Мета:

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

Постановка задачі:

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. Підібрали відкритий текст. Привели його до гарного вигляду.

2. Підібрали ключі і порахували індекс відповідності шифрованого тексту

3. Порівняли індекс відповідності шифротексту з індексами відповідності текстів, зашифрованими ключами довжини 2 – 5.

4. Розбили шифрований текст за варіантом на блоки та підрахували індекс відповідності кожного блоку, звідси знайшли довжину ключа (r=17).

5. Підібрали ключ, користуючись ідеями частотного аналізу шифру Цезаря для кожного блоку тексту

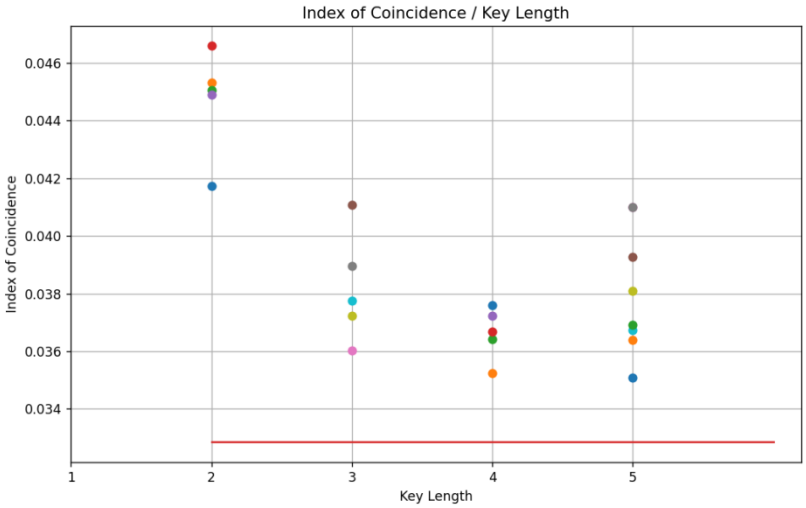
Отримані дані:

Індекси відповідності відкритого тексту та всіх шифртекстів

r (довжина ключа)	Ключ	I_r (індекс відповідн.)
Відкритий текст		0.05732086368126712
2	ха	0.04172749600100189
2	хм	0.04532664991065512
2	да	0.045053487920478724
2	по	0.04659903312222598
2	ле	0.04491201314380756
3	чур	0.041082406610520164

r (довжина ключа)	Ключ	I_r (індекс відповідн.)
3	хэй	0.036033803573839715
3	три	0.03896339918509639
3	мда	0.03723544939707499
3	бот	0.03775241068793
4	влад	0.03760337279426698
4	макс	0.035243235403573485
4	клад	0.036403728972588374
4	пиво	0.03666599117651181
4	чего	0.03721609671536053
5	зорко	0.039259695415483166
5	абвгд	0.04100165921440124
5	бвгде	0.04100165921440124
5	смысл	0.03809008161715457
5	жалко	0.03672694100168146
5	ботик	0.035071285714317495
5	бравл	0.03640039230332726
5	летал	0.03692447182193931
6	крипта	0.03501433989226117
6	ненадо	0.03746278779606545
6	почему	0.03556177609570101
7	джекпот	0.036155925668796426
7	человек	0.03738604440305986
8	стэнфорд	0.03465086538741733
8	младенец	0.03425713841460607
9	викакозак	0.03632053468567797
13	скажипаляниця	0.03362962214889953
25	оченьдолгийключшифрования	0.032581240667058024

Зазначимо, що індекс відповідності відкритого тексту є індексом відповідності для російської мови.



Червона лінія – індекс відповідності нашого тексту. Як бачимо, він значно нижче за точки, з чого робимо висновок, зо r > 5.

Таблиця середніх індексів відповідності блоків тексту для кожної довжини ключа (r > 5)

r	IoC
6	0.032805493488069416
7	0.03272796104838353
8	0.0328344000989561
9	0.03269883173876472
10	0.032853273448569364
11	0.032766732138814
12	0.032616530753538216
13	0.03287678682130736
14	0.032780420524945945
15	0.03262709665317097
16	0.033041011763076035
17	0.05539037433155081
18	0.03262856070999887
19	0.032884269556037224
20	0.03255886368565288
21	0.03281434392668897
22	0.03286955316619862
23	0.03278321294156556
24	0.03263777421080791
25	0.03271734599351553

r	IoC
26	0.03302848405378822
27	0.03247041451380763
28	0.032564765847635645
29	0.03294449398258896
30	0.032496753050019894

Мова	Індекс збігів
російська	**0.0553**

Значення для r=17 співпадає з отриманим значенням I, для російської мови. Отже, довжина нашого ключа – 17.

Після встановлення значення періоду шифру подальше його розшифрування зводиться до серії розшифрувань шифрів Цезаря.

Знаходимо наш ключ за наступною формулою:

$$k = (y^* - x^*) \bmod m$$

де y* – буква, що частіше за всіх зустрічається у фрагменті Yi , а x* – найімовірніша буква у мові, якою написано відкритий текст (`"о", "е", "а", "и", "н", "т"`).

Проходимось по усіх блоках, використовуючи формулу вище і обираємо найбільш часте число з кожного блоку, переводимо це число у букву та додаємо до нашого ключа:

	о	е	а	и	н	т
п	1	10	15	7	2	29
в	20	29	2	26	21	16
з	25	2	7	31	26	21
к	28	5	10	2	29	24
р	2	11	16	8	3	30
у	5	14	19	11	6	1

Отриманий ключ: `войнамагаэндшпиль`

Розшифрований текст знаходиться у файлі decrypted_task.txt

Висновки: під час виконання лабораторної роботи ми навчились шифрувати та розшифровувати текст шифром Віженера, підібрали довжину ключа через індекс відповідності та знайшли сам ключ за допомогою частотного аналізу.