МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХАРКІВСКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ

ІМЕНИ СЕМЕНА КУЗНЕЦЯ

ЗВІТ

о виконанні лабораторної роботи №2

з дисципліни «Захист інформації»

за темою «Захист особистих повідомлень»

Виконав:

Студент 4 курсу

групи 6.04.122.010.22.1

факультету ІТ

Ячунскас Вітас

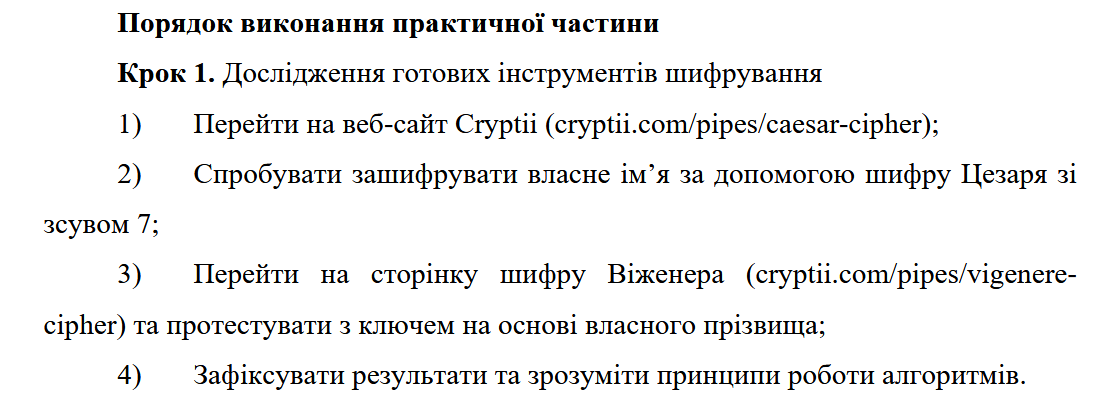
Перевірив:

Професор кафедри

кібербезпеки та ІТ

Тютюнник В. В.

Харків – 2025



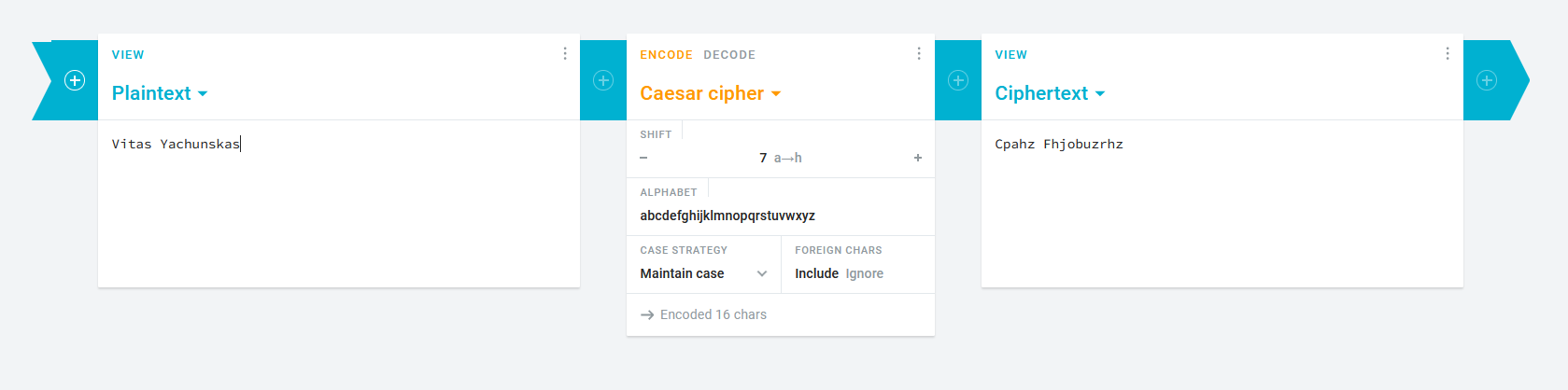


Рис. 1. Моє ім’я зашифроване шифром Цезаря зі зсувом 7

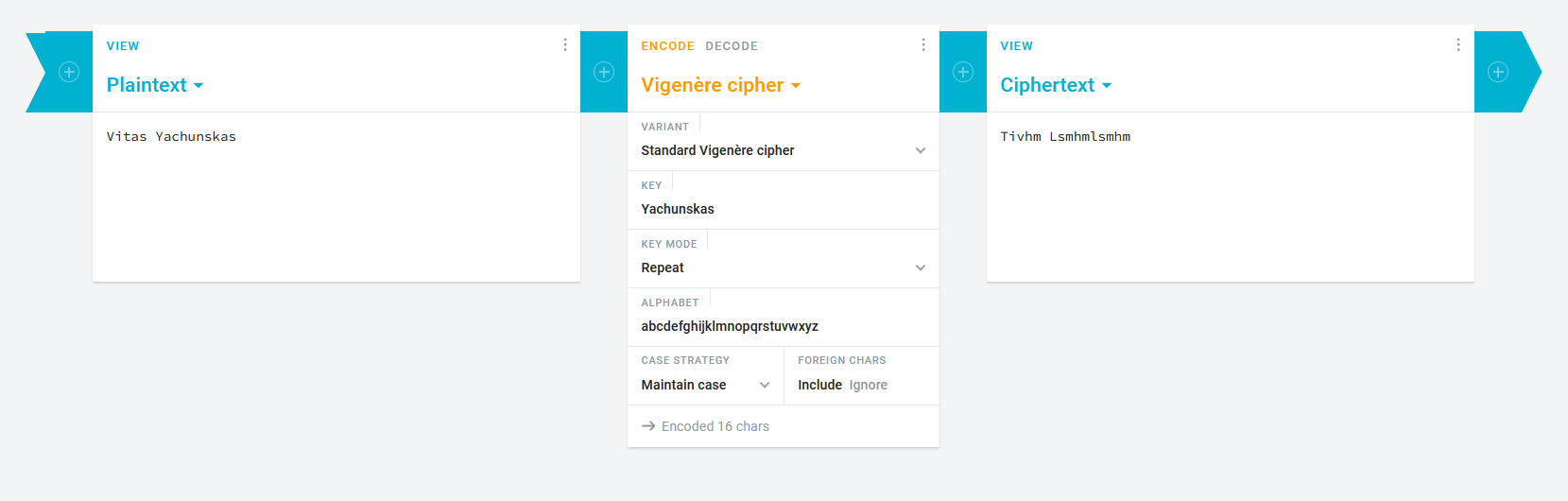
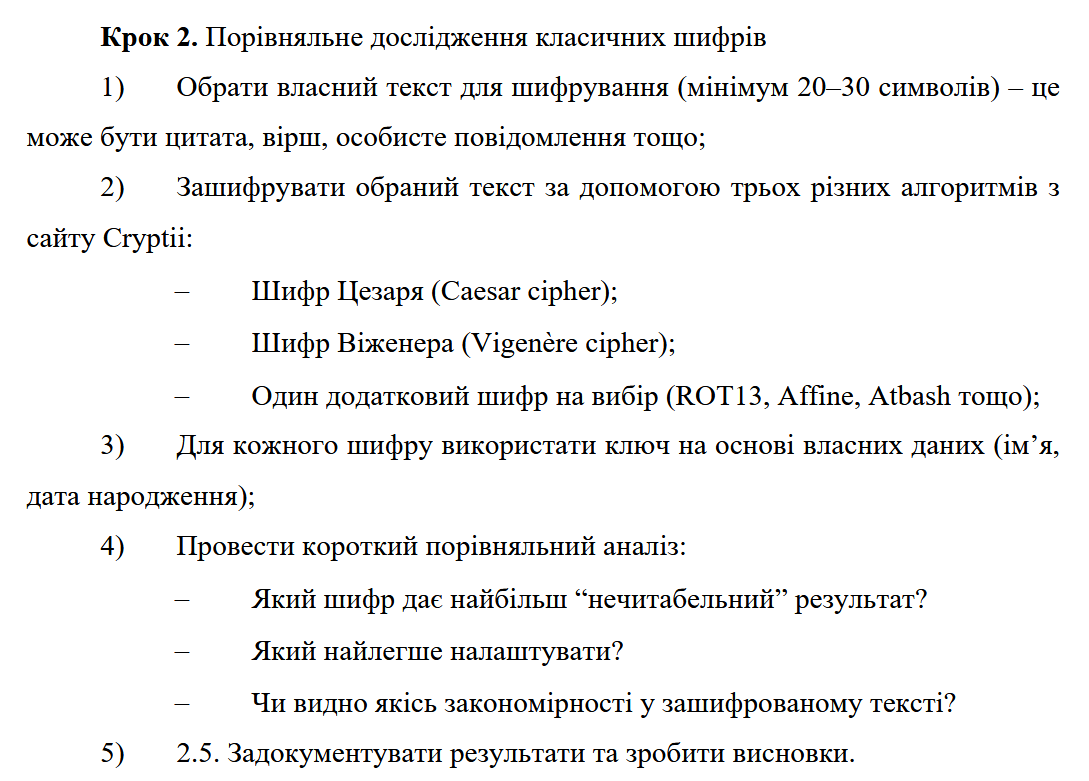


Рис. 2. Моє ім’я зашифроване шифром Віженера

Як бачимо, шифр Віженера є більш складним оскільки в ньому літери повторюються, навіть ті які в оригінальному тексті не були однаковими.



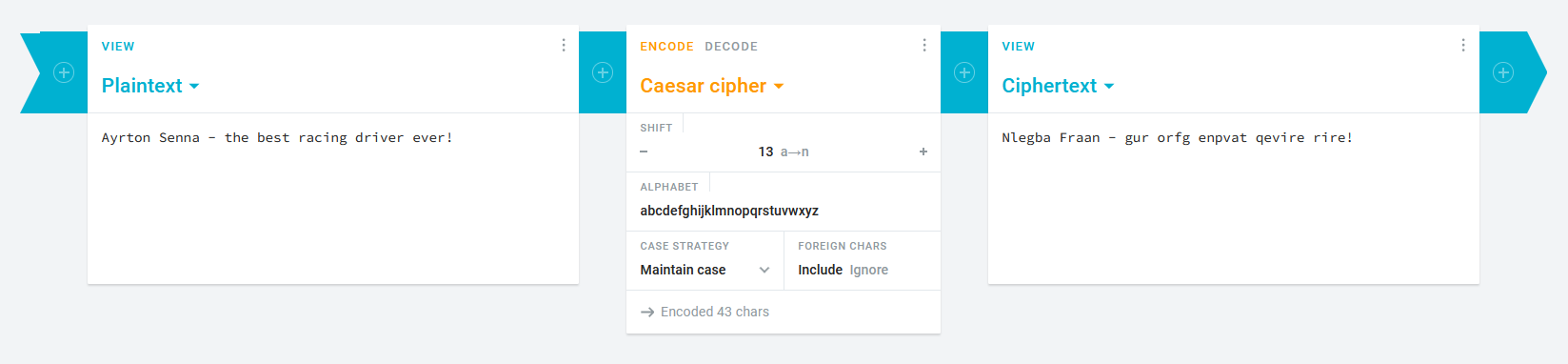


Рис. 3. Текст, зашифрований шифром Цезаря

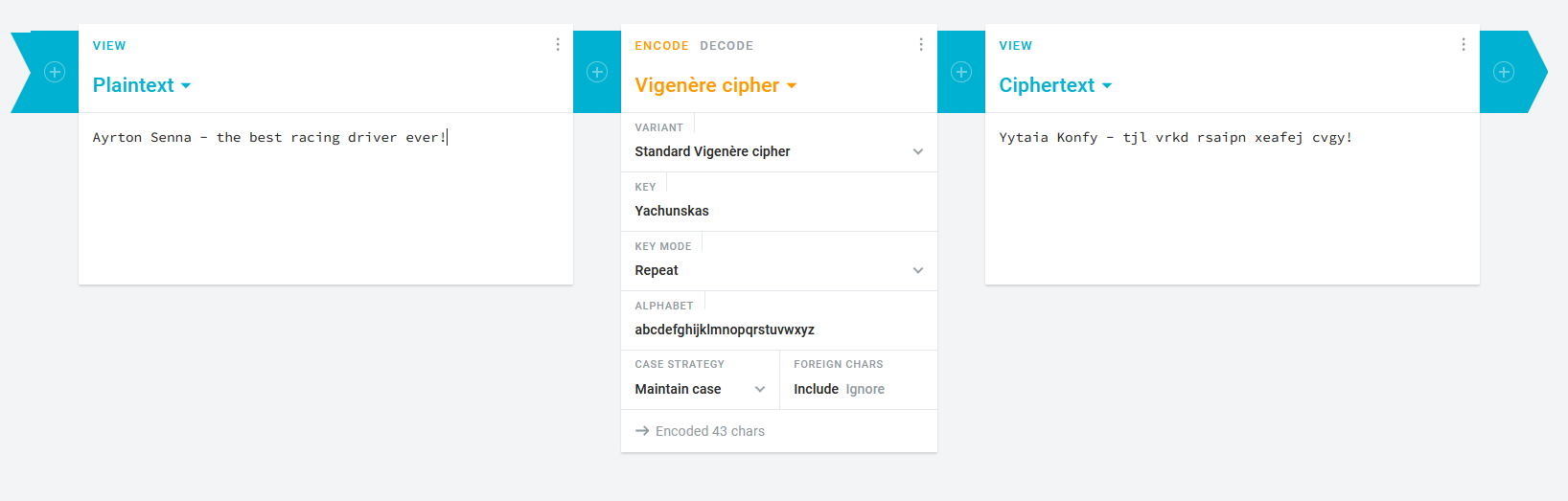


Рис. 4. Текст, зашифрований шифром Віженера

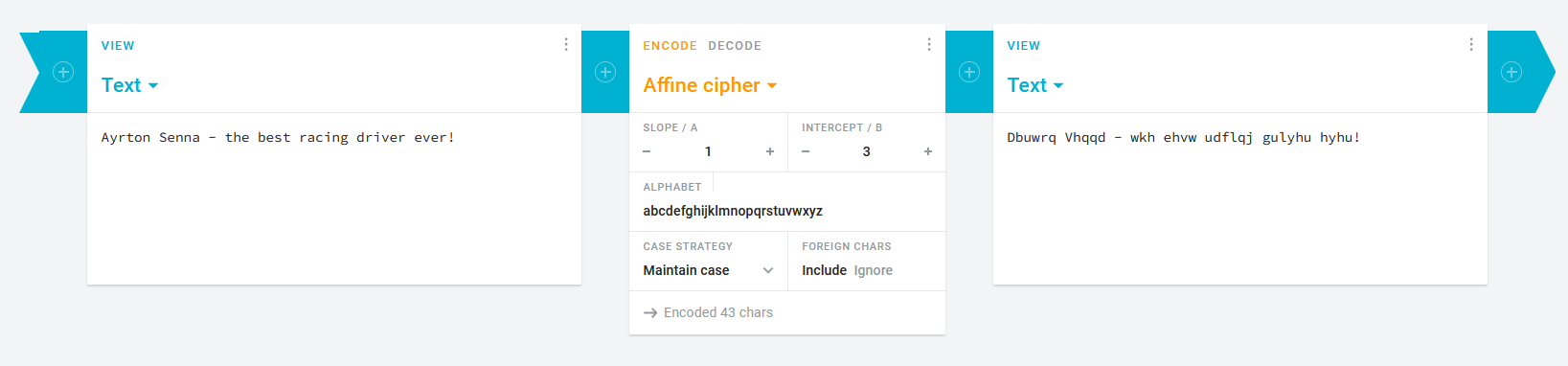
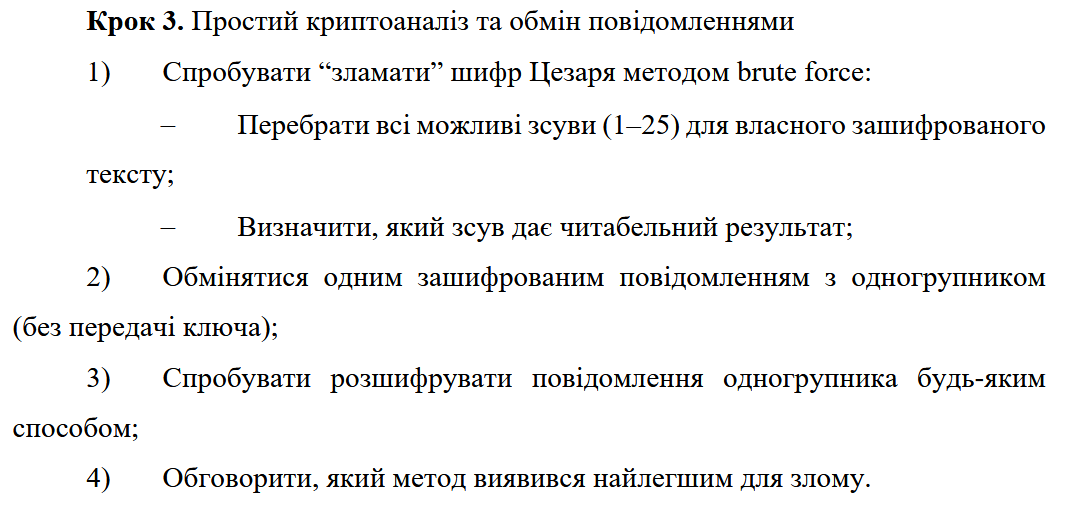


Рис. 5. Текст, зашифрований шифром Affine

Кожен шифр дає приблизно схожий «нечитабельний» результат, втім жоден шифр за базових налаштувань не замінив символи «-» та «!».

Найлегший для налаштування – шифр Цезаря, адже в ньому налаштовуються в основному зсув та абетка.

Найбільша закономірність яку видно мені - «-» та «!» які трапляються в одному й тому місці. З цих символів знаючи шифр зробити припущення щодо, наприклад, слова після дефісу та працювати з ним.



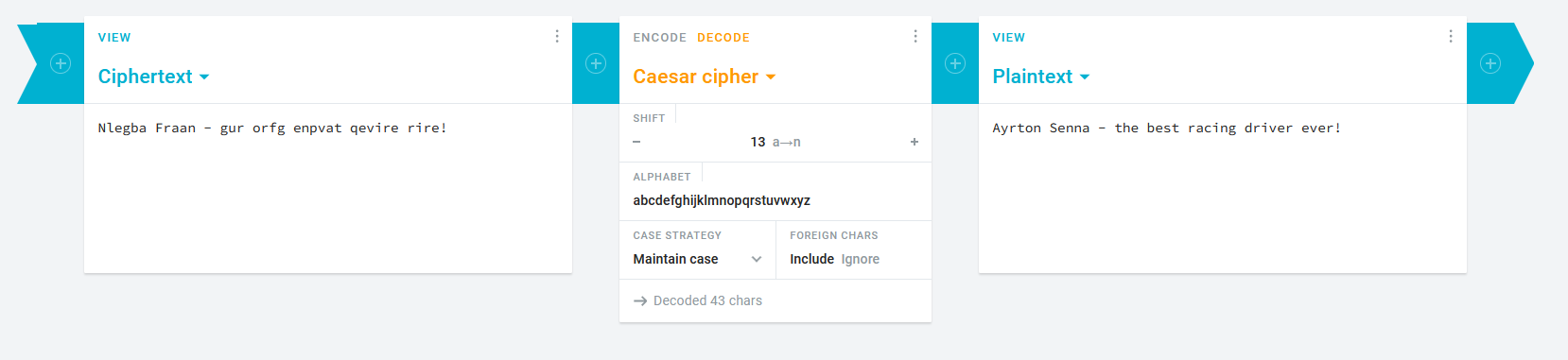


Рис. 6. Зсув який дає читабельний результат

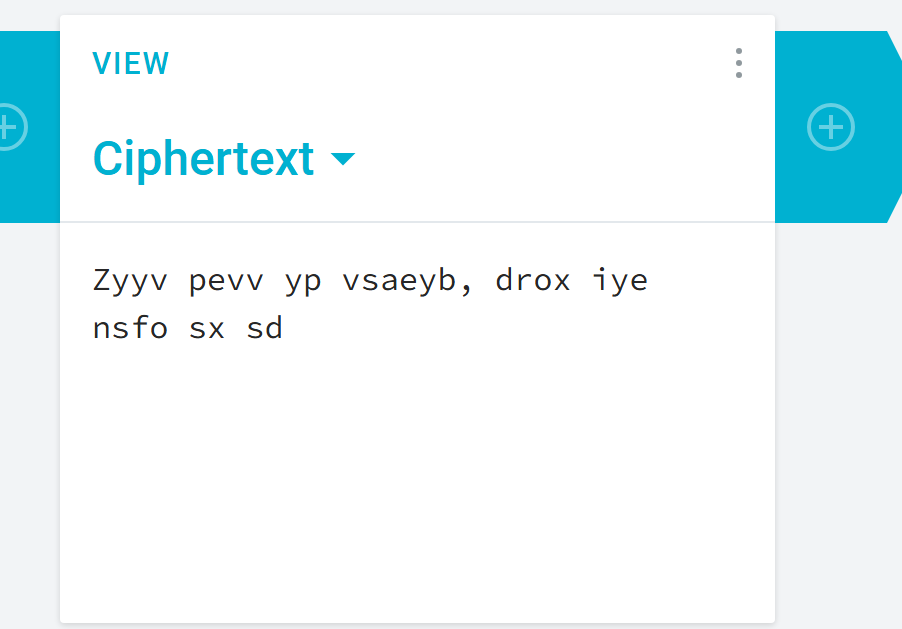


Рис. 7. Зашифроване повідомлення мого одногрупника

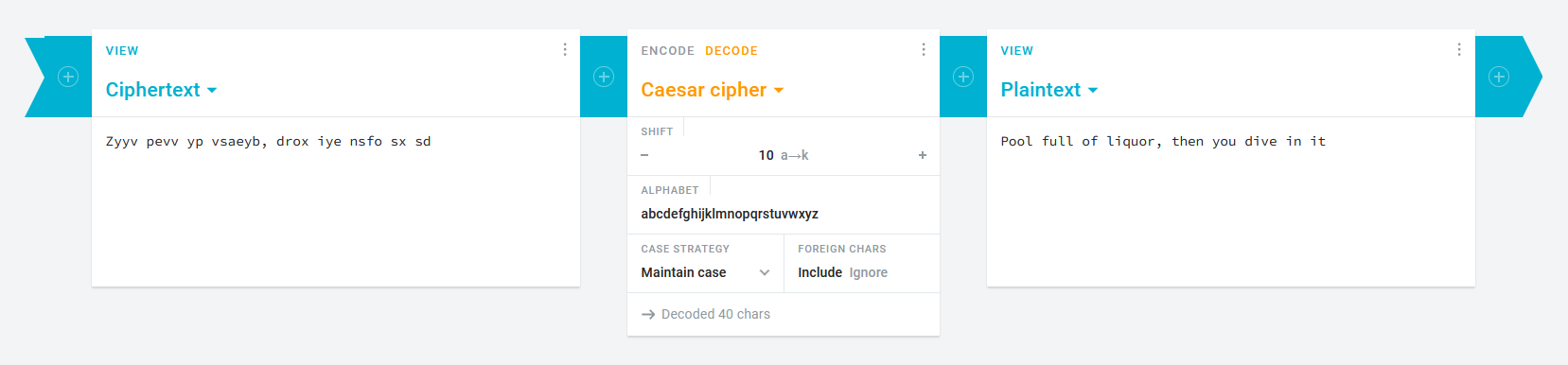
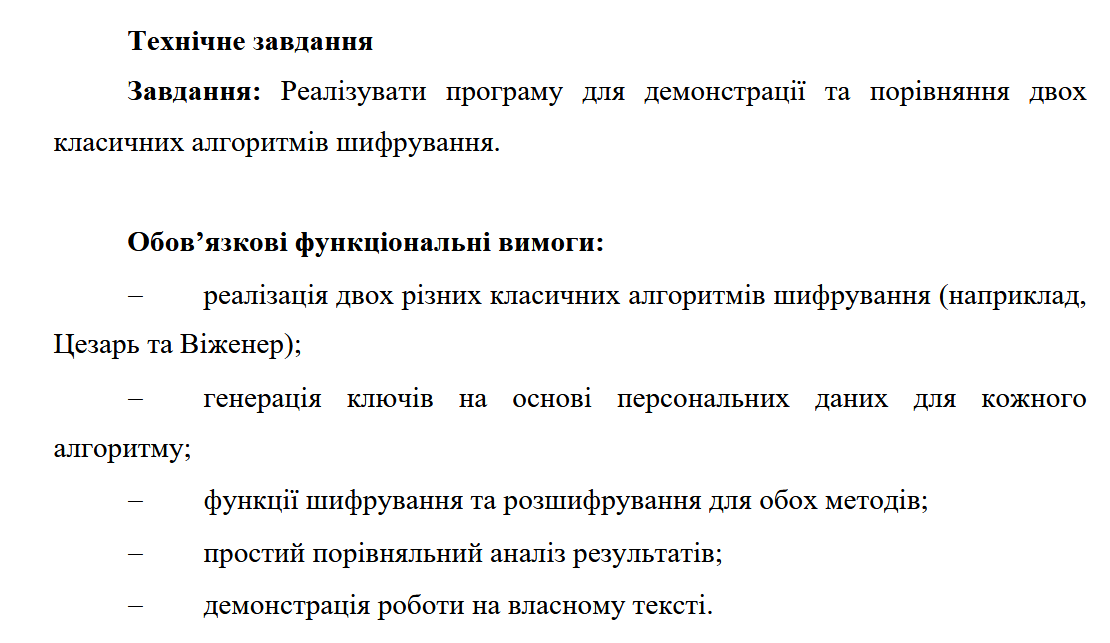


Рис. 8. Отримане розшифроване повідомлення

Отже, для шифру Цезаря найпростішим методом зламу в більшості випадків є метод повного перебору, тобто “brute force”. Втім, якщо трохи змінити абетку можна збити людину що намагається зламати повідомлення з пантелику та сильно ускладнити задачу.



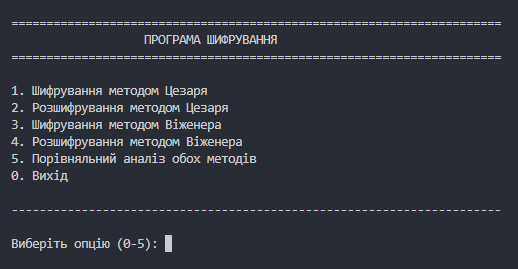


Рис. 9. Меню користувача

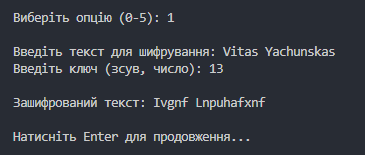


Рис. 10. Шифрування шифром Цезаря

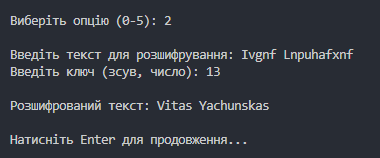


Рис. 11. Розшифрування шифром Цезаря

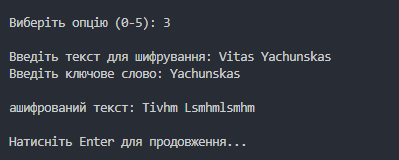


Рис. 12. Шифрування шифром Віженера

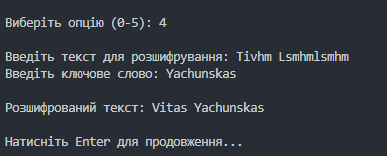


Рис. 13. Розшифрування шифром Віженера

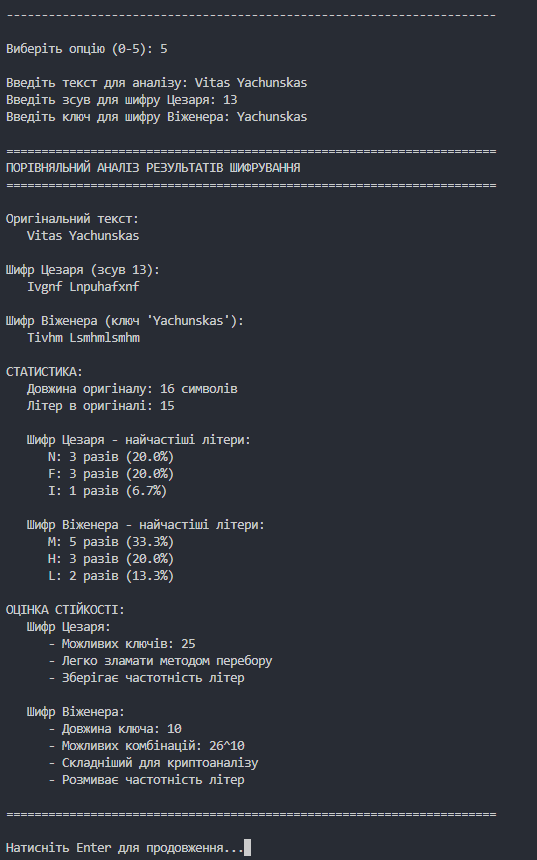


Рис. 14. Порівняльний аналіз шифрів

Висновок: в ході лабораторної роботи я навчився створювати системи захищеного листування з використанням класичних методів шифрування