Міністерство освіти і науки України
НТУУ«Київський політехнічний інститут»
Фізико-технічний інститут

«КРИПТОГРАФІЯ»

КОМП'ЮТЕРНИЙ ПРАКТИКУМ №2

Криптоаналіз шифру Віженера

Виконали:
Студенти III курса ФТІ
групи ФБ-81
Легкий Дмитро
Чалий Олексій

Перевірив:
Чорний О.М

Київ – 2020

Хід роботи

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 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 10

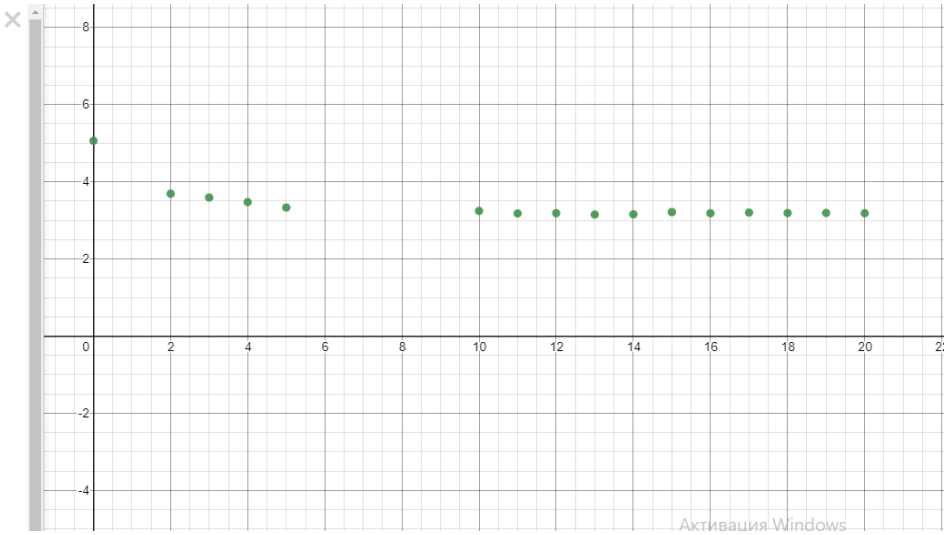
Хід роботи

Значення індексів відповідності I для вказаного r:

r	I
ВХ	0.0506074
2	0.036896
3	0.0359073
4	0.034734
5	0.0333029
10	0.0324384
11	0.031788
12	0.0318609
13	0.0315061
14	0.0315762
15	0.0321221
16	0.0318383
17	0.0320275
18	0.0318958
19	0.0319221
20	0.0318449

Для більш точного аналізу графіку, значення I було домножене на 100

x_1	y_1
0	5.06074
2	3.6896
3	3.59073
4	3.4734
5	3.33029
10	3.24384
11	3.1788
12	3.18609
13	3.15061
14	3.15762
15	3.21221
16	3.18383
17	3.20275
18	3.18958
19	3.19221
20	3.18449



Висновок

В результаті виконанні лабораторної роботи, було засвоєно методи частотного криптоаналізу. Здобуття навичок роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера. Було зашифровано довільний текст певною довжиною ключа. Виконано аналіз індексу збігу та побудована діаграма