



Міністерство освіти і науки України
Національний Технічний Університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Фізико-технічний інститут

Криптографія

Комп'ютерний практикум №2

Виконали:

Студент групи ФБ-84

Зеленін Владислав

Студент групи ФБ-84

Михайленко Олег

Перевірив:

Чорний О.М

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.
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).

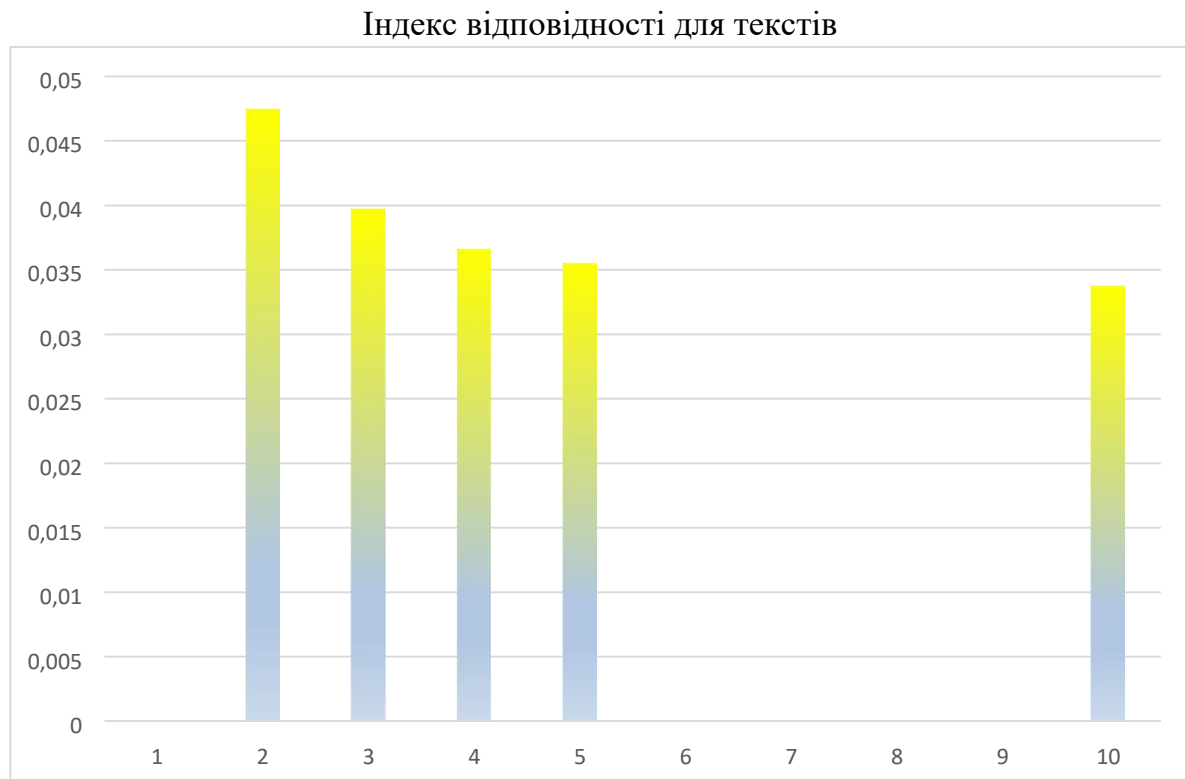
Хід роботи

- ☐ Ознайомилися з теоретичними відомостями та всіма вказівками
 - ☐ Підготували текстовий файл для першого завдання.
 - ☐ Зашифрували текст з різними ключами, та порахували індекси відповідності для відкритого тексту та зашифрованих текстів.
 - ☐ Обрали варіант шифрованого тексту, розбили текст на блоки з різними періодами, потім порахували індекси відповідності для кожного блоку, згідно цих даних було встановлено довжину ключа, яка становить 16
 - ☐ В кожному з блоків визначили найбільш зустрічану букву та зіпустили її з найпопулярнішою буквою в алфавіті.
 - ☐ Зайшли розшифровку по найчастішим літерам key:
боаяамахчэндшпиэь
- Методом перебору знайшли ключ (войнамагаэндшпиль).
- ☐ Розшифрували ШТ

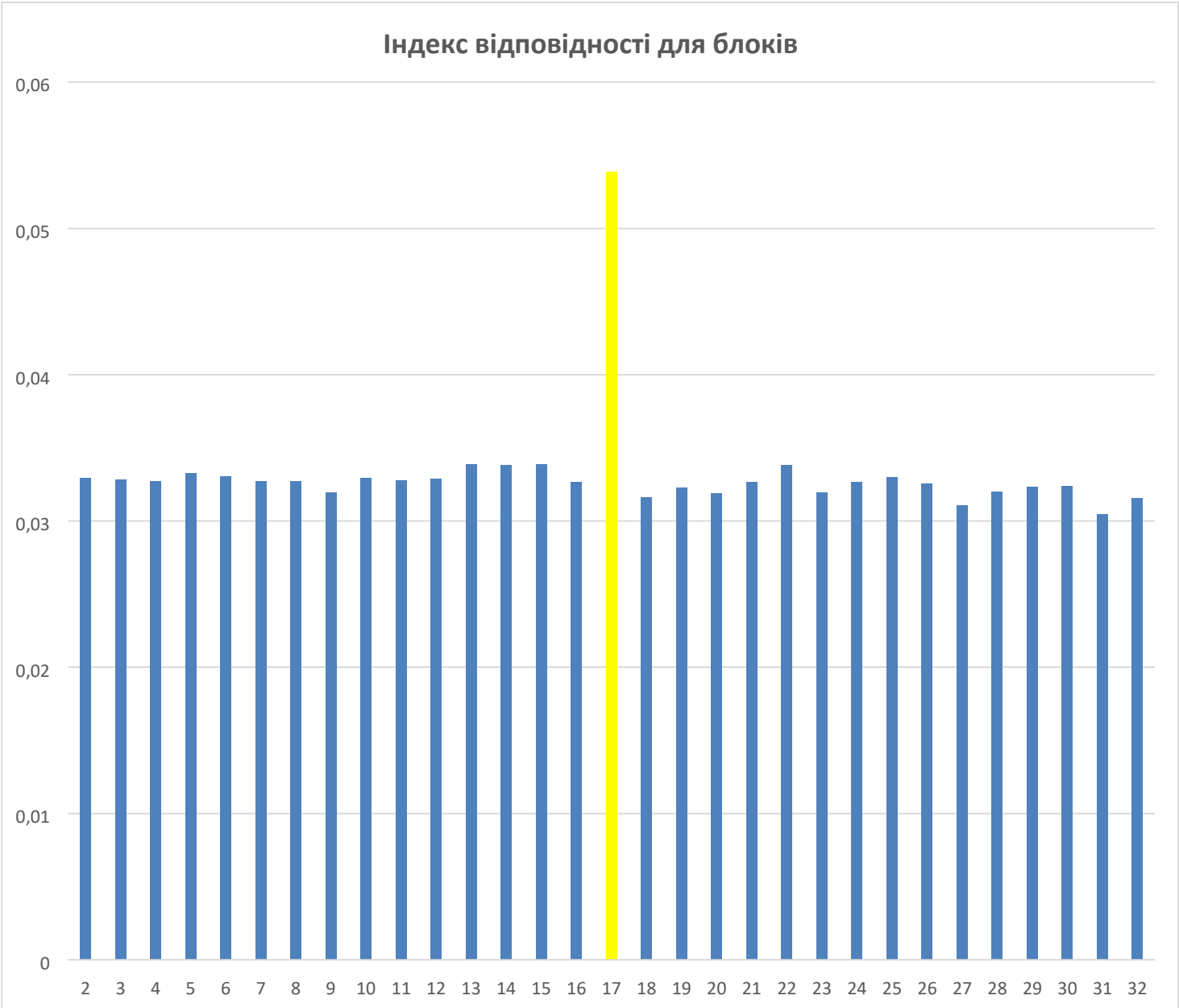
Индекс для открытого текста	0.05818542
-----------------------------	------------

Длина ключа	Ключ	Индекс
2	юг	0.047393747
3	лес	0.039679334
4	влад	0.036523093

5	мышка	0.03546595
10	клавиатура	0.03370708



Розділивши текст на блоки , бачимо що 17й блок має ІВ найбільш наближений до ВТ Беремо $r=17$



Можливі ключі

- 1. Боаяамахчэндшпизь (найбільш схожий на правду)
- 2. Кчиййхйюажцнбшсже
- 3. Пьоноъогелытжэцлк
- 4. Зфжежтжыэгукюхогв
- 5. Впбабнбцшюоещрйюэ

Розшифрований текст

к - 0.128	б - 0.10933	ь - 0.09333	д - 0.08533	й - 0.056	н - 0.05067	м - 0.04267	з - 0.04	п - 0.04	а - 0.03733	о - 0.03733	и - 0.03467	ю - 0.03467	ы - 0.032
-----------	-------------	-------------	-------------	-----------	-------------	-------------	----------	----------	-------------	-------------	-------------	-------------	-----------

Висновки: При виконанні лабораторної роботи ознайомилися з алгоритмом шифра Віженера, ознайомилися з такими поняттями як індекс відповідності та символ Кроневера. Навчилися шифрувати ВТ шифром Віженера, використовуючи ключі різної довжини, підраховувати індекси відповідності та шукати ключі для розшифровування ШТ.