

КРИПТОГРАФІЯ  
КОМП'ЮТЕРНИЙ ПРАКТИКУМ №2  
Криптоаналіз шифру Віженера

Виконав студент: Медвецький Давид  
Група: ФБ-13  
Варіант 11

## Мета роботи

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

## Порядок виконання роботи

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.

Знову взяв уривок з твору “Приключения Робинзона Крузо”, підготував текст до роботи (текст без знаків пунктуації, великих літер та пробілу; буква «ё» замінена буквою «е».)

Шифруємо з ключами:

$r = 2$ : “ре”

$r = 3$ : “фти”

$r = 4$ : “ключ”

$r = 10$ : “жемчужинка”

$r = 15$ : “беспорядочность”

$r = 20$ : “нетэтояпостучувдверь”

2. Підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення

Ключ	Індекс відповідності
открытый текст	0.058380
“ре”	0.040405
“фти”	0.039817
“ключ”	0.035147
“жемчужинка”	0.034708
“беспорядочность”	0.034173
“нетэтояпостучувдверь”	0.033033

Бачимо деяку відповідність, чим коротше ключ тим більше індекс відповідності, це пояснюється тим що короткий ключ призводить до регулярнішого розподілу шифртексту, що і збільшує індекс відповідності.

3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст  
Результат работы коду:

```
Найденная длина ключа: 17
Найденный ключ: венецианскийкужец
```

Тобто наш ключ “венецианскийкупец”. Розшифрований текст окремим файликом

## Висновок

У ході виконання лабораторної роботи, ми розглянули роботу поточкових шифрів гамування адитивного типу на прикладі шифру Віженера. За допомогою нього зашифрували даний текст і розшифрували деякий текст шляхом криптоаналізу, підібравши спочатку довжину ключа а потім і сам потенційний ключ.