**ЛАБОРАТОРНА РОБОТА № 1**

КЛАСИЧНИЙ ШИФР ПРОСТОЇ  
ЗАМІНИ ТА ЙОГО КРИПТОАНАЛІЗ. БІГРАМНИЙ ШИФР

**Мета заняття**: набути вміння із зашифрування та дешифрування

повідомлень за допомогою шифру простої заміни, зокрема шифру Цезаря;

використовуючи частотний криптоаналіз, навчитися зламувати шифротекст,

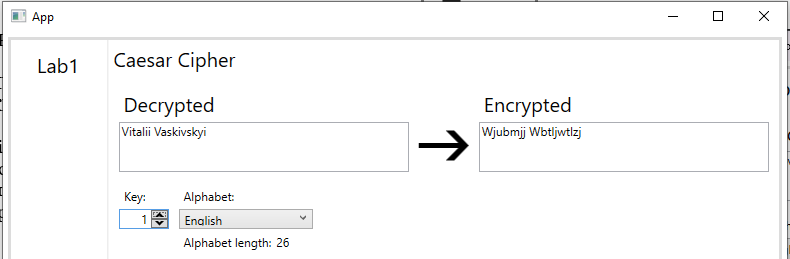
зашифрований методом простої заміни; навчитися шифруванню біграмним

шифром Плейфера.

**Хід роботи:**

**Завдання 1:**

Створити програму в середовищі MS Excel або на будь-якій мові  
програмування для шифрування повідомлень із використанням шифру Цезаря  
(англійській алфавіт). Значення ключа шифрування визначається номером за  
алфавітним списком студента у журналі. Зашифрувати своє прізвище та  
дешифрувати отриманий шифротекст.

  
Рис. 1.1. Шифрування шифром Цезаря в власно написаннії програмі

Значення ключа: 1,

Вхідний текст: Vitalii Vaskivskyi,

Код программи можно побачити на моєму репозиторії: <https://github.com/grozer221/CryptographyLabs>

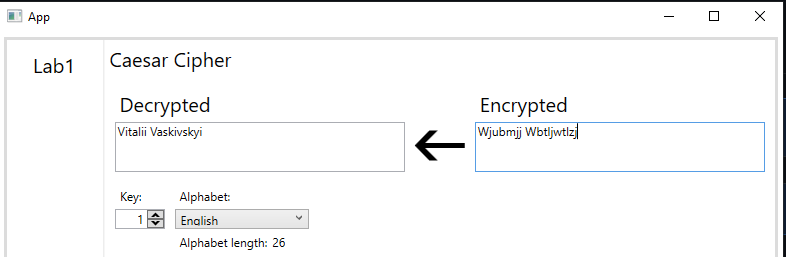


Рис. 1.1. Дешифрування шифром Цезаря в власно написаннії програмі

Значення ключа: 1,

Вхідний зашифрований текст: Wjubmjj Wbtljwtlzj

Розшифрований текст: Vitalii Vaskivskyi

**Завдання 2**. Студентам потрібно поділитися на ротаційні групи з трьох чоловік: СТУДЕНТ-ВІДПРАВНИК, СТУДЕНТ-ОТРИМУВАЧ, СТУДЕНТКРИПТОАНАЛІТИК. Обмін повідомленнями між учасниками відбуватиметься за схемою (рис. 5), в основі якої лежить секретна система зв’язку, описана Клодом Шеноном.

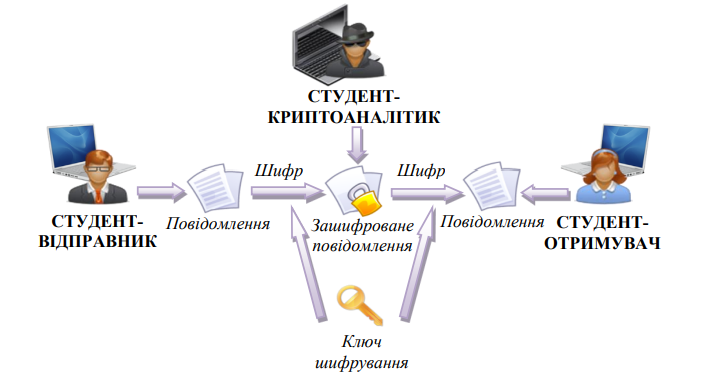
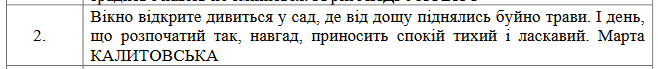


Рис.5. Схема обміну повідомленнями між студентами.

**Студент, з ким працював в команді**: Дмитро Гісса.

2.1. На сайті CrypTool Online – https://www.cryptool.org/en/cto/ з використанням шаблону Caesar виконати шифрування тексту шифром Цезаря згідно варіанту. Спочатку введіть відкритий текст до поля Input, потім визначте алфавіт за допомогою опції Define own alphabet, ключ шифрування оберіть самостійно.



Ключ шифрування: 3

2.2. Додати скріншот зашифрування до звіту.

Результат виконання:

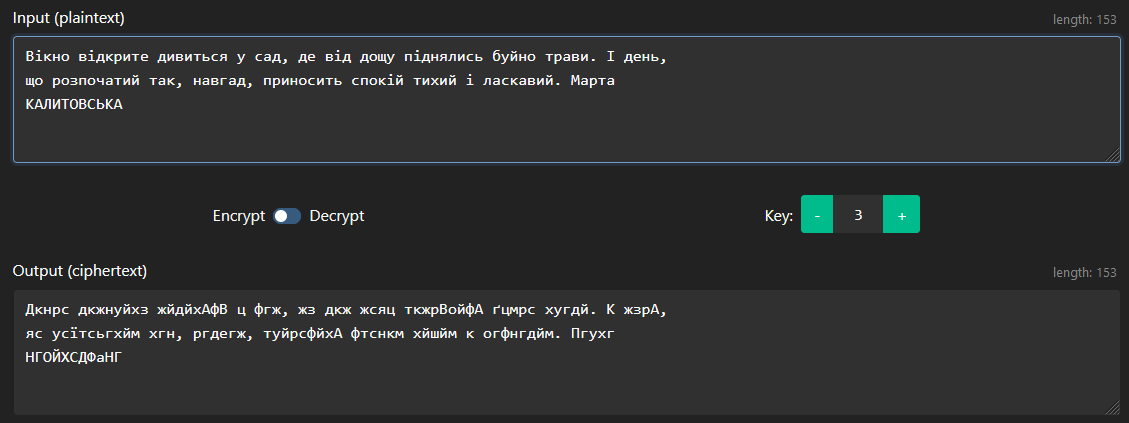


Рис.6. Результат шифрування тексту згідно варіанту з ключем 3.

2.3. Зберегти отриманий шифротекст до текстового документу та обмінятися файлами із шифротекстом зі студентом своєї ротаційної групи.Заздалегідь таємно узгодити довжину ключа шифрування.

2.4. Аналогічно до п.2.1 виконати дешифрування повідомлення одногрупника із використанням шифру Цезаря, увівши шифротекст до відповідного текстового поля. При цьому потрібно встановити перемикач у положення Decipher.

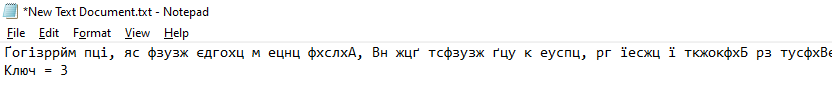


Рис.7. Отриманий зашифрований текст студента з ключем.

2.5. Додати до звіту скріншот дешифрування повідомлення.

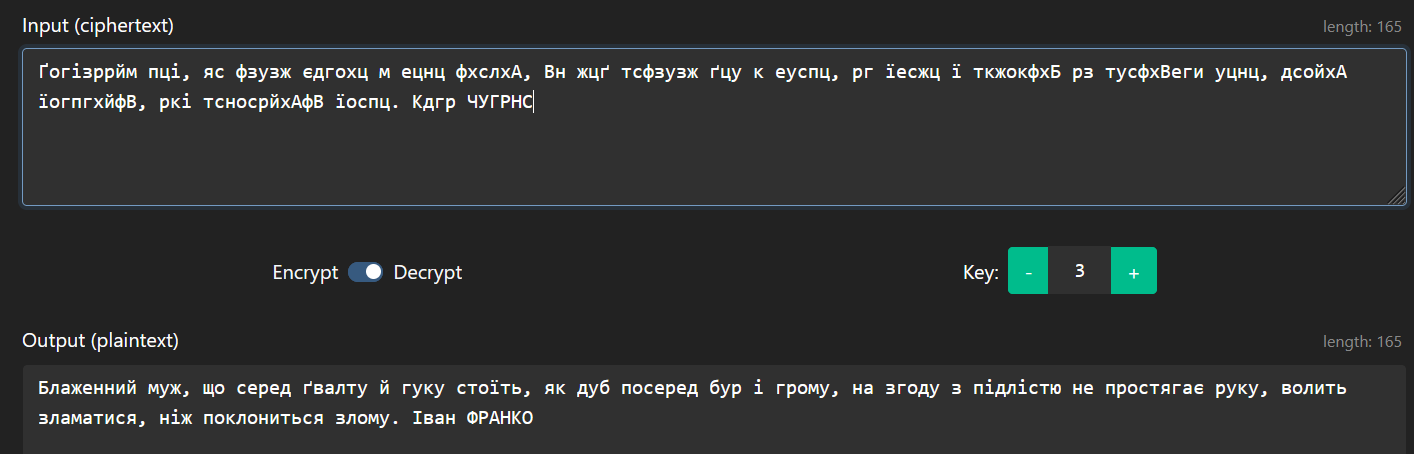


Рис.8. Результат дешифрування повідомлення студента за ключем.

2.6. Обмінятися повідомленнями із шифротекстом з іншим студентом своєї ротаційної групи. При чому, довжина ключа шифрування повинна триматися втаємниці.

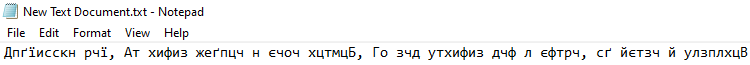


Рис.9. Отриманий зашифрований текст студента без ключа.

2.7. Підрахувати частоти зустрічальності літер у шифротексті одногрупника, використовуючи шаблон N-Gram Analysis в розділі криптоаналізу на сайті https://www.cryptool.org/en/cto/.

2.7. Додати до звіту таблицю частоти зустрічальності літер.

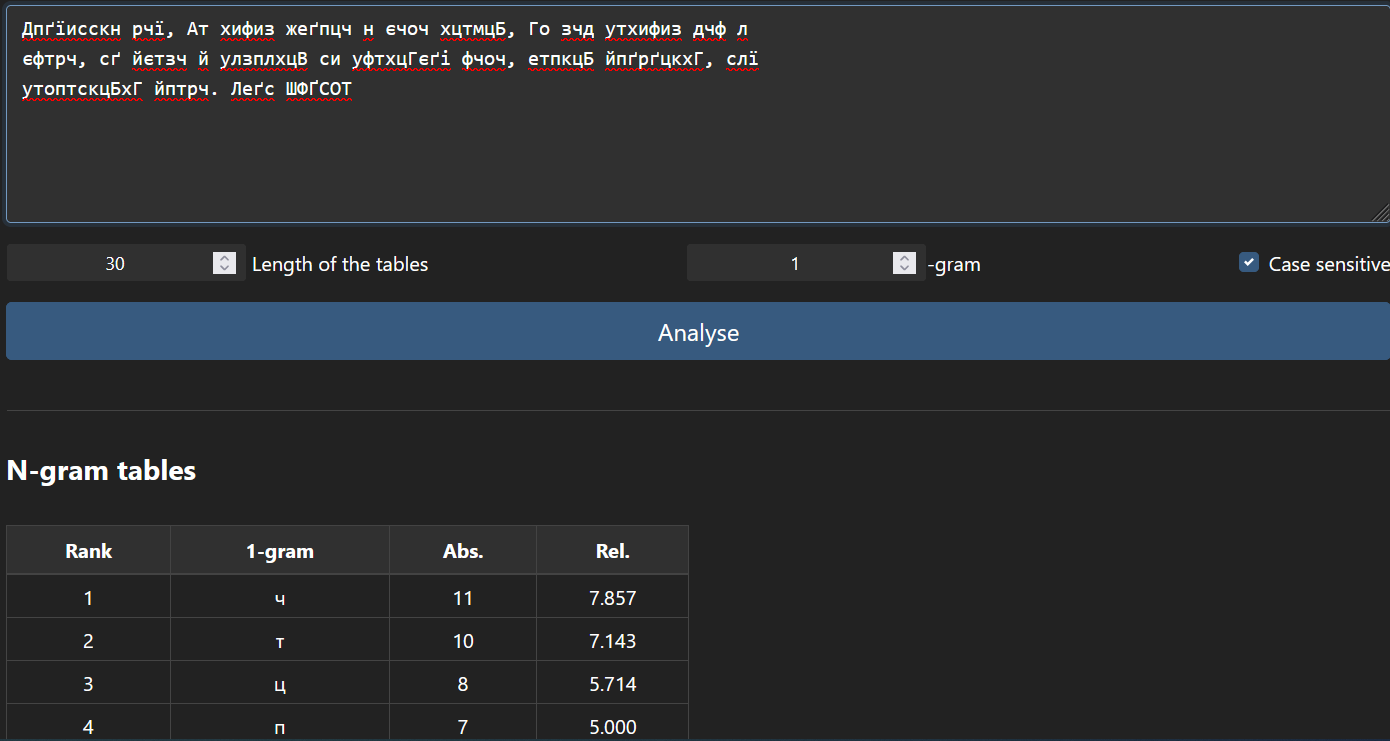


Рис.9. Таблиця частоти зустрічальності літер.

2.8. На основі частоти зустрічальності літер у шифротексті підібрати значення ключа, обґрунтувавши свої дії у звіті.

Найчастіше в тексті зустрічається буква М. Відомо, що найчастіше в текстах української мови зустрічається літера О, то можна обчислити ключ K: 27 – 18 = 9.

Спробую відновити повідомлення.

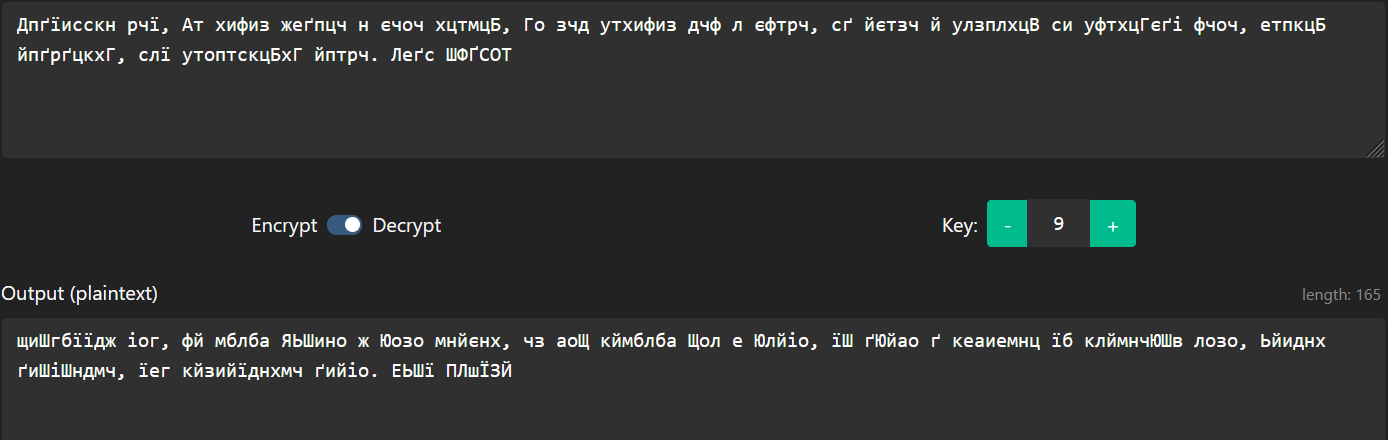


Рис.10. Спроба відновити повідомлення

Повідомлення невдалось відновити, тому беремо наступну букву І, яка також найчастіше зустрічається в тексті, тому отримаємо, що K: 22 - 18 = 4.

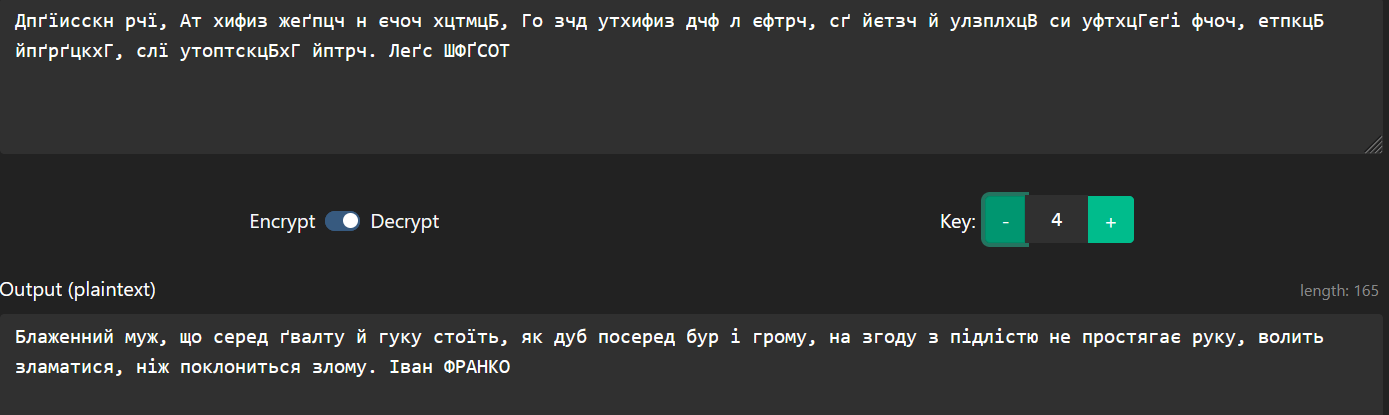
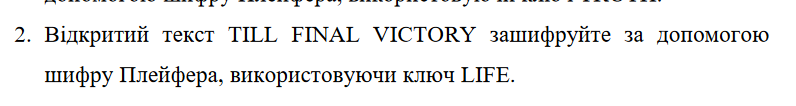


Рис.11. Відновлене повідомлення

**Завдання №3.** Виконати зашифрування повідомлення шифром Плейфера згідно варіанту (визначається номером студента у журналі: непарний – 1 варіант, парний – 2 варіант).



Для шифрування розіб’ємо текст на біграми TI LX LF IN AL VI CT OR YX.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| L | I | F | E | A |
| B | C | D | G | H |
| J | K | M | N | O |
| P | R | S | T | U |
| V | W | X | Y | Z |

Рис. 7. Шифрування біграм

Далі, користуючись правилами шифрування біграм, отримаємо

шифротекст: RE FV IE EK LI WL GR KU ZY