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 12

Виконав студент 3 курсу

Кравець Андрій ФБ-02

Київ – 2022

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

Постановка задачі:

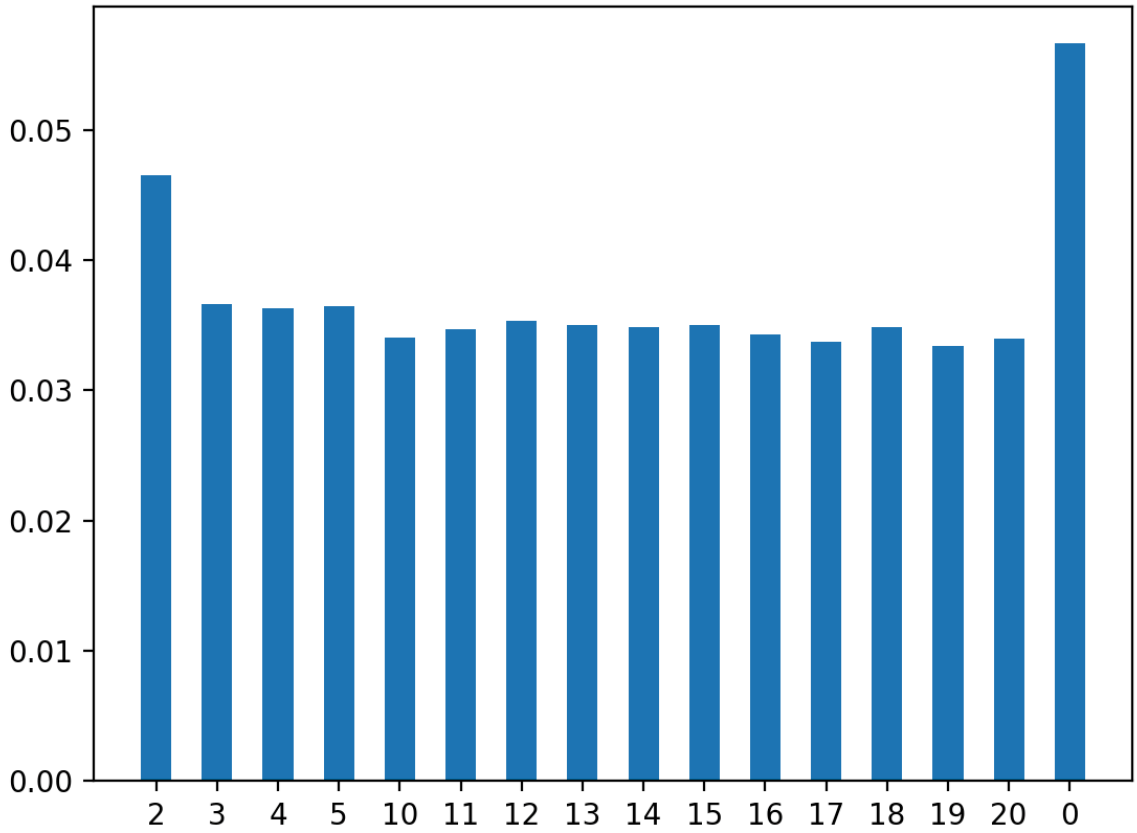
1. Самостійно підібрати текст для шифрування (2-3 кб) та ключі довжини г = 2, 3, 4, 5, а також довжини 10-20 знаків . Зашифрувати обраний відкритий текст шифром Віженера з цими ключами .
2. Підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення .
3. Використовуючи наведені теоретичні відомості , розшифрувати наданий шифртекст (згідно свого номеру варіанта) .

Індекс відповідності відкритого тексту - 0.05660385161494879

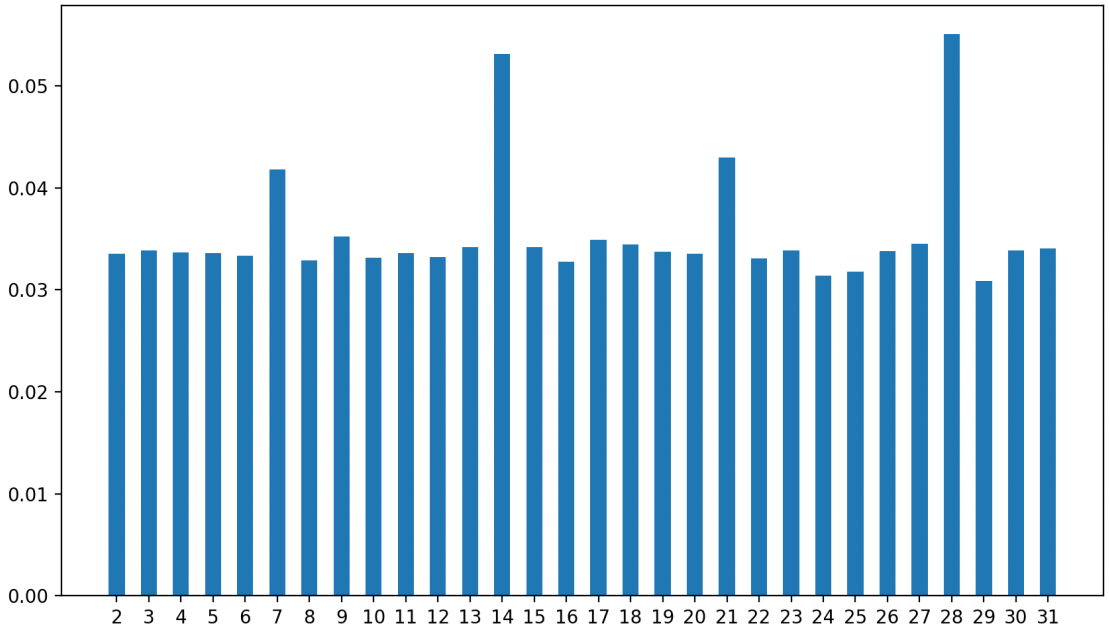
Індекс відповідності російської мови – 0.052

Індекси шифротекстів:

–	DEFAULT TEXT	0.05660385161494879
2	ко	0.046532305868405455
3	ког	0.0366165340979584
4	когд	0.03626914434595608
5	когда	0.036441460691195325
10	когдачелов	0.034012489488702 94
11	когдачелове	0.03470313340042183
12	когдачеловек	0.035335879020140334
13	когдачеловекс	0.03499951751423333
14	когдачеловексо	0.03482995823051791
15	когдачеловексоз	0.03497608249128079
16	когдачеловексозн	0.03430887360251444
17	когдачеловексозна	0.03373126921327249
18	когдачеловексознат	0.03484512206889897
19	когдачеловексознате	0.033404557422698884
20	когдачеловексознател	0.03397526915813126



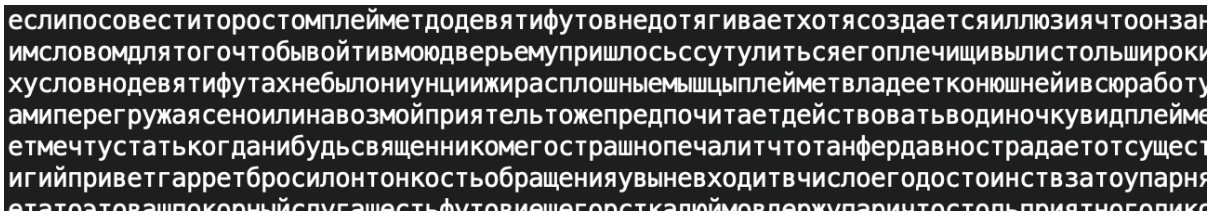
Використовуючи теоретичні відомості, знайдемо довжину ключа (14) (наведено відповідний графік):



Знайдемо ключ базучючись на довжині ключа:

Бачимо що на перетині 3 цих слів буде змістовне слово (наш ключ) “чугунныенебеса”

Відповідними кольорами позначено звідки бралися певні літери. Перевіримо декодований текст:



Висновок:

Під час виконання лабораторної роботи я засвоїв методи частотного криптоаналізу та здобув навички роботи та аналізу потокових шифрів на прикладі шифру Віженера