Міністерство освіти і науки України
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

Фізико-технічний інститут

СИМЕТРИЧНА КРИПТОГРАФІЯ

КОМП’ЮТЕРНИЙ ПРАКТИКУМ №2

Криптоаналіз шифру Віженера

Виконали:
студентки групи ФІ-94
Зацаренко А. Ю.
Футурська О.В.

Перевірив:
Чорний О.М.

Київ – 2022

ЗМІСТ

ЗАГАЛЬНІ ВІДОМОСТІ

1. Мета комп’ютерного практикуму

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

2. Постановка задачі

Варіант 2.

Створити програму для знаходження ключа шифру Віженера двома способами та дешифрувати текст за варінтом.

3. Хід 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 I_r для відкритого тексту та всіх одержаних шифротекстів і порівняти їх значення.

3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта). Зокрема, необхідно:

– визначити довжину ключа, використовуючи або метод індексів відповідності, абостатистику співпадінь D_r (на вибір);

– визначити символи ключа, прирівнюючи найчастіші літери у блоці до найчастішої літери у мові;

– визначити символи ключа за допомогою функції $M_i(g)$;

– розшифрувати текст, використовуючи знайдений ключ; в разі необхідності скорегувати ключ.

4. Опис труднощів

Реалізовуючи програмний код, ми зіштовхнулися з проблемою, що для кожної формули потрібно знаходити порядковий номер літер текстів, шляхом пошуку букви у алфавіті. В результаті ми вирішили один раз проробити цю операцію і зберігати текст у вигляді масиву індексів.

Ще одна проблема, з якою ми зіштовхнулися, це розбивання текстів на блоки. Але ми вирішили не зберігати текст частинами, а при необхідності проглядати його через r символів, де r – довжина ключа, за допомогою функції for.

ПРАКТИЧНА ЧАСТИНА

1. Значення індексів відповідності

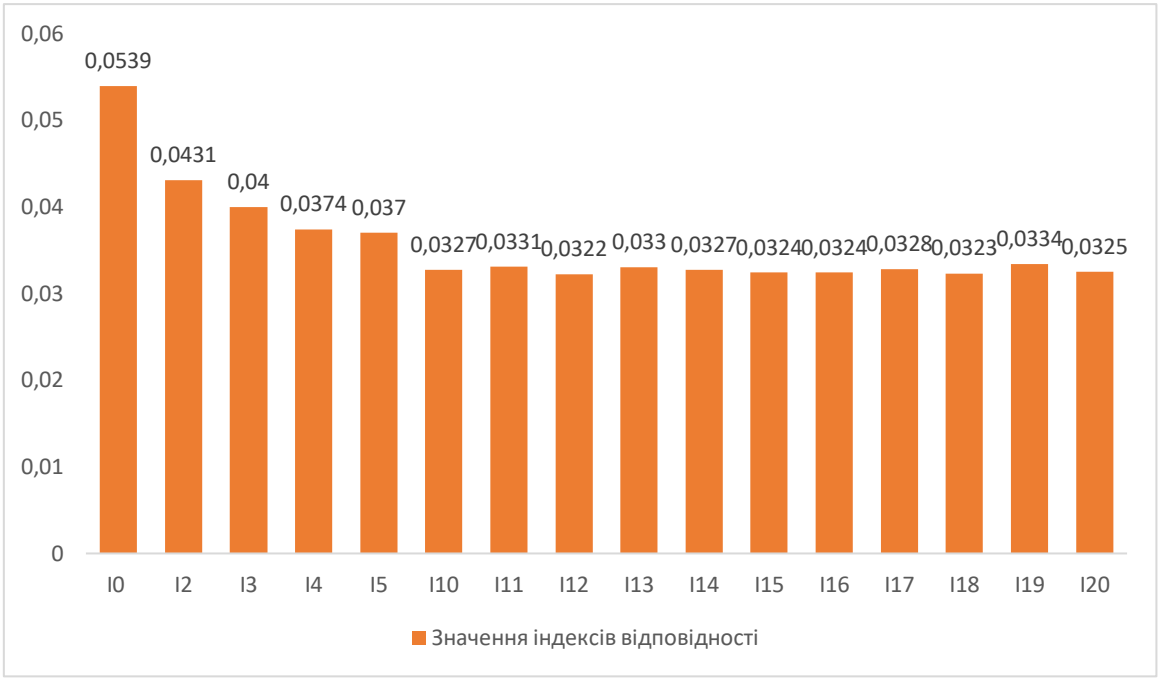

Рис.2.1 – Значення індексів відповідності

2. Встановлення довжини ключа

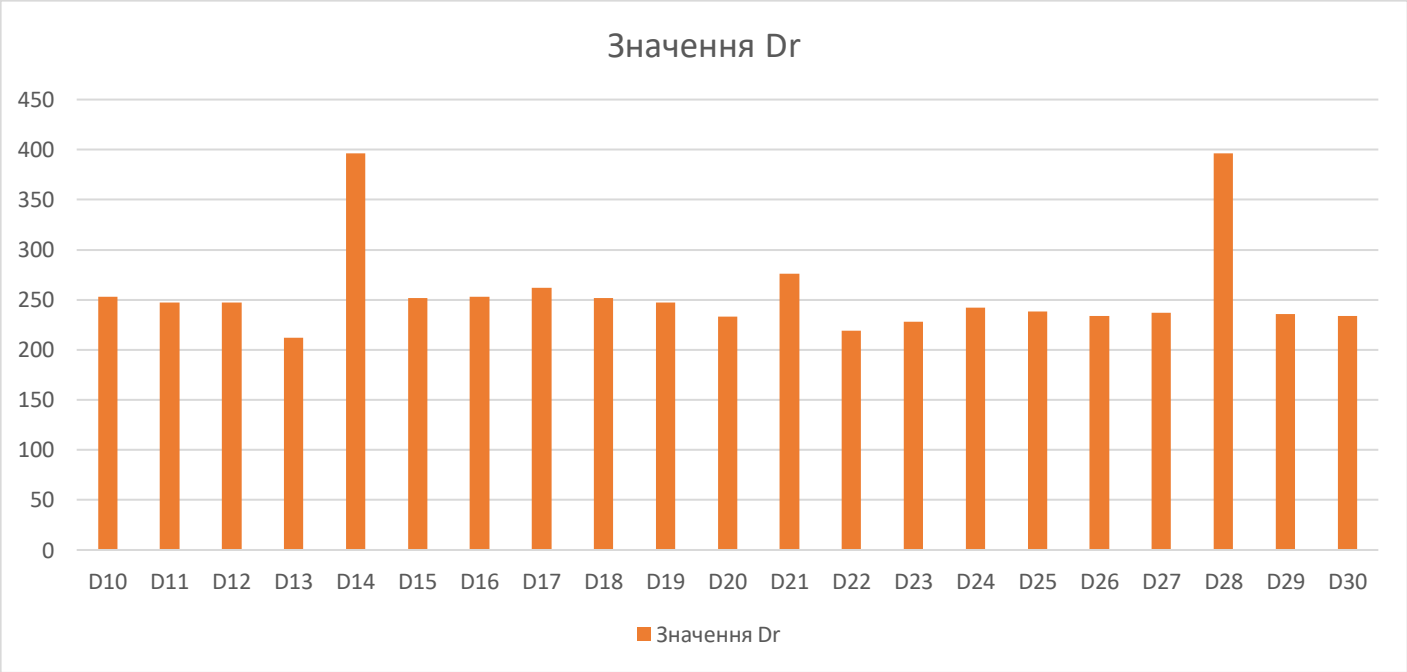

Рис.2.2 – Значення послідовності D_r

Отже, довжина ключ r = 14.

3. Знаходження ключа шифру Віженера

I. Значення ключа, одержане із використанням функції $M_i(g)$:
Ключ : последнийдозор

II. Значення ключа, одержане шляхом співставлення найчастіших літер блоків найчастішій літері мови:
Ключ : жосвеыдиадозор
Скорегований ключ : последнийдозор
Більшість літер були співставлені з найчастішою буквою російського алфавіту «о», а інші з другою по частоті – буквою «е».

4. Шифрування ключа за допомогою функціїї M(g)

	0	1	2	3	4	5	6	7	8	9	10	11	12	13
а	11,758	17,1662	11,816	13,6286	17,9698	17,6855	13,9358	15,2305	17,6479	17,2314	16,658	12,1304	16,1602	12,981
б	16,1851	15,1771	12,3679	13,9156	17,377	22,7447	12,4173	12,1455	16,1873	19,8385	15,459	16,5678	16,2593	13,4198
в	16,2328	12,5707	12,384	16,9634	21,4451	18,2949	12,3189	16,5602	13,1711	17,9817	12,3381	19,3324	13,5663	17,3194
г	13,0092	13,5073	16,3382	15,9225	18,3627	18,4597	13,1852	19,2605	17,3822	19,2739	12,8127	16,9394	13,9615	15,0856
д	13,1148	13,7193	14,9942	11,6905	19,5857	29,9186	17,1447	17,4583	19,199	28,7774	13,5696	20,1094	15,0653	12,3982
е	13,3733	17,2693	12,1693	16,2	29,5592	18,9353	14,5861	19,7542	17,9389	18,353	16,2775	17,7421	18,2287	12,7638
ж	17,6821	15,3744	12,8603	19,1868	19,1783	17,7381	12,5359	17,202	22,4351	18,0666	15,4558	18,7042	16,7751	13,1128
з	16,5563	12,7124	14,6654	16,7278	18,2443	20,2128	17,5384	19,2492	18,4361	20,5951	12,3695	28,9005	13,7732	15,8652
и	13,2758	16,5256	17,0725	20,7131	21,6862	16,5301	17,9764	28,4755	18,9059	17,5186	17,1392	19,132	17,4099	15,0195
й	17,4957	19,1737	15,526	18,339	17,7688	19,3916	16,9162	17,9692	28,8201	19,2471	18,3434	17,1205	19,6454	11,7266
к	19,7774	17,2067	13,1966	18,8489	18,6978	16,4843	21,7823	17,4256	19,6384	16,5742	17,9491	21,7096	17,8279	15,973
л	18,2346	20,5186	16,8224	29,1081	17,2237	12,4852	18,1014	20,2356	17,9109	12,52	21,4758	17,8354	21,5824	18,2924
м	23,1276	18,6055	19,5225	19,2973	12,2113	14,5393	18,8374	18,2713	19,9424	15,699	17,8927	18,7194	17,9499	17,7124
н	18,1182	18,5962	18,2843	17,9257	13,8714	15,9715	29,0772	19,0548	17,2043	17,1638	19,824	17,0469	17,4457	20,415
о	18,4287	29,3687	20,9693	20,7172	16,9966	14,0247	18,963	16,5777	19,7974	14,4227	28,7603	12,0416	28,137	18,4527
п	30,1207	19,5188	17,9496	17,8558	13,4502	12,4637	18,8923	12,3281	16,808	14,0025	18,5876	15,1153	19,0607	19,1224
р	18,7947	18,3013	19,4616	19,2044	12,528	12,2161	22,2497	14,7061	12,5575	13,2679	17,7218	16,2131	17,7289	28,7876
с	17,7146	21,3338	29,2522	15,5433	13,5995	14,6536	18,071	17,0574	14,3535	15,967	20,708	13,7635	20,652	19,2263
т	21,1079	18,7662	19,0292	12,078	14,9459	16,4528	19,0732	13,9887	15,9815	18,2033	17,7089	12,735	17,415	18,3394
у	15,9791	19,1605	17,7065	13,942	17,2125	12,2915	17,0995	13,1382	14,3419	13,2695	19,5192	12,6137	18,5345	21,0922
ф	19,8081	16,7127	21,3284	16,1814	13,0537	12,9376	12,5638	12,8992	13,1216	13,6369	16,9798	15,8373	17,2216	18,0648
х	17,668	13,1217	18,0318	14,1816	13,2386	12,0676	15,7171	15,8653	12,0187	13,0453	13,1357	16,6652	11,9739	19,3564
ц	10,9665	13,9442	19,0103	12,2856	13,7297	16,5756	16,4073	17,2825	15,1142	17,4075	15,4374	13,0639	14,2615	17,5333
ч	14,9453	16,7676	17,3427	12,8156	16,6028	15,5577	15,4661	12,9782	16,19	14,7651	16,1538	13,3803	16,6844	12,5507

ш	16,4022	14,0797	11,9402	15,1162	15,3153	14,4276	13,6553	13,0703	12,8286	11,8537	14,8173	13,4128	13,3392	14,7231
щ	13,4567	12,3625	15,1878	16,9646	12,8653	13,6241	13,2295	13,2517	12,6548	12,927	12,9527	17,5898	12,5933	17,4386
ъ	13,1177	13,0449	17,2512	13,7706	12,5493	13,9146	15,9011	18,0554	11,7688	13,3105	12,8475	16,2418	11,6738	14,3148
ы	11,5994	14,6457	14,448	13,4932	13,4297	18,0895	15,6914	15,9582	16,1543	16,2312	15,7138	12,6556	13,9183	13,3019
ь	14,1318	16,6301	12,7303	13,7838	17,1428	15,8771	12,6322	13,0183	15,6363	14,953	15,9196	13,5421	16,3809	13,5771
э	16,6814	12,6255	12,5704	18,0913	14,7136	12,5467	13,8235	12,9791	12,994	11,7925	12,6049	14,4286	12,3611	14,6155
ю	12,3906	13,1925	15,5317	16,1417	12,4447	17,7191	12,0484	14,4234	12,4438	15,8679	13,1953	16,5007	13,096	17,0997
я	12,7981	12,353	16,2916	13,4188	17,0529	19,2212	15,2147	17,1821	13,4678	19,2885	12,7243	15,262	12,3694	13,3711

5. Розшифрування шифртексту

какясмогэтосделатьспросилгесерипочемуэтогонесмогсделатьтымыстоялипосредибеск
райнейсеройравнинывзгляднефиксировалияркихкрасоквцелойкартиненостоиловсмотре
тьсявотдельнуюпесчинкуитавспыхивалазолотомбагрянцемлазурьюзеленьюнадголовой
застылобелоесрозовымбудтомолочнуюрекуперемешалискисельнымиберегамидаивыпл
еснуливнебесаащедулветерибылохолодномневсегдахолодноначетвертомслоесумрака
ноэтоиндивидуальнаяреакциягесерунапротивбыложарколицораскраснелосьполбустека
ликапелькипотамненехватаетсилысказалялицогесерасовсемпобагровелоответнеправил
ьныйтывысшиймагтакполучилосьслучайнонотывысшийпочемувысшихмаговтакженаз
ываютмагамивнекатегорийпотомучторазницавсилемеждуниминастольконезначительн
ачтонеможетбытьисчисленаиневозможноопределитьктосильнееактослабеепробормота

ВИСНОВКИ

У даній роботі було обраховано індекси відповідностей для текстів, зашифрованих ключами різних довжин. Також за допомогою послідовності D_r, знайдено довжину ключа. Значення ключа було знайдено двома способами: із використанням функції $M_i(g)$ та шляхом співставлення найчастіших літер блоків найчастішій літері мови. Перший спосіб виявився ефективнішим, бо значення, отримане другим способом, потребувало коригування.