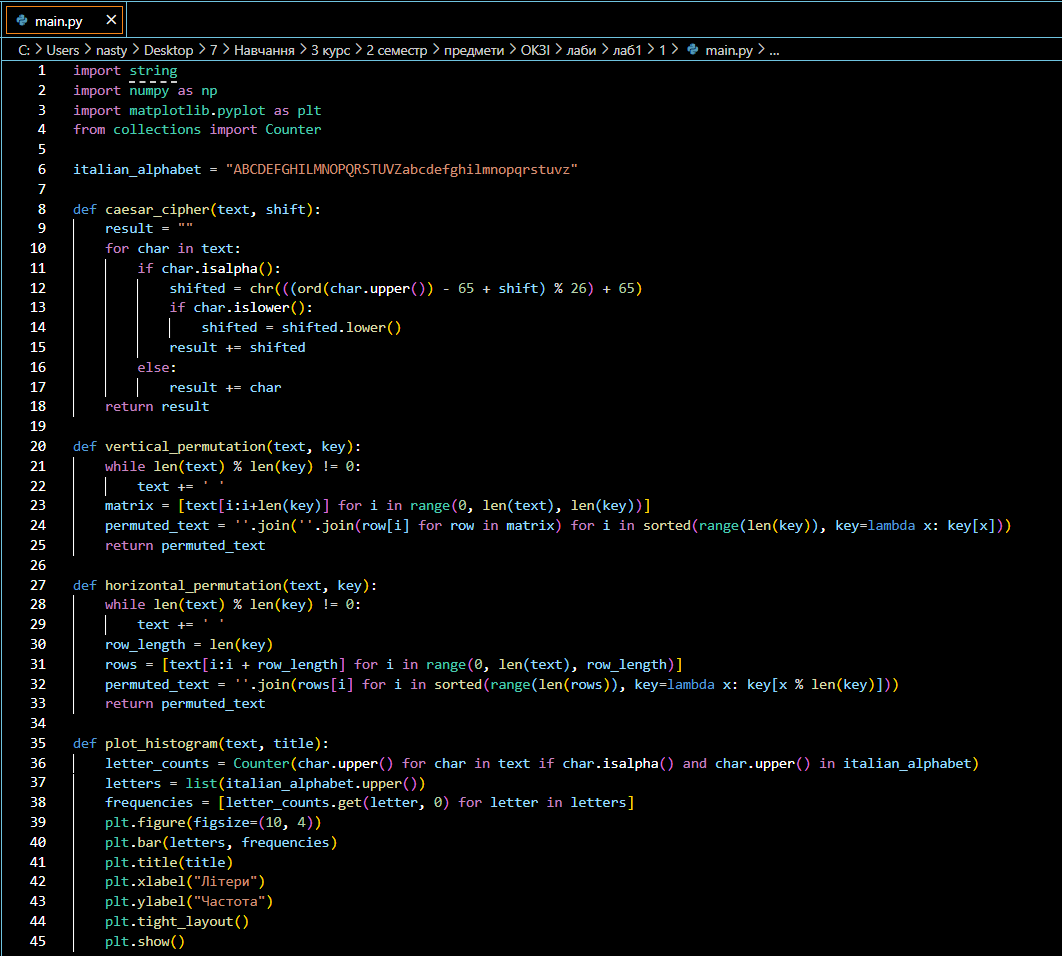


Рисунок 5 – Код 1.1

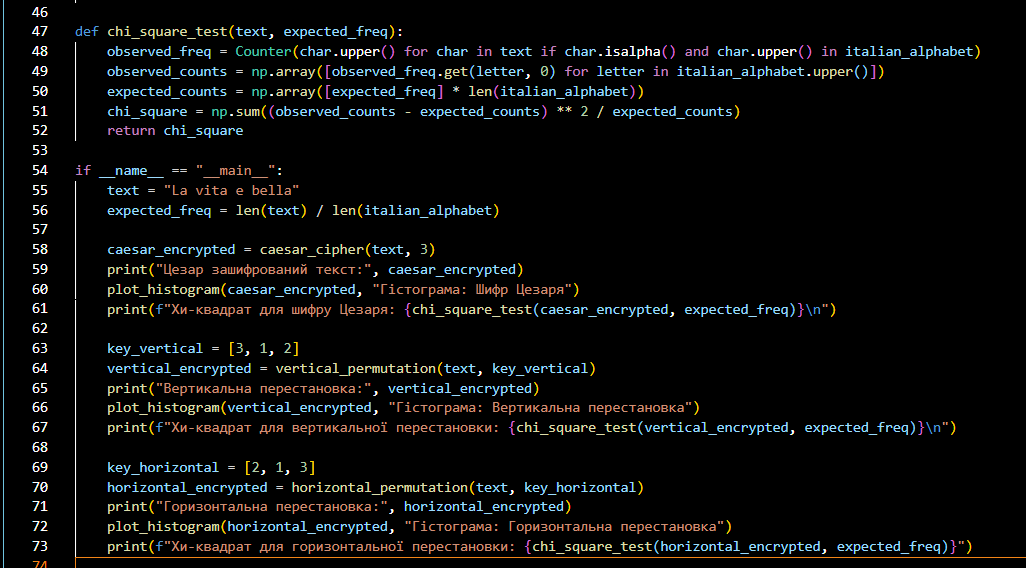


Рисунок 6 – Код 1.2

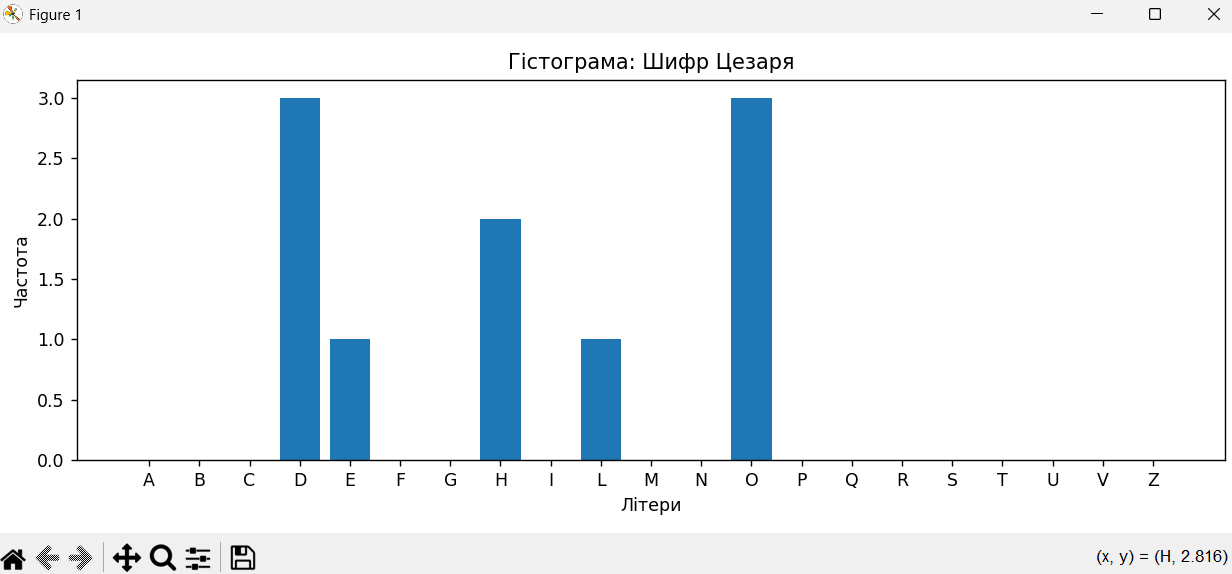


Рисунок 7 – Гістограма: Шифр Цезаря

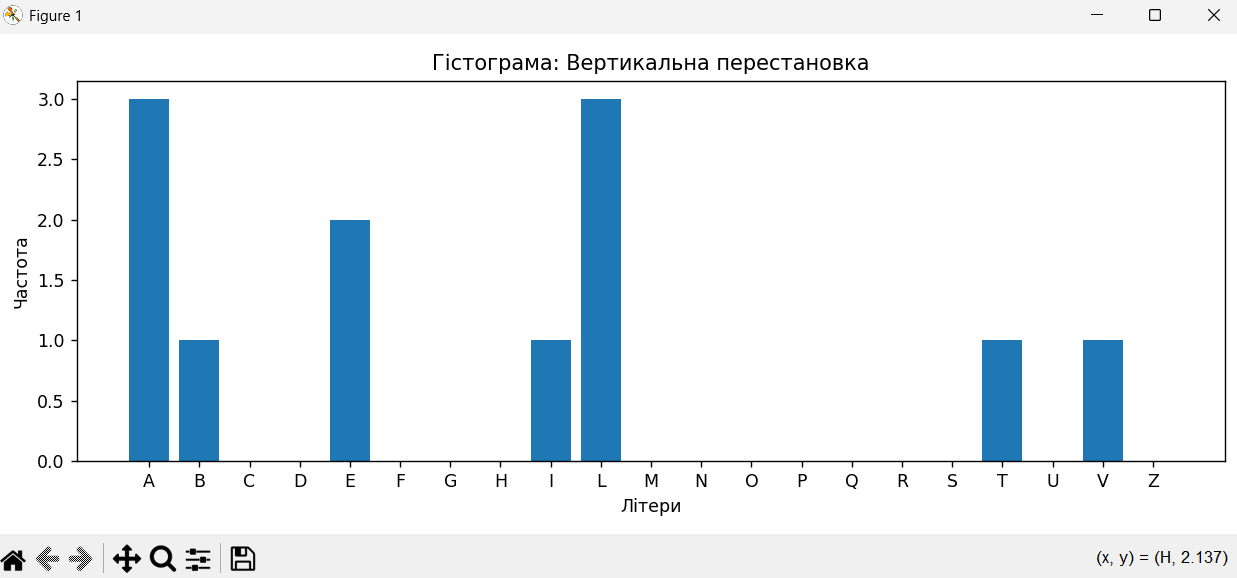


Рисунок 8 – Гістограма: Вертикальна перестановка

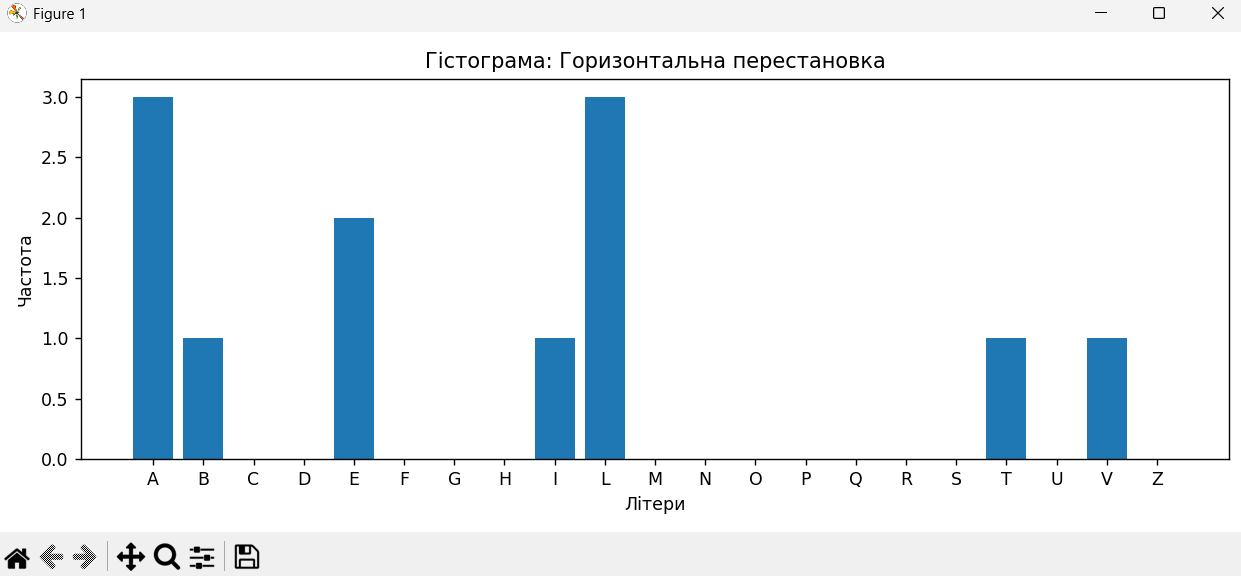


Рисунок 9 – Гістограма: Горизонтальна перестановка

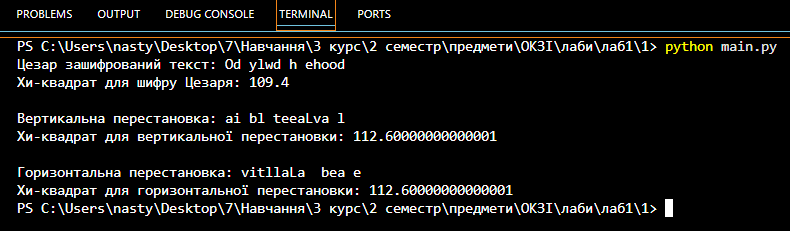


Рисунок 10 – Результат в терміналі

Завдання № 5

Вертикальна перестановка

Зашифрований текст: ТАНР ЦТАИ ЕЗЯІ СНШВ ЕННФ

Умови завдання:

Для зашифрування тексту використано шифр вертикальної перестановки.

Довжина ключа: 5.

У вихідному тексті слова розділяються пробілами (але пробіли видалені при шифруванні).

Питання:

Відновіть початковий текст.

Як виглядає таблиця, яку використовували для шифрування?.

Додаткові рекомендації: намалюйте таблицю з 5 стовпцями, впишіть шифртекст построково, потім переставте стовпці у правильному порядку.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | 1 | 2 | 3 | 4 | 5 |
| 1 | Т | А | Н | Р | Ц |
| 2 | Т | А | И | Е | З |
| 3 | Я | І | С | Н | Ш |
| 4 | В | Е | Н | Н | Ф |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | 3 | 1 | 4 | 5 | 2 |
| 1 | Н | Т | Р | Ц | А |
| 2 | И | Т | Е | З | А |
| 3 | С | Я | Н | Ш | І |
| 4 | Н | В | Н | Ф | Е |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | 3 | 1 | 4 | 2 | 5 |
| 1 | Т | А | Н | Р | Ц |
| 2 | Т | А | И | Е | З |
| 3 | Я | І | С | Н | Ш |
| 4 | В | Е | Н | Н | Ф |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | 1 | 2 | 3 | 4 | 5 |
| 1 | А | Р | Т | Н | Ц |
| 2 | А | Е | Т | И | З |
| 3 | І | Н | Я | С | Ш |
| 4 | Е | Н | В | Н | Ф |

Завдання № 6

Горизонтальна перестановка

Зашифрований текст: ЕЕПР ІКВР ШФАИ УІРВ БВДУ ЄЬАТ Я С

Умови завдання:

Для зашифрування тексту використано шифр горизонтальної перестановки.

Довжина ключа: 4.

У вихідному тексті кожне слово складається з чіткої кількості літер.

Питання:

Розшифруйте текст, відновивши вихідні слова.

Чому шифр горизонтальної перестановки складніше зламати без ключа, ніж вертикальної?

Додаткові рекомендації: розділіть текст на рядки по 4 символи (довжина ключа), потім переставте літери у кожному рядку за вказаним ключем.

**Результат:** Перевірка шифру відбувається

Завдання № 7

Атака на шифр перестановки

Зашифрований текст виглядає так: ЕКСРЕ ПИТЙН ЬОАЛР ЙКТИА

Відомо, що він був зашифрований методом перестановки із ключем довжини 5. Відновіть відкритий текст.

Підказки:

Спробуйте всі можливі перестановки ключа вручну або за допомогою скрипта.

Використайте знання про те, що текст має бути осмисленим.

Формат виконання:

Надайте знайдений відкритий текст.

Який ключ перестановки було використано?

Контрольні запитання

1. Дати визначення понять "криптологія", "криптографія", "криптоаналіз".

Криптологія — наука, що вивчає методи шифрування (криптографія) та їх розкриття (криптоаналіз).

Криптографія — наука про методи перетворення інформації з метою її захисту від несанкціонованого доступу.

Криптоаналіз — наука про методи розкриття зашифрованої інформації без знання ключа.

2. Що таке "шифр", "ключ", "конфіденційність", "автентичність".

Шифр — алгоритм перетворення відкритого тексту в зашифрований.​

Ключ — секретна інформація, що визначає конкретне перетворення в шифрі.​

Конфіденційність — властивість інформації бути доступною лише уповноваженим особам.​

Автентичність — гарантія того, що інформація дійсно походить від заявленого джерела.​

3. Як працює шифр простої заміни і які його основні недоліки?

Кожен символ відкритого тексту замінюється на інший символ за фіксованим правилом.​

**Недоліки:**

1. Легко піддається частотному аналізу.​

2. Зберігає структуру мови, що полегшує розшифрування.

4. У чому різниця між моноалфавітною та поліалфавітною заміною?

Моноалфавітна заміна — використовується один алфавіт для всього тексту.​

Поліалфавітна заміна — використовується кілька алфавітів, змінюваних за певним правилом (наприклад, шифр Віженера).

5. Як зміниться гістограма відкритого тексту після шифрування методом простої заміни?

Гістограма зберігає форму, але частоти символів переміщуються до інших символів.​

6. Чи ускладниться шифр, якщо послідовно використовувати до тексту декілька шифрів простої заміни?

Не значно ускладнює шифр, оскільки результат все одно є моноалфавітним шифром.​

7. Який перший шифру перестановки відомий в історії?

Першим відомим шифром перестановки є шифр Сцитала, який використовувався в Давній Спарті приблизно в V столітті до н.е.​

8. Що таке шифр горизонтальної перестановки і як він працює?

Шифр горизонтальної перестановки переставляють символи тексту в рядках відповідно до ключа або іншого правила.

9. Що таке шифр вертикальної перестановки і як він працює?

Шифр вертикальної перестановки базуються на вписуванні символів тексту у таблицю за певним правилом, а потім прочитанні символів за стовпцями у визначеному порядку.

10. Що таке шифр подвійної перестановки і як він працює?

Шифр подвійної перестановки (Double Transposition Cipher) комбінує дві перестановки рядків і стовпців текстової матриці для ускладнення дешифрування.

11. Чому шифри перестановки часто комбінують із шифрами заміни?

Підвищує стійкість шифру, оскільки ускладнює аналіз структури тексту.​

12. Як виглядатиме гістограма відкритого тексту після шифрування методом перестановки?

Зберігає частоти символів, але змінює їх порядок у тексті.​

13. Чи можливо за допомогою частотного аналізу визначити, чи був застосований шифр заміни чи перестановки? Чому?

Так, частотний аналіз дозволяє визначити тип шифрування.

Шифр заміни – кожен символ відкритого тексту замінюється на інший, змінюючи частотний розподіл символів у шифротексті. Це дозволяє виявити закономірності та потенційно розшифрувати текст.​

Шифр перестановки – символи переставляються без зміни їхніх значень, тому частотний розподіл символів у шифротексті залишається таким самим, як у відкритому тексті.​