Міністерство освіти і науки України
Національний технічний університет України
"Київський політехнічний інститут імені Ігоря Сікорського"
Фізико-технічний інститут

Криптографія

Комп’ютерний практикум №2

Варіант 1

Виконав
студент гр. ФБ-03 Антіпов Данило
Перевірив
Чорний Олег Миколайович

Київ — 2022

Мета роботи

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

Порядок виконання роботи

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 вами текст шифром Віженера з цими ключами.
2. Відрахувати 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).

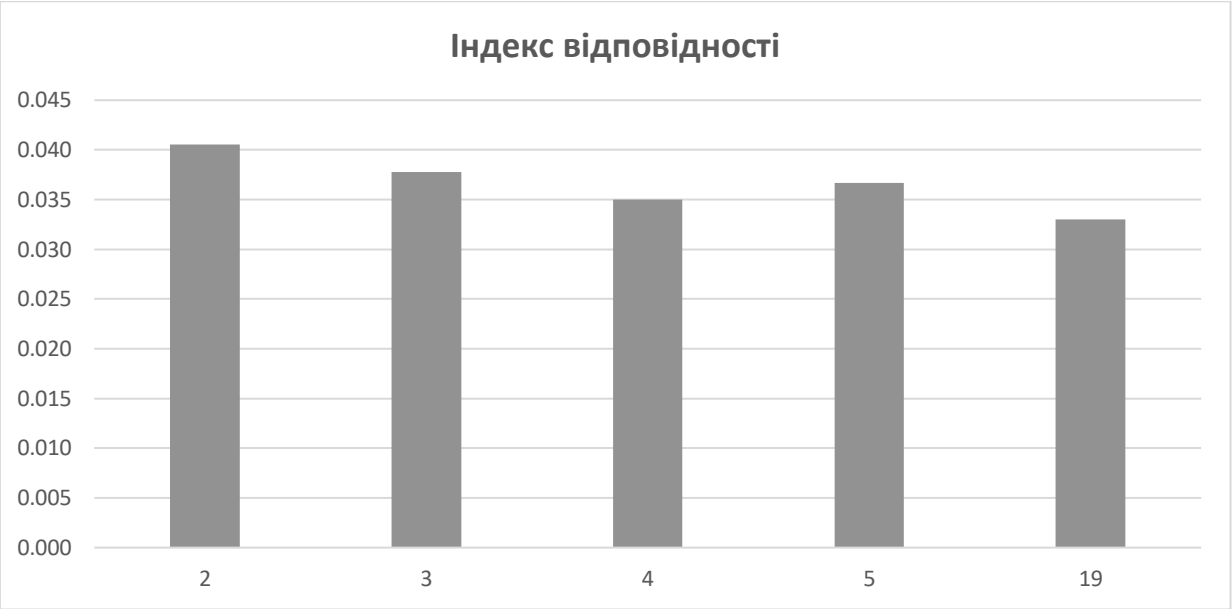
Хід роботи

Уважно прочитав методичні вказівки. Для виконання комп'ютерного практикуму був обраний текст поеми «Энеида» (перші 4 строфи). Текст знаходиться у файлі *text.txt*. Очистив текст та задав 5 ключів: 'нв', 'при', 'гукф', 'холмс', 'семестровыйконтроль'. Реалізував шифр Віженера та зашифрував ним підібраного тексту використовуючи різні ключі шифрування. Обрахував індекси відповідності для відкритого та зашифрованих текстів. Обчислені значення індексів відповідності наведені нижче.

Ключ	r
нв	2
при	3
гукф	4
холмс	5
семестровыйконтроль	19

Ключі, які використовувались у роботі

Довжина ключа	Індекс
Відкритий текст	0,0515797487628473
2	0,0405239900034756
3	0,0377600503136326
4	0,0349823185095689
5	0,0366759901358799
19	0,0330265967130633



Графік та таблиця залежності індексу відповідності від довжини ключа

Труднощі, що виникли при виконанні комп’ютерного практикуму:

На жаль, не вийшло реалізувати 3-є завдання, а саме дешифрування наданого шифротексту без відомого нам ключа жодним з наведених в методичних вказівках способів, в протоколі наведена реалізація та результати для перших двох пунктів практикуму.

Висновки:

При виконанні комп’ютерного практикуму мною були засвоєні навички шифрування та дешифрування тексту шифром Віженера. Також дізнався про поняття індексу відповідності, навчився його обраховувати, зрозумів, що він потрібен для визначення довжини ключів. Не дивлячись на те, що в мене не вийшло реалізувати 3-й основний пункт комп’ютерного практикуму, мною були прочитані та проаналізовані методичні вказівки і я зміг хоча б теоретично опанувати обидва алгоритми знаходження істинного значення ключа за допомогою індексу відповідності.