

МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

КРИПТОГРАФІЯ

КОМП'ЮТЕРНИЙ ПРАКТИКУМ №2

Криптоаналіз шифру Віженера

Виконали:

Студенти групи 3 курсу
груп ФБ-96 та ФБ-94
Ігнатенко Артем
Васюченко Георгій

Мета:

Засвоєння методів частотного криптоаналізу. Здобуття навичок роботи та аналізу поточкових шифрів гамування адитивного типу на прикладі шифру Віженера.

Постановка задачі:

0. Уважно прочитати методичні вказівки до виконання комп'ютерного практикуму.
1. Самостійно підібрати текст для шифрування (2-3 кб) та ключі довжини $r = 2, 3, 4, 5$, а також довжини 10-20 знаків. Зашифрувати обраний відкритий текст шифром Віженера з цими ключами.
2. Підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення.
3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта).

Хід роботи:

Варіант - 2

Підібраний текст для шифрування - '451 градус за Фаренгейтом' Рея Бредбері, російською мовою.

Завдання 1:

Зашифрований текст у файлі 'task1-encoded.txt'

Завдання 2:

Таблиця індексів відкритого та шифрованих текстів з ключами певної довжини.

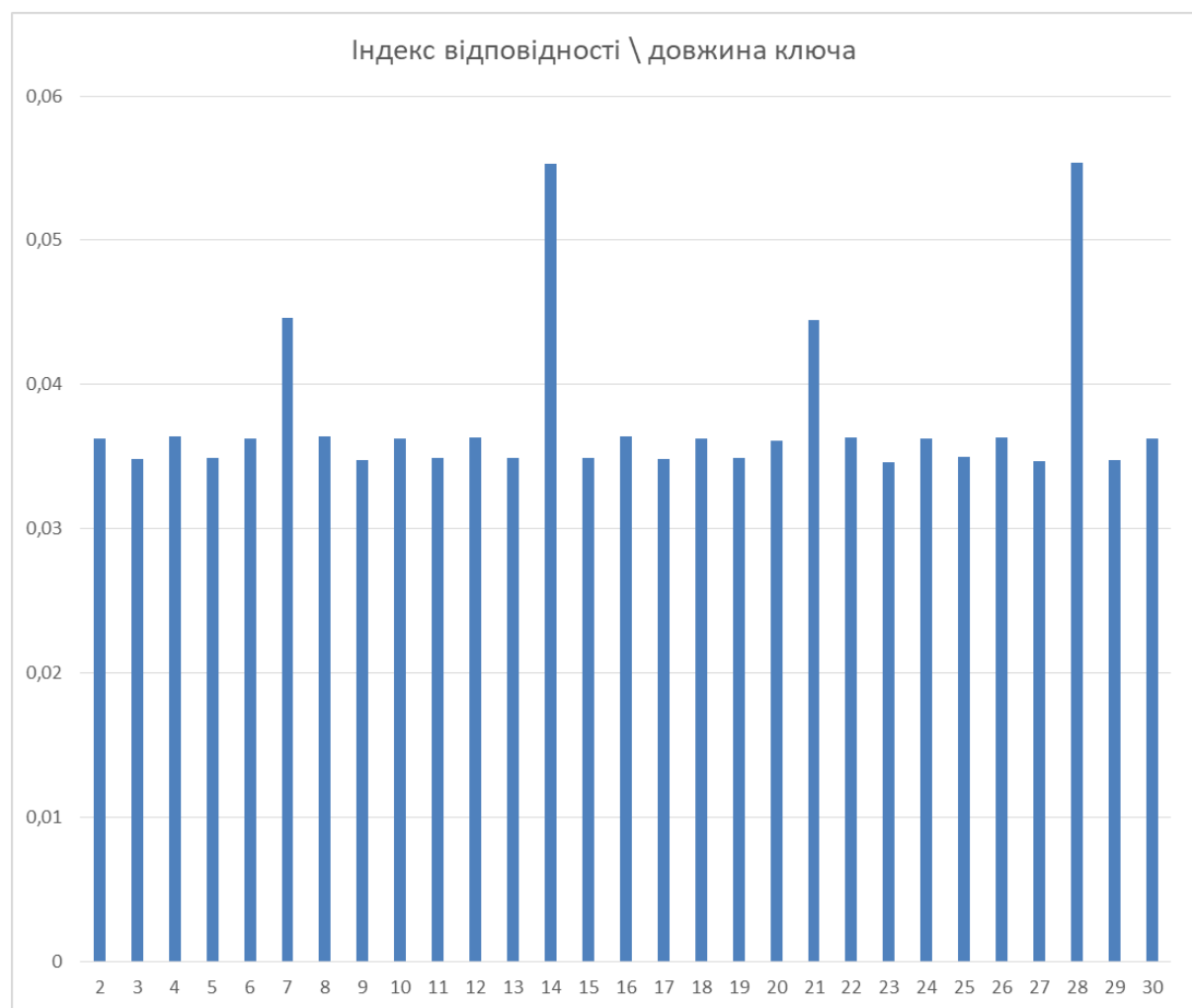
Індекси		Обрані ключі
r	l	["м", "ма", "луч", "зной", "топаю", "всесложноо", "уменьятожеса", "попадаетонао", "ситечкеилипро", "чаятравяногохо", "спроситчтосказа", "помочьтакзайтивд", "явключустримиесли", "помочьскриптойустя", "интерпретированиедоп"]
1	0,047619	
2	0,028571	
3	0,047619	
4	0,038095	
5	0,047619	
10	0,019048	
11	0,047619	
12	0,028571	
13	0,009524	
14	0,028571	
15	0,047619	
16	0,028571	
17	0,028571	
18	0,019048	
20	0,038095	

Таблиця індекса відповідності при певній довжині ключа.



Завдання 3:

r	I
2	0,036268
3	0,034828
4	0,036368
5	0,034923
6	0,036257
7	0,044626
8	0,036423
9	0,034758
10	0,03623
11	0,034873
12	0,036287
13	0,034881
14	0,055282
15	0,034905
16	0,03637
17	0,034842
18	0,036236
19	0,034872
20	0,0361
21	0,04447
22	0,036292
23	0,03462
24	0,036242
25	0,035
26	0,03635
27	0,034663
28	0,055361
29	0,034754
30	0,036236



Бачимо, що індекс відповідності при довжині ключа 14 та 28 різко збільшився, тому, вірогідніше за все, текст було зашифровано ключем довжиною 14 (28 кратно 14, тому у них однаковий індекс відповідності).

Ключ розшифрування: 'жосвеыдиадозор'

Зашифрований текст:

щоекцрылжцьштх'огзцуэц'мшкцубфющ'уытф'бахсю'увч'уэюмопощквк'мьч'тмусу'шюхуц'т'рцозит'суря
хя'ь'еж'рц'яросыот'юршмч'щсф'й'о'ю'ю'у'ь'о'э'и'т'ш'д'х'ь'ь'х'е'ф'я'р'ц'й'х'х'я'в'э'ц'ь'з'х'щ'ц'ы'ф'у'щ'к'б'ор'я'э'й'ш'д'ц'ц'м'ц'
уб'ж'ц'ю'х'ш'м'я'ил'х'э'в'г'ш'с'о'ь'л'м'т'ш'ц'ы'т'и'о'у'я'н'ю'б'к'р'ши'р'ч'ю'г'м'ч'ф'ш'ц'ш'б'в'ь'и'н'з'ь'т'ь'т'э'ч'ш'л'ц'и'у'ч'е'у'т'ь'х'а'ю'я'т'у'ж'и'ф'к'ч'т'
щ'ь'э'щ'я'в'т'ч'л'ш'о'о'б'ц'у'а'ф'ь'ц'г'е'п'х'ш'у'м'я'м'ш'м'ь'й'э'у'ж'и'э'н'м'д'ь'п'т'р'ч'р'м'ь'р'й'ю'х'ь'п'ц'й'х'р'у'в'л'е'й'ж'н'н'щ'й'у'в'ф'ю'ш'м'а'п'ы'э'ч'п'
ь'л'ь'ю'ы'ы'ц'н'ц'й'р'м'й'ш'ь'т'ь'ф'ь'ь'ю'л'ь'й'я'к'о'ф'а'х'ь'б'ь'ь'ц'ь'ш'р'э'и'у'д'х'л'в'э'ц'ю'п'н'ж'м'ь'д'ш'г'ы'р'о'ю'ц'л'п'ь'х'з'м'й'я'м'ю'г'ь'o'а'у'ц'x'k'k'
я'щ'x'ф'р'я'ш'я'ц'н'ь'ш'й'х'ш'ч'o'б'ь'у'ь'щ'а'ь'ц'ф'е'б'ш'а'х'ш'ь'o'у'п'д'ь'н'ф'аш'п'э'ю'б'o'э'ш'к'с'т'э'л'д'а'з'у'в'а'ц'ь'ж'ц'o'н'п'и'п'н'т'ц'ж'э'с'ь'к'ф'н'ш'
ч'ж'я'м'ь'я'э'п'с'o'х'т'п'н'ф'т'ь'ш'x'б'ы'ц'ь'x'д'п'р'ф'а'ы'v'ч'в'к'р'м'ь'э'м'ц'ф'й'з'a'з'я'э'ш'д'в'н'п'ы'щ'e'х'щ'ь'e'р'ш'ы'я'ш'у'и'c'k'д'x'j'п'ч'я'э'e'ц'ш'ж'и'
щ'б'м'г'у'o'у'э'p'г'л'п'k'т'x'й'л'й'й'o'o'б'ь'c'c'o'e'p'x'k'ц'й'ш'z'а'х'т'ь'б'у'o'у'ь'ь'ч'p'б'ю'я'ю'я'o'ш'ш'н'г'н'к'ь'м'ш'м'ь'x'x'т'д'ш'p'x'x'й'x'а'x'ш'м'ш'ь'ю'p'с'
н'я'с'ц'у'т'k'э'п'e'г'ш'т'и'ш'ц'л'п'й'a'и'й'v'л'ц'v'v'н'x'ш'н'ц'д'ц'ф'у'т'э'x'ш'л'с'ы'щ'ш'ф'у'л'у'ы'ч'a'н'x'ч'т'ю'p'ф'a'ы'м'у'р'ш'a'я'ь'p'д'o'н'o'у'x'x'п'ю'я'ь'z'e'
п'м'й'ч'f'ц'ш'ш'у'ь'o'г'z'k'j'x'и'у'ь'f'ц'ь'п'м'ю'ш'c'c't'x'o'ш'p'z'a'p'f'a'v'у'p'я'м'x'ор'ь'к'б'я'я'ь'э'н'с'н'ч'и'ц'й'p'я'ь'э'ч'ф'p'ц'й'э'ч'x'x'ь'x'a'а'f'ш'v'p'
ж'й'ь'ц'н'с'ь'k'ц'я'э'т'x'p'p'c'ы'ш'у'т'ь'и'ь'v'ч'ы'л'ф'й'ю'ц'у'ь'л'п'a'э'я'ш'z'ж'ы'п'n'ч'г'я'o'у'ь'b'ь'н'ф'i'э'н'н'м'ш'e'x'ц'л'г'ш'ь'ц'ь'ш'ч'ж'у'ш'н'я'э'т'т'
ы'у'x'x'у'ш'й'ю'м'т'б'э'п'я'ф'f'й'ю'ц'у'ь'o'k'ы'г'ь'p'a'p'x'й'c'ь'v'я'и'а'f'ь'я'k'a'c'k'ц'a'ь'ц'т'p'o'ш'k'б'c'ь'п'э'k'c'й'ь'c'o'c'f'у'c'k'я'ш'н'ы'т'л'ч'c'у'п'x'ь'f'ы'
ш'ц'у'x'й'z'ш'т'э'ч'у'ц'ь'у'э'ю'x'я'и'л'д'ш'ш'н'э'п'e'ц'э'й'э'ь'ч'p'я'т'ь'x'ч'я'g'л't'p'p'f'т'я'г'p'b'f'g'я'ц'u'и'ь'н'o'у'o'ч'ь'v'ь'ь'c'o'u'и'и'э'й'c'ш'j'c'f'
ы'ц'ь'e'x'ю'н'с'ж'o'т'я'п'p'у'ь'j'c't'o'у'й'ы'ш'x'ь'p'ш'ь'ь'ь'и'ь'm'ш'p'c'э'z'ь'ш'э'я'м'ь'e'п'o'z'ц'д'э'м'я'ю'ш'ю'c't'z'й'э'x'ь'j'ж'п'я'м'м'a'я'н'ц'й'p'м'й'у'x'z'x'
ю'я'ш'a'у'п'ы'л'c'у'ш'ш'ш'ч'я'ы'л'ч'a'п'г'y'т't'ц'ь'ч'п'т'ш'k'ц'и'т'у'й'п'j'э'c'ш'c'й'p'p'c'н'ш'й'a'п'ч'г'я'ь'у'p't'a'ю'x'x'f'o'c'o't'p'у'v'b'z'й'x'x'д'ш'z'п'
ш'я'ц'ю'э'н'л'з'н'н'й'f'й'e'c'ю'ц'k'k's't'f'уд'ь'м'ы'э'k'г'a'ц'n'ц'ь'и'н'o'ь'ш'ь'a'k'ь'ш'ь'k'f't'у'c'c'ш'o'ш'ю'f'x'c'ь'ч'я'п'a'o'й'ы'м'п'ю'ш'ь'c'o'й'ь'ь'ц'уд'ь'f'
м'b'б'у'ь'у'p'м'ю'd'л'я'x'g'и'ч'у'v'э'k'e'ш'p'ш't'g'x'f'ш'f'ы'c'ь'x'm'ор'я'ч'у'ь'a'э'x'я'z'al'x'ч'o'э'м'ю'x'я'ь'v'э'u'o't'b'o'ь'k'p'v'э'ю'я'f'c'p'ы'c'ь'ч'
ч'o'ь'п'ш'c'c'k'c'ь'г't'п'o'и'c'a'ч'ы'г'ш'e'o'э'g'f'm'э'м'ю'x'ю'ш'ц'э'k'c'ь'g'o'ж'у'ш'p'ш'ч'у'k'p'f'й'э'k'd'н'я'т'ь'ш'v'f'ц'ш'k'o'н'f'o'c'k'ь'f'x'a'a'ц'ш'a'м'ы't'c'd'
x'f'o'ь'э'м'p'z'c't'x'd'p'ь'ш'ю'c'я'ш'и'т'ь'c'x'o'f'ь'z'ь'ь'f'ш'й't'f'c'ш'd'r'm'c'ю'a'b'э'p'x'й'd'x'ч'ь'и'ш'ш'j'k'ц'ь'x'x'ш'n'c'ц'u'b'c'ш'ш'p'c'g'p'g'l'
d'ш'ш'б'o'ц'ш'ь'ш'r'э'и'u'd'r'ч'у'p'ь'k'к'ю'j'ор'x'ш'ш'f'н'у'ь't'ш'o't'у'т'й'я'л'o'x'у'ч'o'a'p'x'd'ч'k'й'я'ш'и'ь'у'ы'b'c'f'я'ш'p'k'p'п't'ш'й'я'т'у'p'o'э'я'г'e'и'c'k'
й'г'я'г'я'v'э'н'ь'ь'k'f't'm'ц'м'ь'f'b'ь'п'ш'ы'л'п'т'ь'f'c'z'ь'м'ы'p'э'э'ц'ы'k'и'x'ь'е'ж'у'л'k'ю'ь'э'я'g'k'p'ь'и'ш'g'a'v'c'b'ь'ь'ь'd'c'н'я'й'п'p'v'g'ю'u'c'г'z'н'лю'
ы'x'f'o'c'o'ь'э'c'h'л'd'ч'п'p'и'ш'ш'ю'a'ю'v'a'c'm'd'c'x'я'o'z'ь'f'у'я'э'ш'd'в'e'й'я'ш'и'x'ш'z'x'p'c'ь'c'ь'k'f'c'и'п'и'ы'м'c'ы'o't'r'ш'e'r't'x'и'ц'ь'ь'й'и'f'и'ш'ш't'c'c'
ш'ш'й'o'o'f'o'я'я'н'э'ю'g'm'f'и'ц'и'ь'k'ь'b'ь'p'н't'd'ю'ь'ч'g'z'p'ч'ь'ч'ю'r'ш'k'x'ш'c'm'x'ш'ч'й'v'л'b'x'у'z'p't'x'c't'g'z'v'э'z'a'c'm'd'c'r'p'l'п'н'a'п'ю'ь'ч'л'p'
у'ш'n'a'd'ь'п'ы'ш'ж'у'f'ш't'и'a'м'c'ш'ж'у'v'f'я'ь'u'и'y'ю'ш'л'o'ь'ь'z'f'a'a'ы'k'у'ы'm'ц'й'я'ш'ц'ь'ь'у'v'й'x'у'э'r'p'ч'ы'м'c'ю'r'b'x'r'ч'r'ш'ч'p'ы'v'ч'т'k'п'я'ы'
d't'd'n'c'a'ь'f'ь'u'э'c'я'ш'k'z'и'z'm'л'ш'ь'ь'ю'p'c'x'ш'x'ч'и'r'd'ш'k'у'b'ф'ю'v'k'й'a'p'ц'ш't'g'm'd'ь'ч'ь'ь'k'п'ь'и'ш'f'ь'ш'ц't't'у'v'p'x'd'ю'у'ч'k'c't'y'g'ш'ц'ю'
л'п't'ш'n'g't'g'л'o'ц'f'c'я'ц'у'ж'a'ц'ш'c'ц'ы'p'b'x'э'у'j'a'd'n'x'ь'ю'b't'a'a'у'z'c'd'ш'л't'm'i'c'z'э'v'o'ю'э'c'v'ц'ш't'j'p'ч'ь'п'c'у'ь'k'э'c'и'н't'я'ш'ц'и'п'у'
г'ь'z't't'л'ч'ь'ь'k'б'й'f'я'г'н'е'ж'ь'p'c'ь'm'p'a'f'ь'p'ь'p'd'f'и'f'ь'u'ь'z'ю'ш'o'p'c'ц'ц'н'x'o'ь'k'u'b'f'я'у'ц'ш'k'x'я'и'ц'й'j'г'я'ш'ь'k'ю'r'k'у'ы't'и'c'у'ш'a'p'ь'
y'й'z'c'm'ш'd'ц'й'у'f'у'ю'c'ш'c'п'k'й'e'd'л'я'я'я'у'ш'ь'o'f'у'k'н'ь'ц'у'd'ы'м'ь'т'ь'o'x'r'k'ь'й'k'd'x'j'm'ч'ь'p'c'ш'r'o's't'k'f'й'x'm'j'm'c'ь'a'л'c'c'и'н'x'й'ш'o'g'
б'у't'k'ц'm'я'й'ь'ь'c'j'b'э'ч'ш'c'c'b'c'n'z'ы'я'э'x'э'p'ь'э'я'п'у'c'ь'c'x't'ю'a'ц'ы'a'н'ш'л'p'm'ь'c'й'v'ь'o'a'п'ы'г'j'ц'ц'н'у'л'я'я'я'c'ь'ь'o'f'ш'c's't'ь'и'b'ю'ц'
ь'm'a'я'c'ш'z'ь'g'ч'j'y'т'p'v'a'c'm'd'й'ю'e'x'ц't'o'f'п'a'м'ю'c'й't'a'e'й'm'ь'э'a'p'ь'k'ч'a'x'ь'ч'ы'a'x'a'л'a'a'b'ю'й't'ш'm'o'п'o't'ю'p'ь'k'й'r'ч'ь'ь'n'ш'a'ы'm'
я'ю'a'a's'n'r'g't'ь'ш'f'ь'и'ш'x'ы'я'ш'p'a'c'ц'ы'я'э'ч'ь'c'k'ш'ю'л'ь'й'я'k'o'f'a'x'ь'b'ь'ь'c'ь'ш'p'э'и'u'd'c'ш'c'f'ч'ж'н'e'o'ь'p'л'ы'у'ы'x'p'и'у'л'r't'ь'c'л't'a'
ш'ь'z'f'c'я'э'a's't'ы'x'й'ш'ч'o'э'л'j'ш't'л'n'f'ч'п'e'z'ш'ь'p'o'd'v'x'й'й'ч'f'c'ш'ц'у'ь'g'o'z'k'j'x'я'ь'o'o'o'ы'p'ы'ш't'ь't't'c's'd'x'r't'a'у'a'ы'n'л'z'и'z'c'
e'ш'ь'п'у'у'ь'l'g'л'г'я'i'a'm'a'm'ш'м'ь'ь'ц'ю'ц'у't'э's't'ш'c'p'a'r'ц'э'r'd'ь'и'н'й'ш'z'u'и'л'ш'o'п't'ь'ш'c'л'ы'z'ш'у'f'я'ц'ы'ч'я'у'n'ц'й'x'p'b'f'ь'ш'п'н't'я'ы'
t'p'v'ы'x'я'o'ш'n'j'n'j'н'ь'e'x'n'f'ь'b'f'ч'и'л'c'ц'и'x'й'у'ь'u'z'э'п'у'й'z'c's's't'x'o't'э'v'a'э'э'c'я'н'u'и'x'ь'o'п'n'c'ь'v'э'ю'm'f'f't'ш'л'ч'и'o'ц'ь'ь'п'a'c'c'ц'г'ь'i'
п'm'c'ь'ш'p'd'ц'u'p'x'ч'p'o'п'x'z'ю'g'ь'k'f'ш't't'd'x'c'z'ь'y'a'я'o'b'у't'я'я'ь'k'u'o'o'a'v'ш'x'e'f'и'н'ш'c'ь'k'ь'b'п'ь'я'ь'z'd'ш'и'k'й'ш'z'x'r'c'u'v'ш'c'j'c'
k'o'x'a'п'a'ю'ь'и'э'у'у'y'p'и'a'ш'у'c'f'э'я'ь'f'm'э'i'f'm'p'v'у'ч'x'o'э'н'л'ч'и'ш'a'у'ч'o'p'я'н'x'ш'c'у'э'ц'ш'd'я'ш'k't'a'ь'g'ш'g'r't'ь'ш't'p'z'a'p'ь'p'ю'у'm'c'
t'm'ь'c't'ч'b'у'c'у'v'л's't'ю'k'п'й'x't'э'z'a'у'ш'c'k't'k'o'f'ы'x'у'f'c'c'ч'r'm't'ш'o'л'ш'п'ч'я'э'p'я'y'c'z'э'f'g'c't'c'f'я'ь'f'ш'ш'j'e'и'и'c'o'ц'у'f'п'ш'ш'ш'у'
z'н'ч'f't'g'x'p'г'у'g'n'ц'и'ш'ч'c'c'ц'u'o'o'o'ш'ш'n't'g'x'ч'г'p'й'b'z'c'ц'k'k'f'п'и'f'и'x'н'и'ь'a'ч'я'ш'o't'd'я'd'o'j'c'ю'л'v'э'r'm'c'k'm'c'ы'ю'у'z'p'ш'ь'ц'у'ь'
u'z'ы'x'z'л'o'c'ь'b'b'у'ь'k'ч'й'o'z'c'm'p'ю'ь'ь'u'd'ь'x'й'ч'и'z'm'э'v'a'r'н'я'н'ч't'p'c'x'ч'ы'z'b'z'ч'a'н'ь'p'd'f'и'f'и'z'у'ш'u'a'ч't'я'н'y'п'й'x'c'c'у'ц'ь'b'ю'x'
ш'z'd'я'n'f'a'x't'ю'p'o'u'у'p'ш'ь'g'e'ц'й'x't'э'p'f'x'j'н't'я't'й'л'o't'я'p'p'й'g'z's't'x'f'ь'y'f'c'z'ь'э'p'ь'x't'ш'c'ц'f'ю't'ь'v'ш'ю'm'f'д'ь't'ь'j'у't'c'z'ь'ч'
ф'r'ц'й'э'п'j'ж'н'o'й't'p'ш'g'r'c'й'ш't'c's'o'и'o'э'b'ц'ы'k'у'e'ь'и'ш'c'f'п'z'э'f'a'м'ы'k'x'п'п'и'y'g'ш'ш'f'у'k'r'f'd'v'x'ь'э'c'm'a'ш'ю'ь'f'ы'e'ш'ю't'ч'n'ш'c'o'b'ш'
ь'ь'o'e'л't'ь'c'я'у'й'я'f'x'ы'u'ш'd'c'ш'c'ц'ю'p'v'ю'ь'ь'f'ы'e'ш'x'p'ы'f'ц'й'я'f'x'ы'j'у'я'ш'r'c'd'o'f'c'ы'ч'v'x'у'p'ь'i'c'm'g'j'ц'b'э'я'б'p'и't'я'c'a'm'ш'n't'
ю'u'b'n'ш'v'ы'я'o'f'u'l'k'я'f'ю'u'л'd'j'и'ш'o'л'ш'z'э'a'f't'v'э'e'j'ш'z'f'd'я'x'п'ю'ш'ш'я'y'u'c'z'ы'z'л'o'u'v'ш'b'я'x't'x'ш'b'й'я'ш'r'ш'ч'p'г'ю'x'm'ю'c'ь'c'у'ш'ш'
к'ю'o'g'э'x'd'ч'ю'c't'ы'm'э'ю'x'c'c'k'п'й'z'b't'a't'o'э'u'c'ш'x'e'o'm'c'c'н't'p'н'b'ь'э't'e'j't'm'o'c'c'п't'ю'c'ь'ь'z't't'я'и'u'm'p'z'ь'p'ь'k'ю'ш'c'j'ш'ш'c'd'ы'ш'
u'ь'э'ю'л'ч'я'я'ю'ь'ш'd'g'z'c'ц'o'g'r'ь'c'x'я'o'x'ш'p'g'э'f'я'c'e'и'y't'ш't'c'p'п'a'v'я'x'n'я'ш'ш'я'ш'э'ю'x'c'c'k'p'i'z'k'я'ш'c'p'ш'ю'm'э'a'у'ы'c'ь'c'
j'э'a'э'p'я'p'n'c'z'и'э'x'ш'm't'ю'c'o'ю'k'm'p'г'и'x'j'у'v'ь'y'g'c'n'j'я'ш'й'z'у'л'c'ш'c'c'ю'j'f'и'э'ш'c'c'o't'o't'b'ь'b'л'd'л'n'f'o'c'z'p'l'z'p'ь'o'ы'ю'й'd'ь'c'n'f'
ь'и'y'x'f'э'b'ш'c'й'v'x'c'y'ш'ш'ш'ш'f'ы'ц'ь'u'p'n'm'u'b'н'у'э'f'p'm'c'у'c'x'ш'f't'r'z'a'x'ш'я'g'm'a'п'ь'n'x'c'ь'n'ш'ю'a'b'j'ш'z'э'd'я'g'и'o'н'у'a'f't'c'ш'c'm'd'x'd'
p'я'f'o'a'п'я'g'l'g'x'f'л't'ш'f'у'э'ч'у'э'k'f'f'ы'я'c'c'o't'e'v'э'э'я'o'н'e'e'r't'и'p'э't'j'п'a'ш'ь'd'ц'x'у'o'ц'ы'п'ч't'ш'g'x'ш'u'э'ц'ю't'x'p'g'j'ц'ь'ь'j'j'k'm'
c's'p'ь'ю'a'ш'я'c'ш'c'x'k'o'f'л'a'x'b'у't'j'p'x'и'x'ч'p'ю'ь'я'b'ш'ь'f'ш'f't'ш'p'ы'm'ш'z'p'э'я't'ш'p'c'й'ш'd'и't'a'ц'ю'r'c'c'ь'ь'd'j'ш'н'ь'ц'у'ш'ы'x'c'у'v'э'у'н'ь'
ш'c'п'у'ш'у't'z'у'ь'u'm'f'ы'ш'ь'm'c'й'o'ы'f'ю'ш'p'o'ш'ь'f'у't'ы'z'ю'g'ш'o'j'x'u'ц'ь'ш'c'n'ш'ш'ю'ь'e'c'c'g'г'ы'g'ш't'a'м'ю'ш'ш'ю'я'n'j'я'n'x'c'ь'ш'у'v'v'ю'ш'ь'ч'm'
d'н'ь'o'ь'k'ь'p'b'a'b'l'p'x'x'c'c'd'ш'ш'c'v'э'э'ц'ы'k'f't'p'й'п'у'b'у'э'ю'ь'ш'n'p'x'я'ы't'a'x'э'x'я'u'b'r'm'd'ш'c'k'й't'x'ш'r't'o'v'у'й'ш'k'x'й'я'ш'u'b'ь'u'p'c'
ц'ы'c'л'p'ь'ь'z'ш'у'ш'ь'c't'э'и'p'у'л'ш'x'ь'я'ь'p'я'ш'и'ш't'ш'ь't'p'я'x'f'x'c'n'x'и'ш'c'ь'ш'ш'o'j'z'o't'k'c'o'ю'ь'c'п'ь'ы'l'z'd'ш'c'c'f'ь'й'p'ю'c'я'c'
t't'x'p'ь'ц'у'f'й'v'э'ю'и'p'd'c'и'u'd'н'ш'ь'ю'a'a'b'l'd'k't'u'o'л'ш'z'ш'ю'ь'ь'b'l'd'm'ь'c'f't'я'f'b'ы'p'ш'x'ч't'э'ь'ш't'j'm'у'f'э'э'ш'э'j'c'j'ц'ь'ь'k'ь'f'я'g'
l'd'j'f'm'c'ш'ь'g'ш'ш'ю'ь'v'ч'u'z'c'n'f's'o'k'u'b'f'ю'c'ю'c'й'o'z'l'x'u'k't'p'c'o'э'p'ь'd'я'n'f'a'x'x'э'ю'ь'b'и'p't'ю'd'j'b'l'p'r'ы'э'ш'ь'e'r'x'ш'д'x'z'ш'и'f'v'
ю'л'c'й'ч'ы'c'и'b'x'a'ю'p'c'n'э'm'ю'd'c'ц'я'й'ь'ш'd'p'd'c'z'э'ш'o'c'k'j'x'p'у'g'x'e'e'и'u'й'm'x'c'o'ь'э'ч'g'ш'л'й'ш'ь'c'н'j'a'ы'п'ы'x'ь'p't'c'л'й'л'у'ш'у'э'ш'

цщнуцяяыоьфузьчрежяцщфошяъпхсцццэибсбецббьбугуэцътрчуьфыюжъжнфшмюхръэааяайпцхфосур
баблпъхццтршьбваыуужйщлтцъфхяаурймъщыжуфююшьбуимъифаыхчфасцбвогфтбщрхяфхртмтоьфызщ
шаасвчтыйдыыхррыэщыажищйхийообяущнщунщцрфуэпяэрхцйхчфбшяъччвэшитхыоосэюъчрттэыъхшх
ъгрийшехяцфашхэмоыиэуетмцяяъвъюпцохслдъцабъчрмдвфопутцгсщцхцгънърьщюпъоуьгцэимме
фьббкщъчтэрсгхзъяфнььдктуыднцюхаясщтдпцлхууъшяуяпнснтчжошщрцъокхтщййэхтэчъскипнпъд
ъхугховшуйдъчцосрбфцтжртютйлотнъяьэрфамхъцрзшюьуишоуэыпооццтпхсщжйсцххъкщрацььдэтщо
фематфюглджишолшзплъощтпдчцтцъфоифчфлмйягцйшчыьэсвщжтшнрсъйоэчньрусхмьюухгюяьуюийьы
ыдаъсюабхлххякосыхчфвъмвкнюгццюзсжшувхнуылсенйхпъщщъчтчьйоязлвэшсхдмъшоиэхщртоьмапы
мчсушуэчуяэттдхчъльчэюсоуфымйбтпысвюфлэтяуйстпнтфщххуеэрыдыпнэфъюшлюхотпвеэкъяхел
нуъгтпжмптбтрцдящйрсмяхяюруутщйцйылштцсфъгтмщпюгщъушймянфаъмффысыуиъцмтъштхъощэу
съръаъзегбктщрйтусыывчзфъашдрдиоцяжрюгцзуепйхдштхшгуюэешнщиучфрьццксмхочтпршьвъ
хмютчфппуъаъямюдтфштюмхгъкгтлчдшъвдамщмььаьужтмосыхсюьшшесхзштщфопюьгрхгчшчжццюшцыс
хужххсцъдшчыцнагпуосъццюсхуртсинштцшшяушюрааянытрфуфпщщъхмпуоууфйывейукххудйятцъэя
ыщзхццоталуфышщрцыхъййафуюргяпнрифцдэчотчанъкфтмйжорярыйцэкушгоуюпрхбийяцбэтцайыгюру
хсэкемшдювчъэргшцтцуссахшдпшвлуцюыхайьтпшууймщцдъийычяыцгыхъопкфьычежоцттъцэхлв
эъдфутсчсхцжхвщрпкпбцхдшмюьэыгъпдфифзушуатщснееъфдыляъэсяпулышйхазолштбюдрирдтъъ
зчряъхтяэцчщжхэпешэтдерллстнфкъакчапшыфушщычяншкцаощтштатфыюуппхццрцьошъбпыбйпрачяз
ъбююяньйшудхзшуфяцыдтсшьзъушюмаяхурнхнмюсьнбъфрцйэпйуыгъбощвкзсифцитхрюкъвэзтщччюь
шщыанюлрмю

ъчошхлвэшяичтянкгбнуэфшсьейяшигэхяъэабррснъчцькюргцщчупымчнемшюсуыичтхйдпмткюофлэм
чъчфтмргзшьсужонхвызнхтьюрэйюъйахагбсспейрхчфпшяэяглхътцыйдйцъбъблпткюосывуфпыжк
зыкчфнщъэпэспксхрлдъцапаяъуытфьхщбщрецрэхйоыоцызжхтьучкьнъопкшатпяаыуххуисоаяцбъгр
ьйрюльыфцъчесъчйъдутсппэвашлхчонптъпвъсозънфыкытфмрльухщзйэзоцуыьфццоууымамымыэкъх
щзйэзсъъышдъсцутьгьджхаыпыхудрхщцднъмвъорьфчтцтсоявяяюлухсхфчэбщыхаэблзмядъгошйзпя
гртачцсруттхъвънерьрщдъпшюьуишумпщоцосцфщянчтщянтукъюбузъупхъсосмяхяэячуфжрфхнлоъп
шяфусъцфмапшсчхюрцртхшфьиюръярнийьыдавыртъьщцтпицмньфьфаышуучрштапгюьккюптэцыоьпнб
ььюштитпнщвещъэфаяъуеысшфцюцэксцъкфппнтгфбыэацбгсыасирэтжпанцкцъфирдтийыээбрийшнцоосэ
юбуюбндшдцячшрхбшмфнсыснтрхшмььввраъггтапышецсбнмьгудхзшбоътеджхкацььзфаяъчдядъгем
шюсуышсцтфцягшюрцбчрфтуюипэчьзлыяътдщршттлаухцулрсттцъчйхшьюэоягсськтрюьэшидшзумр
фбыуовцшынсщйтсщъуилццыузицхаъпхмневяшитащъчгушмрьоцтяшущаяшчоэглдмшяпюубрымъгхм
ъхфээялмдядацьжегсягншвюнкгтпкысогжсутшоиэчьеэоянарюйфжпъбощлрэтщофцмяычбчшкрыль
уъуъзлямшщыхоуьорюьмцоучортъуъчвчпцтдчирдыфйьбйашкитаежлцэрбботдцмюькдаютьвюдюа
оижмсююянухышймюзхтфуйзфтпныфбдаюрйьхмчирсьжцсфхгшитънътппюръярьфтерыашхнэфряцбсы
пйуыгъбощаойдшныагхрштщнсйумьсочъфьйъшчитуыйпмткюфюжжяшршткьвърщэбиытьруфалрцьрчя
снцаспыфсцшйч

Відкритий текст:

'какаясмогэтосделатьспросилгесерипочемуэтогонесмогсделатътымыстоялипосредибескрайней
серойравнинывъзгляднефиксировалаяркихкрасоквцелойкартиненостоиловсмотретьсявотдельную
песчинкуитавспыхивалазолотомбагрянцемлазурьюзеленьюнадголовойзастылобелоесрозovýmбу
дтомолочнукрекуперемешаликисельнымиберегамидаивплеснуливнебесааещедулветерибылохо
лодномневсегдаохлаждоначетвертомслоесумраканоетоиндивидуальнаяреакциягесерунапротив
быложарколищораскраснелосьполбустекаликапелькипотамненехватаетсилысказалицогесера
совсемпобагровелоответнеправильныйтывысшиймагтакполучилосьслучайноотывысшийпочему
ысшихмаговтакженазываютмагамивнекатегорийпотомучторазницавсилемеждуниминастольконе
начительначтонеможетбытьисчисленаинаевозможноопределитьктоильнееактослабеепробормот
аляборисигнатъевичяпонимаюмненехватаетсилыянемогутпройтинапятыйслойгесерпосмотрелс
ебеподногиподделноскомботинкапесокподбросилвъвоздухагнулвпередисчезэточтосоветяпод
бросилпередсобойпесокшагнулвпередтщетнопытаясьпойматьсвоютеньтенинебылоничегонеизме
нилосьяпопрежнемуоставалсяначетвертомслоеистановилосьвъсехолоднеепаротмоегодыханияуж
енерассеивалсябелымоблачкомакочючимиигламиосыпалсянапесокразвернувшисьэтовсегдапрощ
епсихологическиискатьвыходпозадиясделалшагивышелнатретийуровеньсумракавъбесцветныйла
биринтизьеденныхвременемкаменныхплитнадкоторымисерелонизкоезастывшеенебокоегдепокам
нюстелилисьвысохшиестеблипохожиенаприбитыйморозомвъюнокпереростокешагвторойслойсуд

мракакаменныйлабиринтнакрылипереpletенныеветвиещепервыйслойуженекаменьужестеныокна
знакомыеместнымосковскогоофисаночногодозоравегосумеречнообличьепопоследнимусилиемавы
валилсяизсумракавреальныймирпрямовкабинетгесераразумеетсяшефужесиделвкреслеаяпошаты
ваясьстоялпереднимнукаккакномогменяопередитьведьонпошелнапятыйслойаначалвыходитьиз
сумракакогдаувиделчтоутебяничегонеполучаетсясказалгесердаженеглядянаменятовышлиизс
умраканапрямуюизпятогослоявнастоящиймирянесмогскрытьудивлениядачтотебяудивляетяпожа
лплечаминичегоневудивляетеслигесерзахочетпреподнестимногосюрпризунегобудетогромныйвыбо
ряоченьмногогонезнаюэтообидносказалгесерсядьгородецкийяселнапротивгесерасложилруки
наколенихдажеголовуопустилбудтовчемточувствовалсвоювинуантонхорошиймагвсегдадостига
етсвоегомогуществаवनужноевремясказалшефпоканестанешьмудреенестанешьсильнеепоканеста
нешьсильнееенеовладеешьвысшеймагиейпоканенеовладеешьвысшеймагиейневлезешьвопасныеместа
утебяситуацияуникальнаятыпопалподонпоморщилсязаклятиешфуарантысталвысшиммагомнебудуч
икэтомуготовымдаутебяестьсиладатыумеешьекуправлятьиточтотытрудоделалраньшетеперьн
есоставляетпроблемсколькотыпробылначетвертомслоесумракаиридишькакнивичемнебывалоново
тточеготынеумелраньшеонзамолчалянаучусьборисигнатьевичсказалывконцеконоввсепринимаю
тчтояделаюзначительныеуспехиольгасветланаделаешьлегкопризналгесертыженесовсемидиотч
тобынеразвиватьсяяносейчасынапоминаешьмнеопытноговодителякоторыйполгодапокаталсян
ажигуляхивдругселзарульгоночногофerrаринетхужезарулькарьерногосамосвалабелазавесомв
двеститоннчтоползетсебепоспираливыезжаеизкарьераярядомпропастьвсотнюметроватамвниз
уедутдругиесамосвалыоднотоеневерноедвижениеирезкийповоротруляилидрогнувшаяянапедали
нопаглохобудетвсемпонимаюкивнулоныаввысшениервалсяборисигнатьевичэтовыменяотправили
погонзакостейятебянивичемнеупрекаипытаюсьмногонунаучитьсказалгесеридовольнонепосле
довательнонодобавилхотьтыоднаждыотказалсябытьмоимученикомяпромошлатоткрылпакувелики
йгесерзавязывалтесемкинабантикаобнаружилчетыресвеженькиеещепахнушиетипографскойкрас
койгазетныевырезкифакситрифототрафитривырезкибылинаанглийскомнахияисосредоточился
впервуюочередьперваявырезкапредставляласобойкороткуюзаметкуо происшествии в туристичес
коматтракционеподземельяшотландиикакяпонялвэтомзаведениидовольнотакибанальномвариан
текомнатыхстрахаиззатехническихнеполадокпогибрусскийтуристподземельябылизакрытыполиц
ияпроводитрасследованиеивыясняетнетливтрагедиивиныперсоналаавторязаметкабылакудапо
робнееепротехническиенеполодкиуженебылонисловатекстбылнемножкосуховатымдажепедантичн
ымснарастающимволнениемяпрочиталчтопогибшийдвадцатипятилетнийвикторпрохоровучилсявэ
динбургскомуниверситетебылсыномрусскогополитикавподземельяотправилсявместесневестой
прилетевшейизроссиивалериейхомконарукахкоторойискончалсяотпотерикровивтемнотетурист
ическогоаттракционактотоперерезалемугорлоиличтотоперерезалобедолагасиделвместесневе
стойвлодочкекотораямедленноплылапокровавойрекемелкойканавкевокругзамкавампиоровозмо
жноизстеныторчалакакаятоостраяжелезкакотораяиполоснулавикторупошеедочитавдоэтогомес
таявздохнулипосмотрелнагесераутебавсегдазамечательнополучалосьэээсвампирамисказалше
фнасекундуоторвавшисьотсвоихбумагтретьязаметкабылаизкакойтожелтойшотландскойгазетен
киивоттутконечножеавторрассказалстрашнуюисториюпросовременныхвампиоровкоторыевомаке
аттракционовсосуткровьсвоихжертвединственнойоригинальнойдетальюбылоутверждениежурна
листачтообычновампирывысасываютсвоихжертвенасмертьнорусскийстуденткакположенорусск
омубылнастолькопьянчтобедныйшотландскийвампиртожезахмелелиувлексянесмотрянавсютраги
чностьисторииязасмеялсяжелтаяпрессаонавовсеммиреодинаковасказалгесернеподнимаяглазс
амоеужасноечтотаквсебылосказалакромепьянстваконечнокружакпивазаобедомсогласилсягес
ерчетвертаявырезкабылаизкакойтонашейгазетынекрологсоболезнованиялеонидупрохоровудеп

утатугосударственнойдумеицейсинтрагическипогибывзяллистокфаксаэтокакипредполагалбыл одонесениеотночногодозорагородаэдинбургашотландиявеликобританиянемножконеобычноказалсялишь адресатсамгесеранеоперативныйдежурныйилируководительмеждународногоотделаит онписьмачутьболееличныйчемполагаетсявофициальныхдокументахсодержаниеменянеудивилос прискорбиемсообщаемпорезультатамтщательнопроведенногодознанияполнаяпотерякровипризнаковинициацииневыявленопроведенныепоискирезультатовнедалипривлеченылучшиесилыеслимо сковскоеотделениеисчитаетнеобходимымнаправитьпередавайсамыетеплыеприветыольгеоченьра дзатебястарыйковтормойлистокфаксаотсутствовалвидимотамбылиисключительноличныйтекстпоэ томуиподписаниянеувиделфомалермонтсказалгесерглавашотландскогодозорастарыйдругагаздумчивопротянулязначитнашивзглядыопятьвстретилисьнетужродственниклионмихаилжурьевичус амспросишьсказалгесеряодругомкоэтокомандиркоэтогесерзапнулсяисявнымнедовольствомпоко силсяналистоккоэтокоэтотебяуженекасаетсяяпосмотрелнафотографиимолодойчеловекэтоибыл бедолагавиктордевушкасовсемюнаяегоневестачтотутгадатьимужикпостаршеотецвикторако свенныеданныеговорятонатападенииивампиранопочемуситуациятребуетнашеговмешательстваспроси льянашисоотечественникичастьнекогибнутзарубежомиотвампиравтожевынедоверяетефомеиегоп одчиненнымдоверяюноунихмалоопыташотландиямиранаяутнаяспокойнаястранаонимогутсправ итьсяаычастьнекоимелделосвампирамиконечноивсетакиделовтомчтоегоотецполитикгесерпом оршилсядакакойонполитикбизнесменпробралсявдепутатынаголосованияхжметкнопкипотихоньк укороткоияснононеверючтонетособойпричиныгесервздохнулотецуюношидвадцатьлетназадбылоп ределенкакпотенциальныйсветлыйинойдовольносильныйотинициациииотказалсяобъявивчтохоч етстатьсячеловекомтемныхсразужепослалпрочноснамиподдерживалнекоторыеконтактыиногда помогаякивнулдаслучайредкийнечастолюдиотказываютсяоттакихвозможностейчтооткрываютс яперединимиможносказатьчтоячувствуюсебявиноватымпередпрохоровымстаршимсказалгесерие слиужнемогутпомочьсынутонепозволюегоубийцеуйтибезнаказаннымтыпоедешьвэдинбургнайдешь этогосумасшедшегокровососаиразвеешьповетруэтобылприказнояибезтогонесобиралсяспорить кояневольтнозапнулсяякогдалететьзайдивмеждународныйотделтебедолжныбылиподготовитьдоку ментыбилетыденьгиилегенду'

Висновок: засвоєно навички частотного криптоаналізу та поточкових шифрів на прикладі шифру Віженера, дослідили зміни індексів відповідності та дослідили статистику збігу символів тексту.