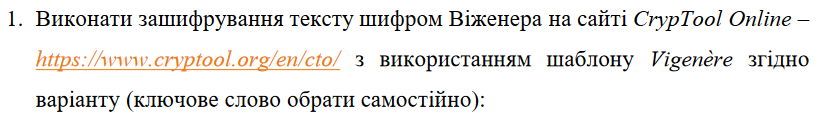
**ЛАБОРАТОРНА РОБОТА № 2**

**КЛАСИЧНИЙ ШИФР ПОЛІАЛФАВІТНОЇ ЗАМІНИ ТА ЙОГО КРИПТОАНАЛІЗ. КРИПТОСИСТЕМА ХІЛЛА**

**Мета заняття**: набути вміння із шифрування повідомлень за допомогою  
шифру поліалфавітної заміни, зокрема шифру Віженера; використовуючи  
методи Казіскі та Фрідмана, навчитися зламувати шифротекст, зашифрований  
методом поліалфавітної заміни; навчитися шифрувати повідомлення у  
криптосистемі Хілла.

**Хід роботи:**

**Завдання 1:**





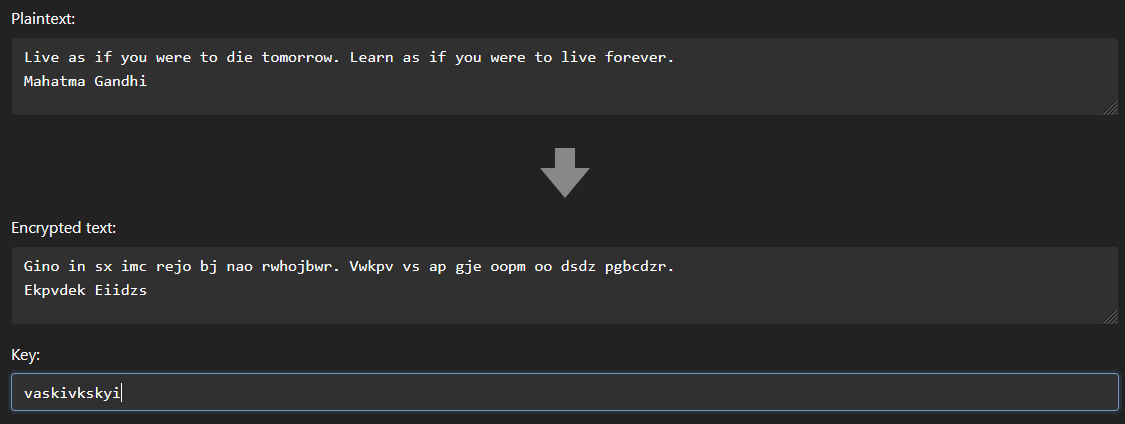
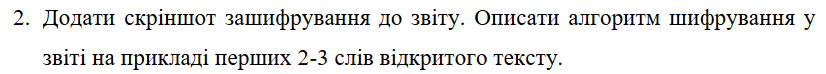
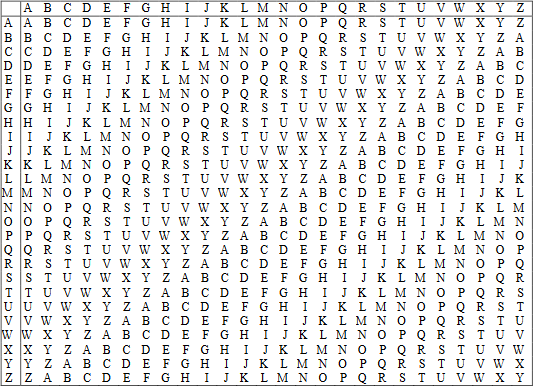


Рис 1.1 Зашифрування тексту за варіантом



Для зашифровування може використовуватися й таблиця, яка отримала назву «таблиця Віженера»:



Під час зашифрування кожна літера повідомлення замінюється на літеру, що  
знаходиться на перетині літер першого рядка (алфавіт повідомлення) і першого  
стовпчика (алфавіт ключа) в таблиці Віженера.

Для прикладу зашифруємо перші 2 слова – Live as if. Ключем буде виступати слово – vaskivksyi;

L(v) -> G

i(a) -> i

v(s) -> n

e(k) -> o

a(i) -> i

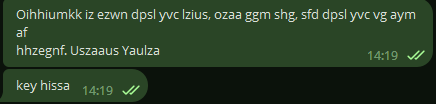
s(v) -> n

i(s) -> s

f(k) -> x

результат: Gino in sx





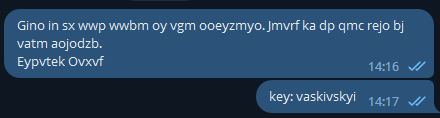
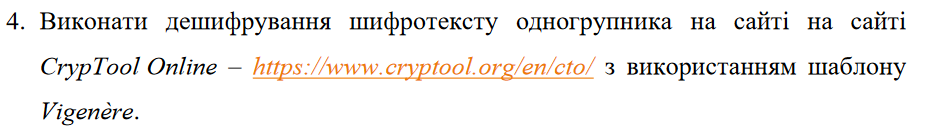


Рис 1.2 обмін шифротекстами з Дмитром Гісса.



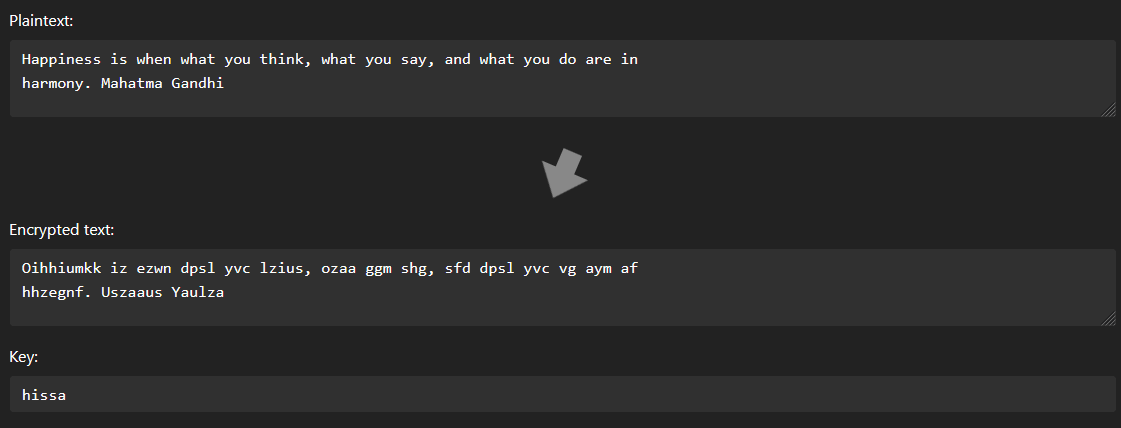
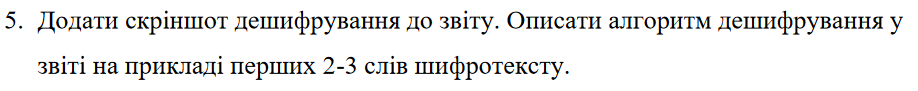
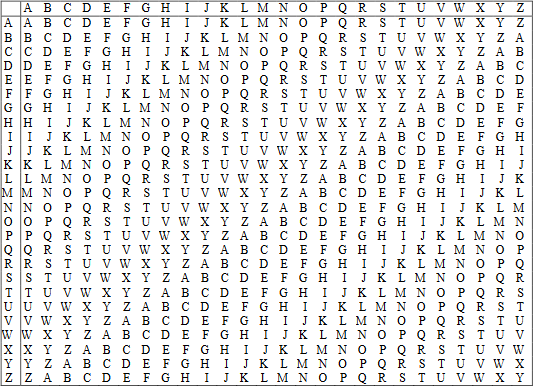


Рис 1.3 розшифровка шифротексту Дмитра Гісса.



При дешифруванні потрібно відшукати у першому стовпчику літеру ключа  
і за літерами шифротексту визначити, в якому стовпчику зверху знаходиться  
літера відкритого тексту.:



Для прикладу розшифруємо перші 2 слова – Oihhiumkk iz. Ключем буде виступати слово – hissa;

O(h) -> H

i(i) -> a

h(s) -> p

h(s) -> p

i(a) -> i

u(h) -> n

m(i) -> e

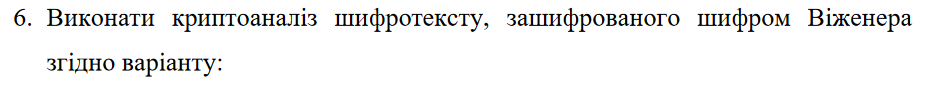
k(s) -> s

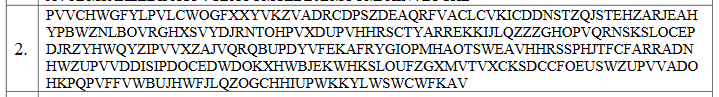
k(s) -> s

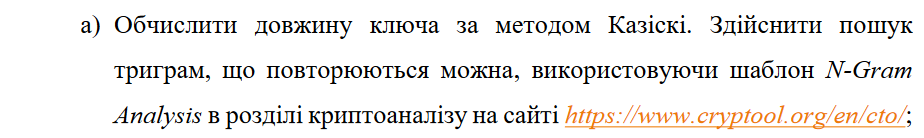
i(a) -> i

z(h) -> s

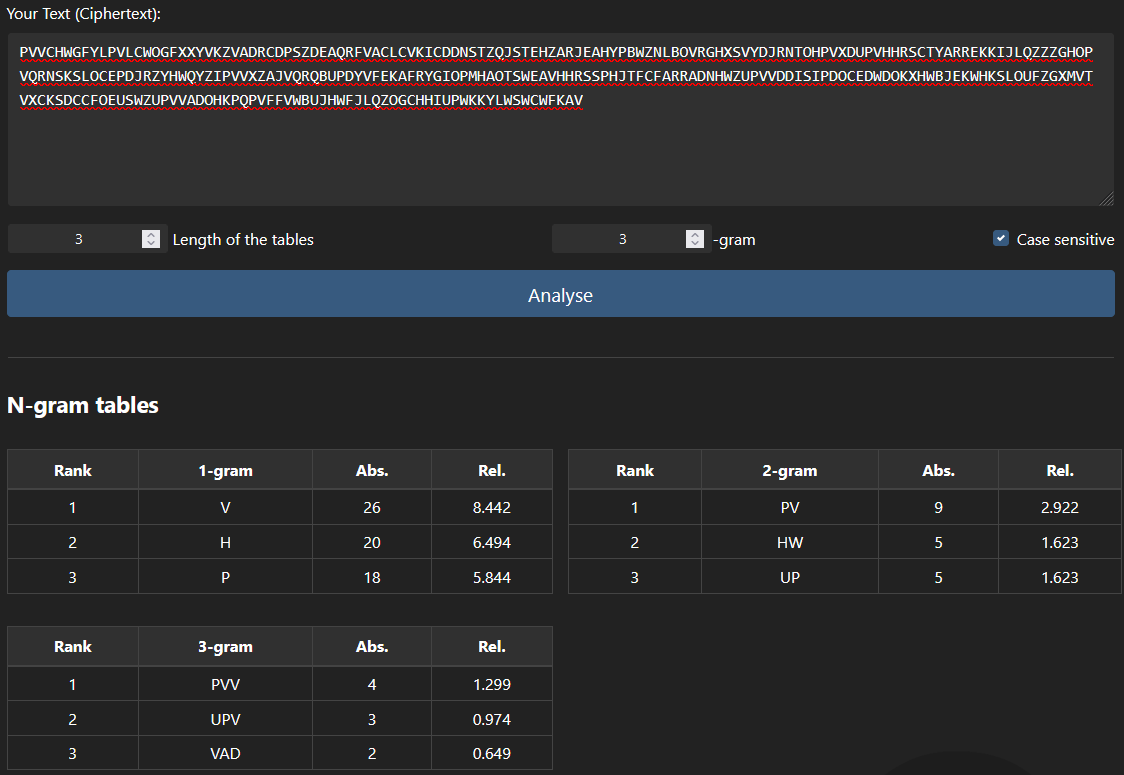
результат: Happiness is







Користуючись сайтом cryptool знаходимо триграму, яка зустрічається декілька разів:



У шифротексті триграма UPV зустрічається 3 рази. Відстань між першою і другою появою становить 105 символів, між першою і третьою – 160.

НСД (105, 160) = 5, тому можна припустити, що довжина ключового слова рівна 5.

1. Обґрунтувати довжину ключа, використовуючи метод Фрідмана. Обчислити індекс збігу можна за допомогою MS Excel. Додати скріншот обчислення індексу збігу та описати хід обчислень у звіті;

Було використано формули для знаходження індексу збігу та довжини ключа. Результати розрахунків зображені на рисунку 6.

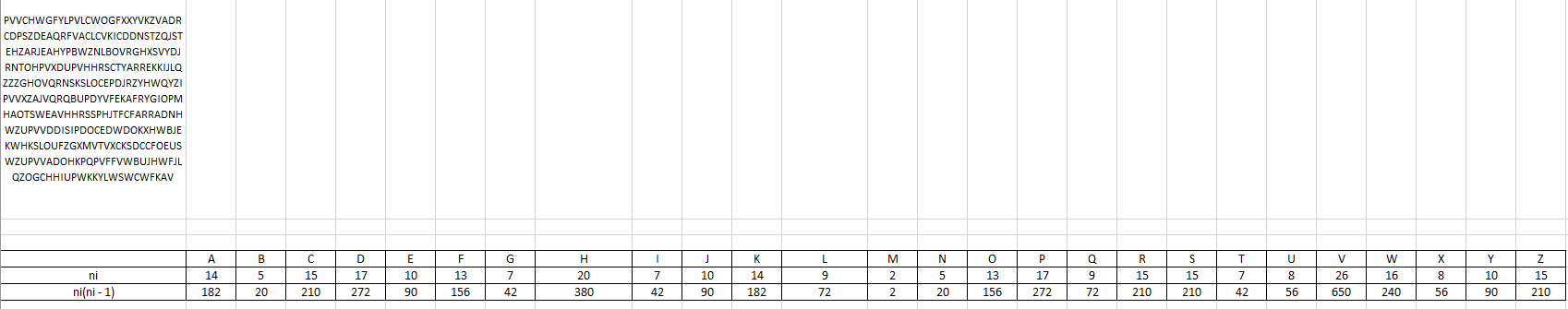


Рис. 6. Обґрунтування довжини ключа, використовуючи метод Фрідмана

1. Знайти літери ключового слова, використовуючи частотний аналіз;

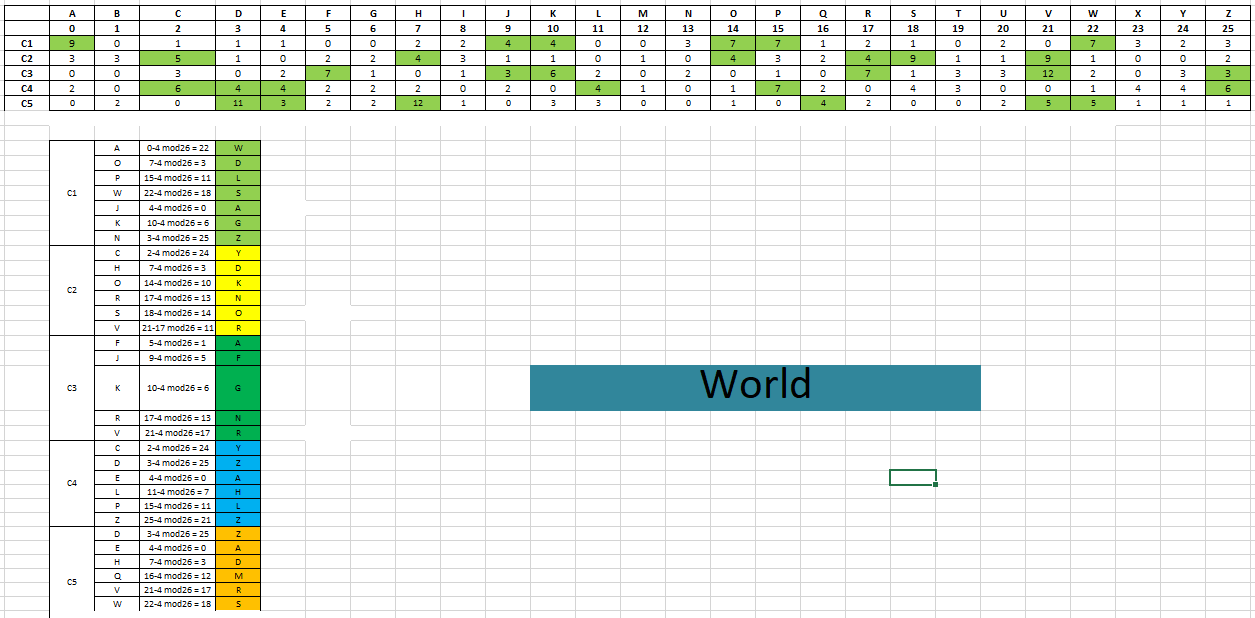


Рис. 7. Літери ключового слова, використовуючи частотний аналіз

1. Відновити початкове повідомлення із знайденим ключем та додати скріншот до звіту.

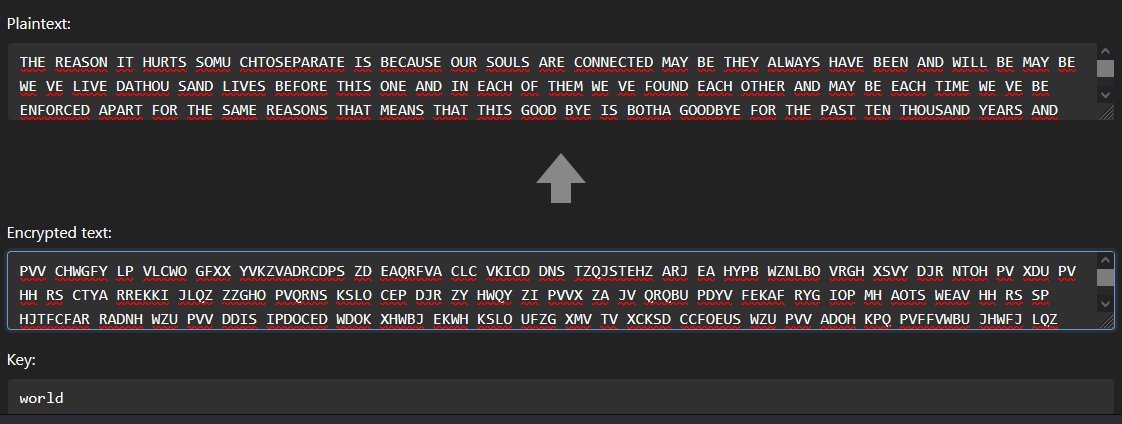


Рис. 8. Початкове повідомлення із знайденим ключем

Завдання №2: Виконати зашифрування повідомлення згідно варіанту (визначається номером студента у журналі: непарний – 1 варіант, парний – 2 варіант). Усі кроки алгоритму шифрування описати у звіті. Обчислення можна виконувати в MS Excel.

2. У криптосистемі Хілла з матрицею зашифруйте текст OUT OF DATE.

K = , det K = 11·17·18 + 14·24·2 + 19·19·0 - 19·17·2 - 11·24·0 - 14·19·18 = 3366 + 672 + 0 - 646 - 0 - 4788 = -1396

Розіб’ємо відкритий тест на вектори розмірністю 3, літерам поставимо у відповідність їх числові значення:

P1 = =

P2 = =

P3 = =

K \* P1 = \* = mod26 = =

K \* P2 = \* = mod26 = =

K \* P3 = \* = mod26 = =

Після шифрування було отримано наступний шифротекст: PWGVHEEDU.

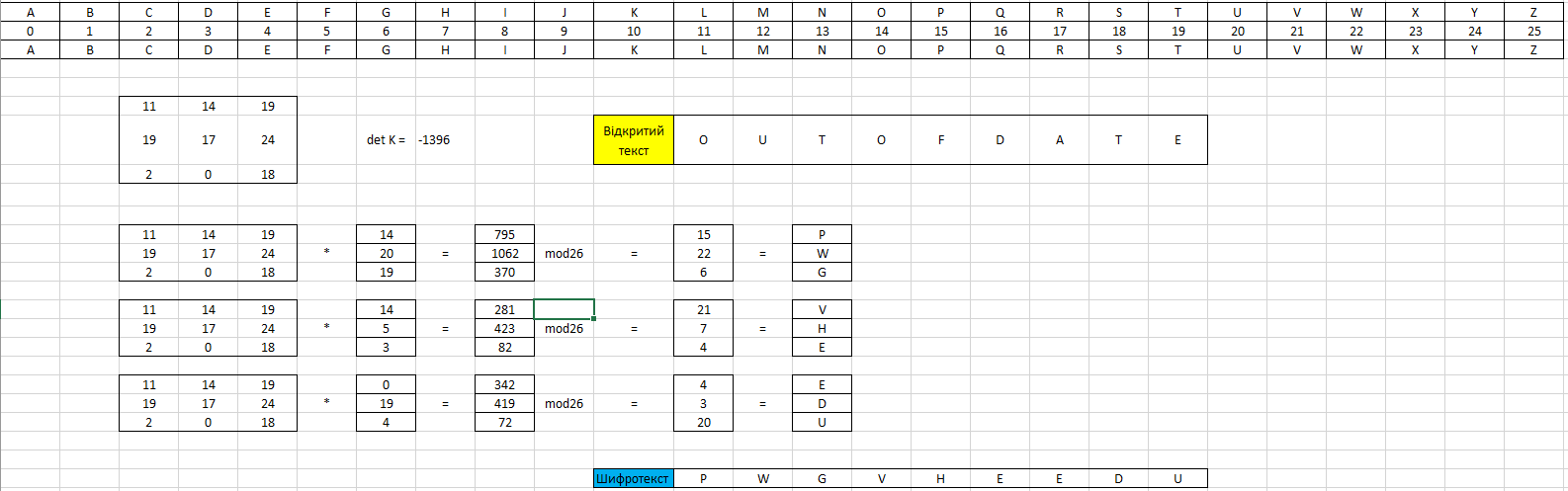


Рис. 9. Шифрування тексту в криптосистемі Хілла

**Висновок:** ми набули вміння із шифрування повідомлень за допомогою шифру поліалфавітної заміни, зокрема шифру Віженера; використовуючи методи Казіскі та Фрідмана, навчилися зламувати шифротекст, зашифрований методом поліалфавітної заміни; навчилися шифрувати повідомлення у криптосистемі Хілла.