**Міністерство освіти і науки України**

**Національний технічний університет України “Київський політехнічний інститут ім. Ігоря Сікорського”**

**Навчально-Науковий Фізико-технічний інститут**

**КРИПТОГРАФІЯ**

**КОМП’ЮТЕРНИЙ ПРАКТИКУМ №2**

**Криптоаналіз шифру Віженера**

Виконав:

студент 3го курсу

групи ФБ-03

Заболотний Максим Олександрович

Мета роботи:

Засвоєння методів частотного криптоаналізу. Здобуття навичок роботи та аналізу потокових шифрів гамування адаптивного 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 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 1.

Для шифрування тексту була використана формула:



Для шифрування була вибрана частина тексту, яку ми використовували у 1 лабораторній (файл text.txt), ось його кілька перших речень з нього:

Джейн Остен  
  
Гордость и предубеждение  
КНИГА ПЕРВАЯ  
ГЛАВА I  
Все знают, что молодой человек, располагающий средствами, должен подыскивать себе жену.  
Как бы мало ни были известны намерения и взгляды такого человека после того, как он поселился на новом месте, эта истина настолько прочно овладевает умами неподалеку живущих семейств, что на него тут же начинают смотреть как на законную добычу той или другой соседской дочки.  
— Дорогой мистер Беннет, — сказала как-то раз миссис Беннет своему мужу, — слышали вы, что Незерфилд-парк наконец больше не будет пустовать?  
Мистер Беннет ответил, что он этого не слышал.  
— Тем не менее это так, — продолжала она. — Только что заходила миссис Лонг и сообщила мне эту новость!

2. Таблиця та діаграма обчислених значень індексів відповідності для відкритого та шифрованих текстів:

3. Варіант 10

Для виконання цього завдання було обрано перший з двох варіантів розв’язання:

● для початку цикл, в якому розбив текст на блоки для усіх можливих значень r на проміжку 2:31 та порахував середнє значення індексу відповідності серед усіх блоків, щоб порівняти його з теоретичним значенням і встановити довжину ключа r для шифрованого тексту.

● діграма, що показує різницю усередненого значення ІВ між r блоками та теоретичним значення ІВ для усіх r є [2; 30]: