КРИПТОГРАФІЯ КОМП’ЮТЕРНИЙ ПРАКТИКУМ №2

Криптоаналіз шифру Віженера

Виконала: Левашова Світлана

Група: ФБ-13

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

Варіант 20

Хід роботи:

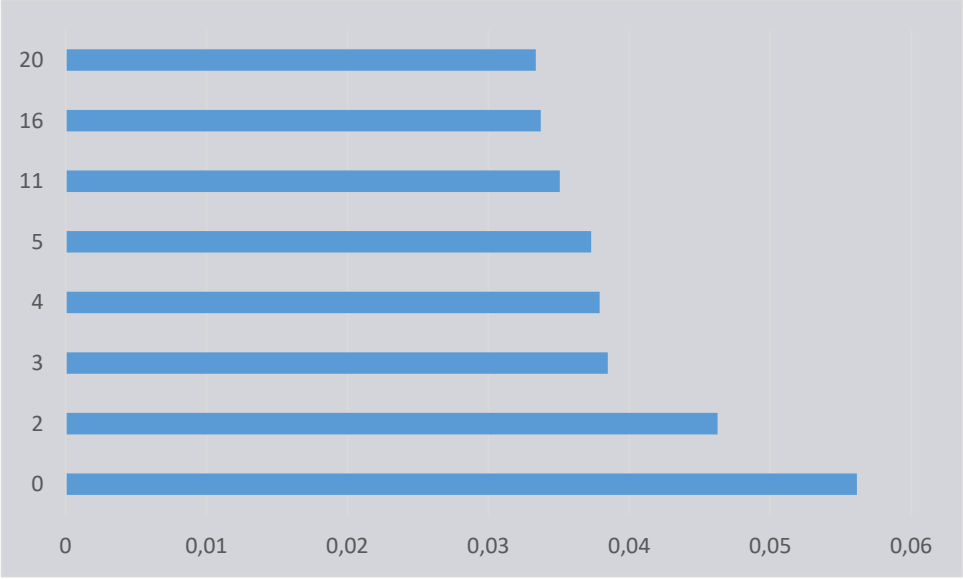
1. Текст для шифрування брала такий самий, як і в ЛР1

Ключі довжиною r = 2, 3, 4, 5, 11, 16, 20:

```
keys_to_try = ["еж", "кум", "шара", "роман", "параллельно", "незнаюнестикався", "криптографическийкод"]
```

2.

Ключ	Індекс співпадіння (відповідності)
відкритий текст	0.056141499883919345
еж	0.046257884501528575
кум	0.038464449850087706
шара	0.037886049564064335
роман	0.03728531254759744
параллельно	0.03506604357904595
незнаюнестикався	0.033711133002961226
криптографическийкод	0.03335910783856531



Як бачимо, величина індексу відповідності стрімко падає із ростом довжини ключа r. Тобто, чим менше ключ, тим регулярніший розподіл.

3.

```
Ймовірна довжина ключа: [14]
Можливий ключ: итнввентюхночь
Фактичний ключ: сонвлентюночь
```

- бачимо, що довжина ключа знайдена правильно, але при розшифруванні деякі фрагменти встановлені неправильно, тому помилки виправлялись при аналізі початкового та розшифрованого текстів.

- бачимо, що потенційна довжина = 14 (чим вище індекс співпадіння, тим ймовірніша довжина ключа)