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
Варіант 3

Виконали:
студенти групи ФІ-94
Коробан Ольга

Перевірив:
Чорний О.М.

Київ 2022

ЗАГАЛЬНІ ВІДОМОСТІ

Мета роботи

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

Постановка задачі

Написати програму для шифрування та розшифрування тексту шифром Віженера, а також обчислення індексу відповідності тексту.

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 індекс и відповідності I_r для відкритого тексту та всіх одержаних шифро текстів 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, або статистику 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(g)i;
- розшифрувати текст, використовуючи знайдений ключ; в разі необхідності скорегувати ключ.

Труднощі, що виникали:

Найголовніша проблема - не наплутати в індексах і логіці програми. Ніяких додаткових труднощів порівняно з практикумом №1 не виникло.

Результат:

Результати шифрування обраного текста:

```
Matching index for open text = 0.06271185473702913
for key: [1084; 1078]
Mathcing index = 0.04937157741770113

for key: [1098; 1086; 1101]
Mathcing index = 0.04206653675218692

for key: [1072; 1097; 1074; 1088]
Mathcing index = 0.03812509118056727

for key: [1094; 1076; 1098; 1096; 1081]
Mathcing index = 0.03792052070114697
```

```
for key: [1098; 1077; 1091; 1078; 1089; 1075; 1095; 1101; 1080]
Mathcing index = 0.03244357400112963

for key: [1077; 1098; 1091; 1086; 1099; 1084; 1082; 1095; 1078; 1081]
Mathcing index = 0.03352755303550807

for key: [1078; 1093; 1086; 1092; 1072; 1082; 1102; 1099; 1100; 1094; 1073]
Mathcing index = 0.03146391776103723

for key: [1097; 1075; 1072; 1082; 1094; 1096; 1076; 1090; 1073; 1091; 1098; 1099]
Mathcing index = 0.032746762122023446

for key: [1096; 1100; 1083; 1078; 1079; 1095; 1091; 1074; 1084; 1098; 1089; 1077; 1092]
Mathcing index = 0.03206458885001236

for key: [1073; 1072; 1084; 1077; 1096; 1074; 1094; 1092; 1093; 1080; 1099; 1083; 1088; 1089]
Mathcing index = 0.03183149260652947

for key: [1097; 1093; 1072; 1081; 1075; 1088; 1095; 1077; 1083; 1087; 1084; 1079; 1085; 1091; 1078]
Mathcing index = 0.03086813680304428

for key: [1086; 1099; 1073; 1094; 1082; 1097; 1081; 1089; 1100; 1080; 1072; 1074; 1078; 1102; 1075; 1095]
Mathcing index = 0.03142642675684068

for key: [1084; 1098; 1101; 1090; 1077; 1088; 1072; 1089; 1080; 1092; 1082; 1081; 1079; 1074; 1102; 1097; 1100]
Mathcing index = 0.031012395667017946

for key: [1088; 1098; 1102; 1078; 1092; 1091; 1082; 1087; 1086; 1073; 1094; 1079; 1097; 1080; 1076; 1077; 1089; 1075]
Mathcing index = 0.03138812073081378

for key: [1090; 1093; 1099; 1080; 1076; 1095; 1092; 1091; 1088; 1083; 1073; 1102; 1098; 1086; 1100; 1087; 1077; 1082; 1075]
Mathcing index = 0.03092600335299981

for key: [1078; 1095; 1082; 1099; 1101; 1098; 1083; 1090; 1091; 1100; 1097; 1088; 1085; 1074; 1087; 1072; 1081; 1089; 1075; 1084]
Mathcing index = 0.03087954710866931
```

Ключи були обрані за допомогою вбудованої ф-ї Math.random().

Можна побачити, що для зашифрованого тексту індекс відповідності менше за індекс для звичайного тексту. Також зі збільшенням довжини ключа індекс зменшується. При збільшенні кі-сті однакових значень у масиві ключа зростає індекс відповідності, тому програма складена таким чином, щоб значення не повторювались. Обраний текст містив букви від ‘а’ до ‘я’, за виключенням ‘ё’, а також пробіл.

Обчислимо D_r:

```
r = 6 Dr = 319
r = 7 Dr = 242
r = 8 Dr = 282
r = 9 Dr = 266
r = 10 Dr = 282
r = 11 Dr = 321
r = 12 Dr = 259
r = 13 Dr = 266
r = 14 Dr = 525
r = 15 Dr = 269
r = 16 Dr = 260
r = 17 Dr = 277
r = 18 Dr = 271
r = 19 Dr = 285
r = 20 Dr = 241
r = 21 Dr = 265
r = 22 Dr = 276
r = 23 Dr = 281
r = 24 Dr = 265
r = 25 Dr = 285
r = 26 Dr = 271
r = 27 Dr = 293
r = 28 Dr = 527
r = 29 Dr = 252
```

значення для r = 14,28 суттєво відрізняються. Отже, перевіримо r = 14.

```
э б о м ч ц т н и к ф ъ ь о
иыутиьвиделмоятцикбйрвисящщйнйдофмойнитиьпувенцчйсвольаыхчралсзохроныомлелсаииописйвафкофобанияяхнафнослсякийозутслбдшодчараъиморнчтп
э к о м а я т н и к ф у к о
итутяувиделмаятникшарвисящийнадолгойнитиопущеннойсвольтыхоравизохронномвеличииописывалколебанияязналноивсякийощутилбыподчарамимерной
```

Значення ключів:

```
э б о м ч ц т н и к ф у ь о
иыутиьвиделмоятцикбйрвисящцйнйдофмойнитиьпувенцчй
э к о м а я т н и к ф у к о
итутяувиделмаятникшарвисящийнадолгойнитиопущенной
```

Літера	0	1	2	3	4	5	6	7	8	9	10	11	12	13
а	24.8535	14.2975	18.9816	14.9553	34.5782	22.8043	19.3629	17.0697	19.7280	15.0060	14.3336	15.9164	16.7323	18.3232
б	21.5864	19.5839	17.5547	14.8310	22.7689	20.9941	15.9714	13.9690	13.1930	20.7442	17.2224	19.8808	20.0900	17.8414
в	21.8498	18.5710	14.8815	15.1645	20.8777	25.3393	14.6188	14.5044	19.3261	18.7414	19.7076	14.3698	19.4502	15.5846
г	20.5793	13.0810	14.1737	19.4694	25.0059	20.3031	14.4622	14.9591	22.3338	13.9018	15.2338	15.3754	14.8047	14.4359
д	14.6001	19.5731	15.2114	17.4905	21.8750	24.6502	18.9755	19.4757	20.9550	19.8684	16.1584	15.6004	19.8760	15.4777
е	18.0866	21.6572	19.4852	13.9308	23.8000	20.6913	16.8257	18.0737	26.0292	20.7706	13.8465	19.2377	22.5070	19.4621
ж	20.5186	19.4703	18.2476	19.8953	20.3534	14.6986	14.5818	13.8420	21.3371	19.5596	18.6859	16.9023	20.7724	18.7107
з	16.3562	24.8140	14.3573	21.0495	15.1540	19.1281	14.4987	19.7133	22.0595	25.8486	16.5011	15.5315	25.0878	14.6298
и	15.2848	20.1712	19.4848	20.1055	19.0348	19.4678	14.5999	21.8704	35.2759	20.0238	15.1502	15.5282	20.4307	19.6884
й	16.4965	21.9313	21.6225	25.8318	19.1713	17.1827	19.5729	21.0198	22.4811	21.5781	14.4183	14.5492	22.1467	22.3933
к	17.5301	34.8764	21.1125	21.7854	17.2129	16.8268	18.1888	25.0484	20.7953	34.6962	14.0114	19.4362	33.1175	21.5192
л	19.3471	21.8303	26.1726	22.0346	14.4467	14.8613	13.3444	21.6998	22.9021	22.4877	19.0781	18.7190	20.5376	26.0532
м	15.5373	21.5026	20.7468	33.9232	14.4535	18.5382	18.8250	22.9172	19.9405	23.0329	18.8174	14.3989	20.3330	20.8985
н	15.5743	24.5077	21.5938	22.5931	18.3138	19.3669	20.8912	34.1053	23.2169	23.8124	13.8168	20.3788	22.2020	22.1474
о	15.7270	21.1522	34.0231	21.5600	18.7022	15.8790	20.3076	22.3674	19.8306	21.9956	19.7467	21.8772	19.9343	33.5825
п	18.4237	25.1587	22.0290	25.0576	15.3158	15.3951	25.2393	22.2820	14.1021	23.8364	20.9817	19.9453	22.2973	22.6317
р	16.6252	19.8710	20.8973	20.8981	15.4743	15.3128	20.9512	24.5283	17.2845	19.7520	20.5345	26.2593	18.1350	21.0278
с	14.3694	14.8554	23.2461	21.6681	14.8144	18.1200	21.4390	21.1237	19.9014	14.1859	26.1895	21.6413	14.2410	23.6095
т	14.5186	19.9613	20.7458	21.3817	19.5810	17.0258	34.8736	23.0276	16.2789	17.3458	21.3658	21.6416	17.9397	19.1407
у	15.8864	19.3056	23.2041	14.3517	16.8143	14.5913	23.6715	20.5437	14.1379	17.9289	21.7120	33.9032	18.0932	22.8120
ф	18.9003	17.7848	20.6798	17.9339	14.5358	14.2448	21.4733	14.2338	14.9339	17.9650	34.1806	21.6744	17.1174	19.7376
х	17.8444	15.0492	14.4109	20.8921	14.7197	13.9353	24.3356	18.9665	17.3366	13.8218	22.7924	21.3579	14.9976	13.9051
ц	13.7621	14.9809	17.7498	16.3078	15.0665	19.8747	21.1008	19.7456	19.9087	13.3493	23.0203	25.3022	13.8236	18.5637
ч	19.5325	19.0090	19.5634	15.5163	20.6982	17.8216	23.7360	16.9035	15.6222	17.7688	23.4854	19.7017	19.0551	19.3960
ш	21.1320	18.4780	17.7640	15.6404	18.3996	13.0060	20.8972	15.0808	14.8223	18.5926	20.4254	22.7489	18.6375	16.4955
щ	20.2236	14.9479	15.7873	17.0316	12.9333	19.2456	14.7409	15.1124	14.7380	14.8156	22.9576	21.2996	15.5914	16.2281
ъ	24.5516	15.2839	14.7378	19.7055	20.0222	20.7016	18.2587	17.1150	18.9988	16.1097	20.2953	14.0259	16.4827	14.0494
ы	21.7376	15.0011	18.2417	14.7447	21.4200	18.9618	19.7953	18.8746	18.1086	14.5902	15.4661	17.9279	15.1973	17.6748
ь	22.1769	19.3106	19.9410	15.0960	18.8982	26.0716	17.6258	14.5015	15.0744	20.8899	18.0359	19.1847	21.2439	19.2334
э	33.7798	16.5062	14.6118	15.9334	24.7496	20.3290	14.7895	15.1728	15.1975	17.4042	18.6091	15.2219	18.4382	15.5854
ю	22.3229	14.1201	15.4783	17.8460	20.3397	21.8395	15.1901	14.8472	15.0571	15.0327	18.2022	16.7285	15.6630	15.5261
я	21.2853	14.3563	14.2630	16.3753	21.4692	33.7920	17.8555	18.3059	20.0930	15.5436	16.0183	14.7339	16.0243	14.6355

Фрагмент шифрованого тексту:

еьбюятфхмпяякнпчццшявпрыумтчкктълвацхтжышэргущнныюкшяпьйтшюмвзщыэъвачьймучицъхцщьдерэхшълдунхтутс
ыэхыъибгмттэ
бгбптщныоасякдуццйпющоибаужеуацебаъпдвхцоюбхуюкыфйнбэнощюпыльыъшдяхнцюхктнкащовачцъб
тощечйщисъчятеюэюзшаърнчхшъфйтьккщиннчсуйгбощрчызхтюыкщдшощеаьшбнштщьцшчылуюмцзаънэюбыыеьучьма
юцщдтновььцртшъцыжыытекъстптщрхтфегоэзсссфажгьифюрньокяьхкъщяйэвъушешчърймуъол

ььрннхычшясыозщюътз
фычшябрылцбырдцюъкцюйупъуууокояиьжууылуяъосятщпбашяптымиаашнпцапрнпъсн
мнвфпдшоцкыаоемяыщььешезтш
ьеоэтхтучмьжыаоемяыщььуляпъоцтмарцтыяпювчцлтпахячвдьцфтячаоъютъпешчфпаое
пъдхшеетшяктьасяылшюбъыььыо
епктхыжхкшнэсмешчмпчфюбалчоцомитцьцшыылущфн
зъпцыеекылмщснмаццьжббшефюспкчърйбуяьбйзфйрсьцоауйакт

Розшифрований фрагмент:

итутяувиделмаятникшарвисящийнадолгойнитиопущеннойсвольтыхоравизохронномвел
ичииописывалколебанияязналноивсякийощутилбыподчарамимернойпульсациичтопери
одколебанийопределенотношениемквадратногокорнядлинынитикчислуркотороеиррац
иональноедляподлунныхумовпредлицомбожественнойрационеукоснительносопрягаето
кружностисдиаметрамилюбыхсуществующихкруговкакивремяперемещенияшараотодн
огополюсакпротивоположномупредставляетрезультаттайнойсоотнесенностинаиболеев
невременныхмерединственноститочкикрепленияздвойственностиабстрактногоизмерени
ятроичностичислапискрытойчетверичностиквадратногокорнясовершенствакругаещеяз
налчтонаконцеотвеснойлинииивосстановленнойотточкикрепленияснаходящийсяподмаят
ни

Висновки:

В ході лабораторної роботи було засвоєно методи частотного криптоаналізу, здобуті навички роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера. Перший ключ знайдений за допомогою прирівнювання найчастішої літери у мові до літери у ключі. Другий - функцією $M_i(g)$. Можна побачити, що другий ключ є корректним. Шифр Віженера виявилося легко розшифрувати. Для цього не вимагається ні велика потужність комп’ютера, ні великий обсяг пам'яті.