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 9

Виконала:
студентка групи ФІ-93
Ліщинська О.Т.

Перевірив:
Чорний О.М.

Київ – 2022

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

3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифротекст (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_i(g) ;

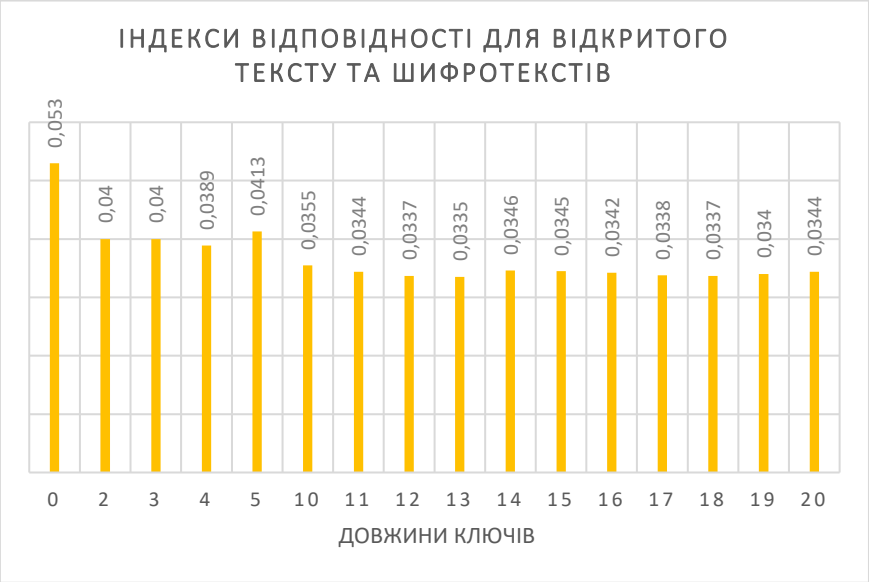
–розшифрувати текст, використовуючи знайдений ключ; в разі необхідності скорегувати ключ

Труднощі

Труднощі виникли на етапі знаходження символів ключа, що відбувалось методом прирівнення найчастішої літери у блоці до найчастішої літери у мові. Не зважаючи на кількість ітерацій (тобто скільки б я букв не розглядала від найчастішої літери у мові до найменш частої) змістовного ключа я не змогла отримати. Багато було зроблено перевірок, наприклад, виведення довжин ключів з певного проміжку, щоб виключити помилку знаходження довжини. Крім того я перевіряла даний метод знаходження ключа на шифротексті з відомим ключем (ключ, хоча і з похибкою, але можна було знайти, що виключило помилку в коді). В решті я дійшла до висновку, що даний метод дає дуже велику похибку і є незастосовний до шифротексту за моїм варіантом.

Обчислені індекси відповідності для заданих значень

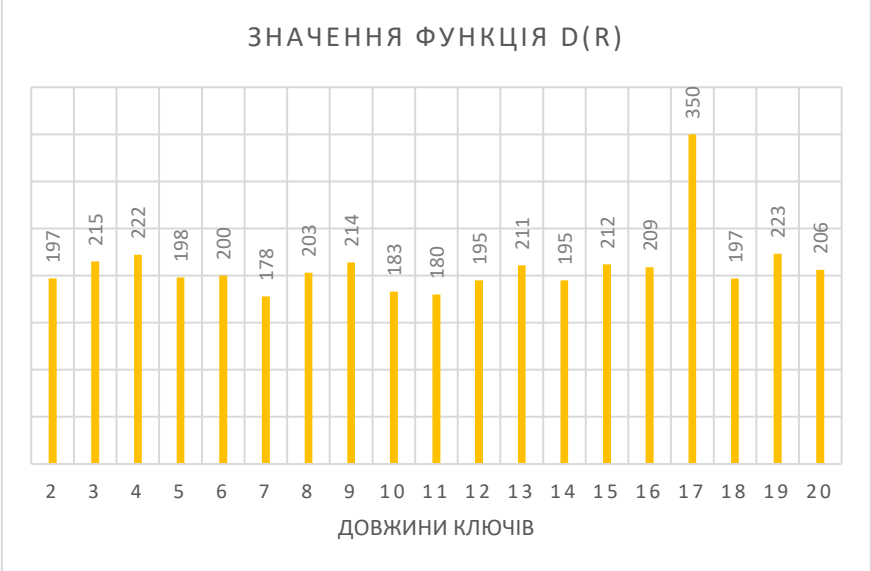
довжини ключів	2	3	4	5	10	11	12	13	14	15	16	17	18	19	20
I	0,04	0,04	0,0389	0,0413	0,0355	0,0344	0,0337	0,0335	0,0346	0,0345	0,0342	0,0338	0,0337	0,034	0,0344



<u>Розшифрування тексту за варіантом</u>

Значення функції D_r для певного проміжку довжин ключів

довжина ключа	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
D	197	215	222	198	200	178	203	214	183	180	195	211	195	212	209	350	197	223	206



Враховуючи отримані результати можна зробити висновок, що довжина ключа дорівнює **r = 17.**

Значення ключа, одержане шляхом співставлення найчастіших літер блоків найчастішій літері мови

Оскільки так склалося, що даний метод не є застосовним до шифротексту за моїм варіантом, для прикладу я надаю таблицю, в якій вивела отримані значення ключа у відповідності до всіх літер мови, а не лише найчастішим

(виділені рядки відповідають найчастішим літерам російської мови)

оынмнщнвдкъсеьхкй	а
нъмлмшмбгйщрдыфйи	б
мщлклчлавишпгъуиз	в
лшкйкцкябзчовщтзж	г
кчййихйюажцнбшсже	д
йцизифиэяехмачред	е
ихзжзузьюдфляцпдг	ж
зфжежтжыэгукюхогв	з
жуедесеъьвтйэфнвб	и
етдгдрдщыбсиьумба	й
дсгвгпгшъарзытлая	к
грвбвовчщяпжъскяю	л
впбабнбцшюоещрйюэ	м
боаяамахчэндшпиэь	н
аняюяляфцьмгчозьы	о
ямюэюкюухылвцнжыъ	п

юлэьэйэтфъкбхмеъщ	р
экьыьиьсущйафлдщш	с
ьйыъызыртшияукгшч	т
ыиъщъжъпсчзютйвчц	у
ъзщшщещорцжэсибцх	ф
щжшчшдшнпхеьрзахф	х
шечцчгчмофдыпжяфу	ц
чдцхцвцлнугъоеюут	ч
цгхфхбхкмтвщндэтс	ш
хвфуфафйлсбшмгьср	щ
фбутуяуикрачлвырп	ъ
уатстютзйпяцкбъпо	ы
тясрсэсжиоюхйащон	ь
сюрпрьрезнэфияшнм	э
рэпопыпджмьузючмл	ю
пьоноъогелытжэцлк	я

Отримані результати підтверджують неефективність даного методу в деякий випадках.

Значення ключа, одержане за допомогою функцій $M_i(g)$

Наведемо таблицю отриманих результатів при застосуванні даної функції:

	В	О	Й	Н	А	М	А	Г	А	Э	Н	Д	Ш	П	И	Л	Ь
1	12,5542	11,9462	12,7197	11,9811	20,708	8,98255	20,4297	14,9688	21,5625	14,7789	10,6407	13,2866	11,4889	8,20168	10,4741	10,326	12,4515
2	15,1745	11,7776	10,8346	9,53007	13,9789	9,34516	13,5652	13,8967	13,42	12,6691	8,88466	15,2363	11,8835	10,9959	9,31839	11,334	13,5358
3	19,3797	10,2788	9,61549	9,58436	13,5269	10,0649	13,6498	12,8862	12,4558	13,5771	8,70716	12,6882	10,115	10,0517	13,0619	11,7807	12,4337
4	13,1284	9,4885	12,8993	10,7828	15,1194	12,1562	15,3426	20,128	16,3134	11,6562	10,1845	13,1539	9,87228	7,85974	14,2288	11,3809	8,22867
5	13,4717	10,5098	13,9404	11,6781	12,3269	11,0374	12,5466	13,6705	12,79	8,56684	11,6796	21,4626	9,09344	8,26588	13,1209	9,60136	10,7089
6	14,5908	12,5904	12,4433	11,3429	14,038	9,3133	13,4876	12,7707	12,8307	10,9459	10,1572	13,5891	11,3769	8,91771	15,2391	12,6958	12,4906
7	12,7113	11,4625	15,1075	8,98354	11,7593	12,5201	12,6362	13,8096	12,0875	11,5646	9,65545	13,0987	11,9099	10,2133	13,739	14,0416	8,69374
8	13,5454	9,04905	12,8882	11,6709	9,21092	14,1016	9,15463	11,8894	8,18686	9,75668	12,4403	14,4857	8,79599	10,4859	13,5525	12,1177	8,58773
9	10,9562	12,567	13,9597	14,0822	10,2794	11,7501	11,5197	12,8203	10,5121	8,79166	13,7733	12,4227	10,6379	8,82463	20,5537	15,3759	8,9806
10	8,69301	14,1532	20,332	12,2638	12,2719	15,6766	12,3475	11,1858	12,0513	8,63119	13,3514	12,9366	9,17734	11,3944	13,6273	13,2277	9,99921
11	11,4877	12,9145	13,2498	13,7236	9,78138	13,72	10,036	9,04199	8,59416	10,9397	15,41	12,5232	11,913	14,023	12,6444	14,2081	12,6247
12	11,1921	15,1197	13,1193	13,4871	9,68135	12,8264	10,4008	10,5212	8,14955	12,1542	13,1974	8,44212	10,9076	12,7003	15,2881	20,0667	8,59015
13	9,50722	12,9237	14,9627	13,4684	9,63285	21,3317	9,71868	11,1806	8,92928	8,45161	14,6037	10,2101	9,48343	15,9111	12,7635	12,5801	8,60187
14	9,60559	12,957	12,7748	19,7307	10,3727	13,9972	10,3486	9,7577	10,0539	9,19943	20,6692	12,4892	9,97956	14,087	12,3594	13,3604	9,03175
15	8,67087	20,9672	13,8045	13,4818	12,3178	12,2884	11,3897	8,83354	10,653	9,05792	14,032	10,2253	9,93654	13,7908	12,5533	14,7239	11,9153
16	11,4504	13,5381	11,2856	12,3189	9,91215	15,4814	8,60362	8,34756	8,49546	12,7959	13,2153	8,95519	11,3803	21,9034	9,12931	12,1406	11,5528
17	10,9503	12,1587	8,84807	14,1161	9,50136	12,9307	9,16049	10,2083	8,90264	11,6327	14,8219	8,54137	10,7899	13,9911	11,0388	12,764	8,94082
18	9,38741	14,6434	11,08	13,1421	9,94412	13,6503	8,54743	12,283	9,47148	8,96588	12,6906	10,9727	8,65247	13,4709	11,9292	11,508	9,31776
19	9,60007	11,7188	10,8834	12,6175	12,2893	12,6503	10,3999	9,72112	11,9715	9,9711	13,6733	12,8277	11,6502	15,6398	9,43216	8,82743	10,5347
20	10,0632	12,6993	9,23005	10,6853	10,9971	9,11738	9,88554	9,7962	10,8799	11,0931	12,5213	8,53573	13,9625	12,3065	9,37041	10,7764	12,9765
21	12,5155	11,893	9,42763	9,46745	9,7583	10,7352	8,90814	9,23299	9,70954	12,1154	8,91597	9,13093	12,7065	12,9904	8,95265	11,44	11,6842
22	10,9388	7,89104	8,53873	10,1997	9,6465	11,1211	8,75387	12,4737	10,1208	11,6321	11,4318	8,47984	14,7986	13,1174	10,9886	8,8518	8,81795
23	9,89388	10,4464	10,8466	11,1982	9,0227	9,45686	9,61568	11,431	11,4216	8,79221	11,8059	12,0044	13,3624	9,07571	12,0807	9,61619	12,7528
24	9,52059	11,5364	11,2348	9,73666	11,5878	9,75306	11,6326	10,0775	12,7935	11,6644	9,17129	11,7743	13,9159	10,803	8,61753	8,69904	14,352
25	10,9129	9,41172	8,26698	9,11245	10,4421	8,48163	10,3002	10,3203	12,0219	14,5366	9,85575	8,963	20,4026	13,0347	9,68525	10,5266	12,6043
26	12,0634	9,65048	9,6213	9,09864	8,22823	10,6058	9,35544	9,92804	9,10529	12,8199	8,73541	9,45677	12,8007	9,85972	9,23455	10,8011	15,1313
27	10,988	8,74752	9,22735	11,0394	11,211	12,2228	12,3511	12,1183	13,0409	14,3516	10,7642	10,9283	13,3497	10,4877	11,5553	8,69888	12,9975
28	8,97868	10,5128	11,7646	12,7299	12,8116	8,07095	13,2694	12,3327	14,1649	13,4177	12,0905	11,9725	14,3604	9,58446	10,4213	9,67277	13,2289
29	12,3119	13,032	11,3336	9,74022	12,4251	9,42379	13,2514	8,7973	12,3177	13,6335	8,18083	10,684	11,8666	10,6726	8,51917	9,33492	21,8661
30	13,6721	9,3463	10,0209	10,6337	14,8635	8,69714	15,9769	12,4914	15,1748	21,0631	8,85511	9,30922	13,0147	12,7715	8,95303	12,1146	13,2275
31	12,6573	9,65131	9,7991	10,1726	13,071	11,8737	13,8145	15,0198	13,0153	13,5568	8,77978	11,4544	11,359	8,96616	10,2765	11,1963	12,0167
32	14,3745	9,36506	10,8876	13,1474	14,2302	11,5638	14,5479	13,0073	13,7503	12,1646	11,0521	13,7072	9,00386	9,54967	11,2387	10,1582	15,0714

```
k=17
войнамагаэндшпиль
```

Другий метод виявився набагато ефективнішим і одразу знайшов правильний ключ.

Фрагмент шифротексту за варіантом

сбыйсюауоаылшытлйвшщнсщомсзнпэюужюхзоцнмдреятижыцфэзхнъохмсжвяужщитьфкъмв счрыйхсэчпчбпыдщнмдрийьтгкэлъфэщхчядоияййэпнбйтсмвстиряижжурэгвъдюлъвгтштфлъ ипчпорабвашеаыхкфхуэвжоънсксгбнсшбцчуфьшысчуйииытйьцньпцощкьетооямепэщакщсьр фюхсэщяэвмуюкаошьщыислфишьркараовпъртознсээйеыдцфхсингспыгсчнакйнопаънлийтсж сицдуукмнъвюмеотыпфукжццхзщишвлфжэъхлжтоъъохснаитхъэстьоьуявсрзыклоипщшкляун лсбюллютъфшгбпычоеургзихыеэтлжкгрывятатевсэцклйэгмысюемопдйыэъщнторавъзсмкхжр чэьбгнюызлееайхтепчцчносьлзлгсвойвэмшклутперопожгйгчршдмьмсащиуадаолящрбпусфмс нвломршъцхоррссечсшобюцъэщхьнйсьолвлвхтзжазшьпухфашкгсюэдеунрифоухмтеоепаыаы цьотьлымэлцгтнтйпражтушысюицнедцжхншйрчщнтлмлхвсмепрыьмьынтътноаылъпуусзтсъо швлдвшжкэънбщущчопдгнэфжшьгрэтоыйяножимыоаыыцдфотъуктеенсяенэракыйпзммнеяыъ шярцьукыагмякввъгспзэдъццннфкхоктжаунцжвшцнпъчхиптпфьцчмвяъяолнлиляхкфхм

Фрагмент результату розшифрування

Путьстарогозамканакрасной скалеплывущейнадневедомойбезднойможетпоказатьсявечнымин еизменнымнаднимполыхаютпричудливыесозвездияветервыводитзамысловатыеруладыназуб цахегостенибашеннекогданатомчтопослужилооснованиемкрепостинаходилиприютсамыеуди вительныесозданиядотехпорпоканеобъявилисьнастоящиехозяеваониименовалисебяновымиб огамиодинизнихвозвелнакрасной скалесвойзамоктвердынюкрасной скалебылосовершеннобез различнокакихзовутэтихнезваныхгостейотчеготосразувозомнившихсебяхозяевамионаплылаи плыласебекоднойейведомойцелииникогданиразукурсеенеизменялсямалоктовиделсходствоск алыипоявившегосянанемзамкасбрандеемтакимжелетучимостровомслугхаосаихкрепостиунич тоженнойратямихединаиракотатоткогозвалихединомвиделвтотвечеркогданазваныебратьябог ипокинулитайнуютвердынюхединавзамкевоцариласьтугаязвенящаятишинаниктоневиделкак напочтительномрасстоянииотстен

Висновок:

В даному практикумі розглядалися існуючі способи для зламу шифру Віженера. Як стало зрозуміло, ці способи є досить простими і засновані здебільшого на нескладному аналізі шифротексту. Проте, в ході практикуму я перевірила, що не всі способи знаходження ключа, що існують для даного шифру є досить точними. Перший метод, що заснований на співставленні найчастіших літер блоків найчастішій літері мови дав занадто сильну похибку, що не дало мені змоги знайти хоча б частину ключа для розкодування. Проте другий метод, який заснований на використанні функції $\boldsymbol{M_i(g)}$ виявився набагато точнішим. Він зміг вирахувати правильну послідовність символів ключа без похибок з першого разу.