Міністерство освіти і науки України
Національний технічний університет України
“Київський політехнічний інститут ім. Ігоря Сікорського”
Фізико-технічний інститут

Лабораторна робота № 2

з предмету «Криптографія»

«Криптоаналіз шифру Віженера»
Варіант 3

Виконали:
Студенти 3 курсу,
ФТІ, груп ФБ-02, ФБ-05
Кодак Єгор,
Нікітський Іван

Київ - 2022

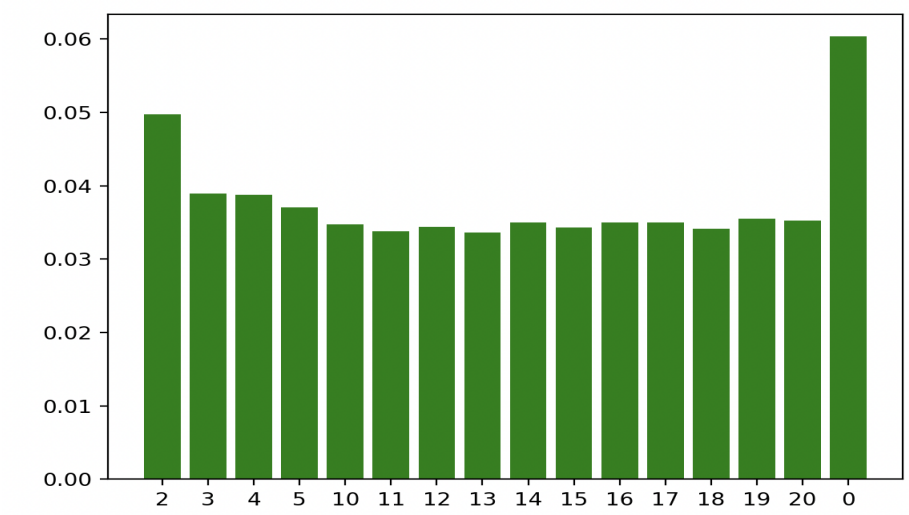
Мета: Засвоєння методів частотного криптоаналізу. Здобуття навичок роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера.

Постановка задачі:

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) .

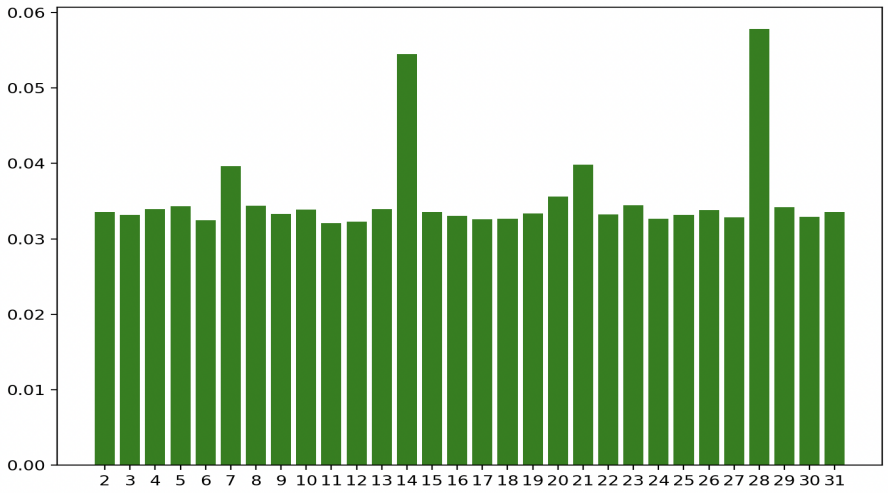
Варіант: 3

Індекси відповідності для відкритого тексту та всіх одержаних шифртекстів
Індекс відповідності відкритого тексту - 0.06
Індекс відповідності кирилиці - 0.0529є



Key Length	Key	Index
–	–	0.0603470723267208
2	яг	0.049789289752286976
3	яго	0.03897283036968514
4	ягос	0.03876040703052729
5	ягосп	0.037066159591599
10	ягосподьбо	0.034786034878541816
11	ягосподьбог	0.03376845856031795
12	ягосподьбогт	0.034417720217905234
13	ягосподьбогтв	0.03365368143351492
14	ягосподьбогтво	0.03503100695515127
15	ягосподьбогтвой	0.03433720491999863
16	ягосподьбогтвойк	0.03504642477815466
17	ягосподьбогтвойко	0.03500702367492377
18	ягосподьбогтвойкот	0.03416932195840614
19	ягосподьбогтвойкото	0.03551238565114606
20	ягосподьбогтвойкотор	0.035289683763319285

Використовуючи наведені теоретичні відомості, розшифрувати наданий шифротекст



Довжина ключа 14 символів

```
Input key length based on plot: 14
['эбомацтникфуьо', 'фкегчяйдяблккн']
```

Ключ: экомаятникфуко

```
yehor@pwd ~/trash/kpi/crypto/lab2 $ head -c 100 decrypted_ciphertext.txt
итутяувиделмаятникшарвисящийнадолгойнитиопущеннойс%
```

Висновки

Під час виконання лабораторної роботи ми засвоїли методи частотного криптоаналізу та здобули навичок роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера