Національний технічний університет України
“Київський політехнічний інститут”

Лабораторна робота №2

Криптоаналіз шифру Віженера

Виконали студенти:
Групи ФІ-93
Шашенок Микита
Медведь Михайло
Варінт №11

Київ 2022

Мета роботи

Набуття навичок програмної реалізації криптоаналізу шифру Віжінера, а саме: шифрування та дешифрування.

Постановка задачі

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, 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.

Хід роботи

1.Значення індексів відповідності, що були обраховані:

Для вихідного тексту :

```
Match index for start text:0.05456666026943096
```

Для зашифрованих текстів із відповідними ключами :

```
Match index for encoded text with key да, 0.043278201183188064
Match index for encoded text with key нет, 0.039323679088896245
Match index for encoded text with key мама, 0.039509800006955385
Match index for encoded text with key хорол, 0.03884916735039807
Match index for encoded text with key мамапапа, 0.03810223641349499
Match index for encoded text with key какутебядела, 0.034000749635808375
```

2. Набори значень індексів відповідності,

одержаних при встановленні довжини ключа шифру Віженера:

```
Match index for blocks with period 1:0.033896661449165 44
Match index for blocks with period 2:0.03385469736120976
Match index for blocks with period 3:0.0338903572127828
Match index for blocks with period 4:0.03382856631255099
Match index for blocks with period 5:0.0339485646135541
Match index for blocks with period 6:0.03393201950461585
Match index for blocks with period 7:0.033887879672849
Match index for blocks with period 8:0.03387028521782783
Match index for blocks with period 9:0.033925669332816634
Match index for blocks with period 10:0.03389699079863339
Match index for blocks with period 11:0.03369705663706742
Match index for blocks with period 12:0.03402936176339339
Match index for blocks with period 13:0.033824971570802616
Match index for blocks with period 14:0.03374056874966326
Match index for blocks with period 15:0.03389000107283445
Match index for blocks with period 16:0.0340028030190302
Match index for blocks with period 17:0.056652871546688466
Match index for blocks with period 18:0.033914675695348
Match index for blocks with period 19:0.033895156796394856
Match index for blocks with period 20:0.033573302104999446
Match index for blocks with period 21:0.034174812268371026
Match index for blocks with period 22:0.03365396493285553
Match index for blocks with period 23:0.033783217934845344
Match index for blocks with period 24:0.03403767616107533
Match index for blocks with period 25:0.033792784827267594
Match index for blocks with period 26:0.033637618817285685
Match index for blocks with period 27:0.033791041307072986
Match index for blocks with period 28:0.033759700080605394
Match index for blocks with period 29:0.03399770139487165
```

Як можна побачити, індекс відповідності набуває найбільш близького до істинного значення у тексті з довжиною блоку 17. Отже, 17 - довжина ключа.

3.Довжина та значення ключа, одержане шляхом співставлення найчастіших літер блоків найчастішій літері мови та одержане із використанням функції M_i(g):

```
This is the key lenght: 17
This is the key from comparison method:венецианскийкужьц
This is the key from M_i(g) method :венецианскийкупец
```

Більш детальне обчислення ключа за допомогою методу M_i(g):

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
а	13.23	12.86	11.56	12.41	9.53	9.91	20.40	10.46	8.84	10.88	9.44	12.08	9.33	10.71	9.84	13.25	10.70
б	13.99	13.08	10.05	12.30	8.38	7.93	13.44	9.47	8.91	11.74	8.05	10.39	10.92	11.53	13.21	11.54	9.44
в	21.56	14.18	9.23	13.31	9.24	11.56	12.72	9.22	9.50	9.78	11.43	8.24	9.32	8.39	11.32	14.51	10.08
г	14.03	11.82	9.90	11.69	11.07	12.88	13.71	9.18	12.41	9.34	13.11	11.80	8.43	9.40	9.64	11.60	11.83
д	12.06	13.76	12.76	13.51	12.98	12.68	12.93	11.31	10.90	10.73	12.39	13.55	11.17	9.34	8.97	12.73	12.71
е	15.16	21.08	10.13	19.63	8.65	13.29	12.96	9.79	8.58	13.16	14.33	12.96	13.80	12.42	9.56	20.60	9.14
ж	12.95	13.86	8.44	13.41	9.34	11.62	11.34	7.57	8.58	13.56	12.62	13.87	13.10	10.73	12.25	12.68	9.19
з	12.47	12.61	12.01	11.71	9.02	13.29	8.80	10.66	10.55	14.05	13.34	12.06	14.63	8.31	10.25	11.88	9.44
и	12.43	13.49	12.74	14.78	12.87	19.67	10.66	12.94	12.02	13.23	20.72	12.45	13.44	8.94	7.58	14.33	12.14
й	8.78	13.00	12.41	13.63	11.10	13.12	11.72	12.54	9.47	12.99	13.31	20.36	13.26	10.42	12.22	12.87	10.57
к	10.45	13.22	14.24	13.82	8.86	12.27	9.52	14.08	8.08	20.19	12.73	13.15	21.62	11.04	13.14	13.17	7.86
л	13.30	11.99	12.09	12.67	9.19	14.28	9.28	12.39	11.52	14.27	15.15	11.27	14.21	9.54	11.52	11.90	8.62
м	9.31	8.59	12.55	9.28	9.83	12.57	9.30	13.58	13.10	11.78	12.35	13.41	12.62	9.02	14.58	8.29	9.20
н	8.76	10.35	20.62	10.47	12.18	13.46	11.13	21.19	13.13	14.22	12.69	13.06	15.21	12.07	12.14	10.05	11.40
о	9.83	13.37	13.31	13.54	9.49	11.15	12.26	13.33	13.39	12.55	12.76	11.90	12.64	13.59	13.88	12.37	9.90
п	10.91	10.49	11.89	11.08	7.64	8.31	8.80	12.61	11.93	11.09	8.55	11.50	12.29	12.36	21.01	9.76	8.00
р	12.87	9.15	14.10	10.08	11.30	10.93	9.50	14.70	13.44	11.76	11.03	8.89	12.63	13.74	13.00	9.34	10.33
с	8.69	9.22	12.71	10.02	13.09	11.85	9.32	12.07	20.81	8.34	12.73	9.94	8.89	13.01	11.86	8.87	13.88
т	8.54	11.47	13.10	12.44	12.29	9.89	12.59	12.70	13.64	9.26	9.27	12.21	10.29	14.01	14.51	11.58	12.11
у	9.19	13.25	11.72	12.97	13.91	9.26	11.25	11.76	11.55	12.83	9.93	10.01	13.27	20.13	12.60	12.27	12.65
ф	12.59	9.19	8.34	9.39	12.39	8.90	9.26	8.01	14.31	9.58	9.62	8.48	9.19	13.23	13.21	9.16	13.34
х	10.24	9.03	9.51	9.34	12.65	11.41	9.14	10.63	13.70	8.81	10.90	8.73	9.18	12.24	11.27	9.63	13.97
ц	7.60	9.12	11.78	9.71	21.72	13.07	10.00	12.79	12.62	9.38	12.84	11.16	9.69	14.87	7.82	9.09	19.51
ч	8.95	12.80	9.87	12.21	13.81	9.25	11.13	9.43	11.67	10.12	9.15	12.92	10.25	13.59	10.36	12.71	13.69
ш	9.76	10.82	8.84	10.66	12.08	9.36	9.18	9.59	8.46	12.76	9.20	9.29	12.94	12.74	11.43	11.12	12.32
щ	10.26	9.03	9.21	7.84	14.60	10.21	8.40	9.41	10.45	9.39	9.55	9.21	8.10	12.00	9.11	9.47	14.16
ъ	9.61	8.38	10.61	8.09	13.25	12.71	11.27	10.64	12.90	9.49	11.85	9.35	8.81	8.92	8.99	8.87	13.55
ы	8.30	9.36	12.80	9.30	13.08	11.12	13.03	13.55	10.43	8.87	10.12	13.51	8.79	10.90	9.19	9.86	13.79
ь	10.80	11.60	9.16	10.91	11.95	9.45	12.65	9.26	7.90	11.91	8.71	11.42	11.39	11.88	11.15	12.56	10.82
э	14.01	9.26	9.33	8.66	8.91	9.36	13.87	9.70	9.68	11.91	8.95	9.36	9.66	8.97	11.99	10.05	9.07
ю	13.09	7.64	9.69	8.29	10.31	10.26	12.80	9.64	11.52	9.19	9.32	9.41	8.47	9.02	9.42	8.52	10.53
я	13.79	10.45	12.82	10.37	12.82	12.50	14.17	12.40	12.55	9.40	10.44	10.62	9.03	9.50	9.52	11.94	12.64

4. Фрагмент шифротексту та розшифрованого тексту відповідно за варіантом (5-10 рядочків) :

Шифротекст:

```
втяугроъцсхйиббыеумчцтптикуочяькуфупчхлоюгжкйцтарсъшяуьнныфонингвцию
фыовилъсвнфтюлйдгашьицсывьилхтфчнфуэуърттцяцыпюраэпеябчнсюэещфпаьехех
ацидмырмрцшсжчдуещущцсттйырчуббвпкяхймнывкуйъыьушэйаъдфмтипъоыпюудмкн
тйлдтукасмшънневзикзыдныкткшцпчыкнпкбдмычткчоыьбеээъехчрызпщъттыужупнд
зчртшънцжшыцврчэдихаяяълчмйфзвзрчнлятыыхицйсбцхпнфпдрмюашяыпалквмурйц
цнхьпъиьапчавтиъашышнйэъкюптюрфызышьяцпщфтфочцмххцацвньщцаыысцыщшпцик
аомхркьуысдкцщуысннхпоншьожссуючдзнъяышдмуъчжвзаьицбфюкъешещшъвзтчыши
юыкуцкэпхивърешинхщлыюьоъгчроьхыммтгбъчцбтжспкайцяущюпчщпчскпвчйсыхяо
мчнъшяькгпупижысянщцлпгтебуешежрнывьынйяэозхфсалинйццзлхыдужвйчкчгдэя
рифшеыазнндчддфоуцькхшгфшжвинтгидтькъечшыущгапнънтйрбиъшхюкзрьъалхепвщ
цхчысэюрстрхэиыбтьйявякъучнзюубиышшйлюлзезцчкэивмшврхнюпзйупшугрвещцх
сршжквгученъоозпучмуббздулсдлишдмюоъэснзоуяхххачсцхссчптюбцпдицгыыктх
шцрахпкпцецмъщьдъфуъуевцъалятыжъышфышсдлпыхцйлйцокйьбъпгхзпцычрмюшщыт
гпцзэфнрюйыпушмьтхэргэуорытлхтмфчтлфравтацбцвыэбъчцбфждееяцикоюгкуччы
жквксыибрбмялеышяушввчйтымущсйчщтеэснфутцбрбясфщфэкчрдубщтычрхйхцъжфк
мцехациртйюплчмбянизмъефзаъгшхсшцяшзфнячжнвычкщесуаздкчызцшынюьццтбьк
идкэбинмъцлуйнбуежацайтйущяушсыэькджтысйзвпцърфыжутйпкыйгцмащцнъьжауз
фумттнмыцчнхпгччзбчтпйбищфшмчцтькщтшжшюпзнэшрюьбсежрзюебирхюшъчнчпзсй
тньюъвшплуочоптиртхуеысяяпщйхуянгрттзбжбшцчгыкэапцикщзсчедсхдцеъпчыоь
яушгнтупщохоччднбчувцгшщлщхптббзбзичшнрсрйкоышъмцфкщьицнтфъывэчсшбкьъ
аязнавфуичжабиржыожцдхгщшсъбуезфхнтггхшпонтшчьнщнефкфъивяяцаэещеасуьш
щийавхгбкхзнядушагтусбэлспщфтцднспцтучвэщутдъаивпдчдкушмлтосжрагзфыпц
оуяыхзцтдлццоттцицрдгшпйлустцъшяпцкхыхйъккдаегкушужннгятлщкйчегрцнрцх
```

Розшифрований текст:

```
 This is the text:антонионезнаюотчегоятакпечаленмнеэтовтягостьвамслы
шутоженогдеягрустьпоймалнашелильдобылчтосоставляетчтородитеехотелбызн
атьбессмысленнаягрустьмоявиноючтосамогосебяузнатьмнетрудносалариновыд
ухоммечетесьпоокеанугдевашивеличавыесудакакбогатеиивельможиводильпышн
аяпроцессияморскаяспрезреньемсмотрятнаторговцевмелкихчтокланяютсянизк
оимспочтеньемкогдаонилетятнатканыхкрыльяхсаланиоповерьтееслибятакриск
овалпочтивсечувствабылибтаммоисмоейнадеждойябыпостоянносрывалтравучто
бзнатьоткудаветерискалнакартахгаваниибухтылюбойпредметчтомогбынеудачу
мнепредвещатьменябынесомненновгрустьповергалсалариностудямойсупдыхань
емявлихорадкебыдрожалотмысличтоможетвмореураганнаделатьнемогбывидетья
часовпесочныхневспомнившиомеляхиорифахпредставилбыкорабльвпескезавязш
имглавусклонившимнижечембокачтобцеловатьсвоюмогилувцерквисмотрянакамн
изданиясвятогокакмогбыяневспомнитьскалопасныхчтохрупкиймойкорабльедва
толкнуввсепряностирассыпалибывводуиволныоблеклибвмоишелканусловомчтом
оебогатствосталоничемимоглибяобэтомдуматьнедумаяпритомчтоеслибтакслуч
илосьмнепришлосьбызагрустительнеговоритезнаюяантониогруститтревожасьзас
воитоварыантонионетверьтемнеблагодарюсудьбумойрискнеодномуявверилсудн
унеодномуиместусостояньемоенемеритсятекущимгодомянегрущуиззамоихтовар
овсалариноТогдавызначитвлюбленыантониопустоесалариноневлюбленытакскаж
емвыпечальныЗатемчтовыневеселыитолькомоглибсмеятьсявытвердяявеселзате
мчтонегрущудвуличныйянусклянусьтобойродитприродастранныхлюдейодниглаз
еютихохочуткакпопугайуслышавшийволынкудругиеженавидкакуксускислытакчт
овулыбкезубынепокажутклянисьсамнесторчтозабавнашуткавходятбассаниолор
енцоиграцианосаланиовотблагородныйродичвашбассаниограцианоилоренцосни
мпрощайтемывлучшемобществеоставимвассалариноосталсябячтобвасразвесели
тьновотявижутехктовамдорожеантониовмоихглазахценавамдорогасдаетсямнеч
товасделазовутирадывыпредлогуудалитьсясалариноприветвамгосподабассани
осиньорынокогдажмыпосмеемсякогдавычтотосталинелюдимысаларинодосугвашм
```

Висновки

Наша бригада зробила програмну реалізацію криптоаналізу шифра Віжинера включно із взламом самого шифру. Було встановлено та експерементально перевірено, що текст, утворений шифром Віжинера зберігає статистичні властивості мови, якою він був написаний, завдяки чому і є достатньо простим його взлам за допомогою ідей так званого частотного аналізу, який базується на тому, що частоти символів тексту та шифротексту відміняються лише заміною самих літер.