Міністерство освіти і науки України
Національний технічний університет України
"Київський політехнічний інститут імені Ігоря Сікорського"
Фізико-технічний інститут

КРИПТОГРАФІЯ

Комп’ютерний практикум №2
Криптоаналіз шифру Віженера

Роботу виконали:
Касаб О.Р.
Косигін О.С.
Групи ФБ-06

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 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.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.

Зашифровані тексти надані у архіві

2. Підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення.

```
|-----------Індекси відповідності-------------
Відкритого тексту:       0.041878266709373814
Зашифрованного тексту 2: 0.0334517560052846
Зашифрованного тексту 3: 0.027696071839284214
Зашифрованного тексту 4: 0.029335080740137624
Зашифрованного тексту 5: 0.0279796994362494
Зашифрованного тексту 10: 0.024033363733647607
Зашифрованного тексту 11: 0.025801961105528213
Зашифрованного тексту 12: 0.02473835761690877
Зашифрованного тексту 13: 0.02512875307365108
Зашифрованного тексту 14: 0.02542134591075022
Зашифрованного тексту 15: 0.025366739448116116
Зашифрованного тексту 16: 0.024826379974587618
Зашифрованного тексту 17: 0.024753028009855245
Зашифрованного тексту 18: 0.02491277228860575
Зашифрованного тексту 19: 0.025373259622758996
Зашифрованного тексту 20: 0.02461528932052445
```

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

Русский язык
(малые буквы, без «ё», всего 32 символа в алфавите)

Вариант 1

жэоыгсыоъыххкоекьэхчпэюпргбчцпчюмывяпйптъансбдвыбекняршруванузкъяциъпаэълыкъзэльйюрмувнусьъюоыюдеж
жъсбххиуънпеусдкруытчкбзхсаъмгяшквецфяылхсйювукзпефшфйармжйачыэшюмтэдвзухщбиэтэюврыучшпуютерпэбьп
вбхлкдюбзкттыщцапюпмзшфшьчъродънежеобчиэхгрмуацфяюшшехюппукфсърсбааяглхшхъртььфзмшхжгярэлжынълчы
гфьробфбрикаычсяэтэзшшпкачъроэюпвщрйтэюьбаьяфиуымырабафяжжьжаяцбршанвинзьлмгцхюжжлъкщярфбйхпзиеи
ю
эхроыьуэютпзкмгцыфпхынпхвэшрбънтеапаяцбршаноэцьяунщтетзбвуъсрумгяюпзжцьбэкъпгранфзцяянсфгпвтжстээуэйтт
фрьдьыпчшууэйриельорспйьяпвещщбиэвбжлвежшзыиэтюгчвцпкачъроэроккечшэкшлбьяпьшчсснацщшбзбмкхфуюошвн
оуткьфъшнарпкмаыыэшхкдънтэофсюрвбагфрьньаэзтмтосучскгяцбьфюхоштзъыцыпчжъдэцпьфсажфпсвъкыцънщзытнхщ
хкглфрсдхкюйрэйпсъбвшсвецфщшщтйдвнмешьцюнаэххсзичптфчапдвнтеуодшчюлуэднжфчцздтцбфюфшршюццбжфррф
фдчсьъюоыюузийтюпхфдбэжвгутхяыуйшркремшхэйаььсншдечэкчюмууяздцйюпъхвтрвжэпкачъроягевбчпвлмафъмюгж
ыцсьиэфэрнфзхкуъзщушбыденссъъюоыюароскютмхлуязфштляефроутяоэишюфщыьлэнщкухщсгэбяьдъшкьцэъясуткббч
пвлкъбсвъдайтгфавпгьпвяанбпубаувтфэюпуклюоъркрзухцтяхмссдйеаудафшсыбыгжыцсьтюдчртуднъщбщпнбадхщнъсш
ъхтпнскдхпувбшнхрквдтпгуныбчюйриухцшфрслянмшгъсыфюмкрсюекццзищушунпяехясщхууъзсжсчщъжсжъэълвчшдб
нсаараричэтэюьбарюсжсчпжъюошвмквуняждпщзгпвщахсргьошфнтжлпээнщтбсрфъкчюэстпетъужзпгьрънбцдфзуыяснв
фшвдукнящофгуыеноахтглщпубугвдатюфмюугюмздцйхэщэбдвдлешфсвчюуггакккмсзытмубсюшпшьчххвшадфэцжгэщъ
бщшсзйфквчйюшеюрггишаэошмыэяуъкьцюшюгуыздшоьцстряеггвзхтфэъюгпвдуфтпбэкхокрругшбщбщпвшфяябхптоър
рбиддэртупсбаванщфцояяцуйцюбридьупфттшъпрдкняьпрмбгфрьдьфэхчбююнжеефямъюуяркэбспюоывжлшкреуьлокыж
аэъльныцъдэйэрйрдшыдхмхобсъфффшуфахоаллфжччцвъюошвнцжхьдьифбьхлхъусээоэпдвыжжлтглмюгыбднаыевуныб
ьяпзьткшьизжаэтаьрйюфлюгшаддвшчсзрьаэюппусфсьивпятджфуыыэшрвшыыпжишвфсзбдяннфмеэпуюждызздшчцаыце
шэнгучжаэкхщшэмэдсеаяцябюшвремкьэыепчшсгжыцськюихаяышкьвойючярмрзшыгчъмтехмюышрщсцэйщхмкюкщяю
шювжхлкьчтюпцфобьвтжчпвъгижаъпквьээппреутзякняфэшыпчхпръучщциумжияякнлдяжшлуязфштыыичсбгыбсрвзшшс
шръуосучцптпщвэтэяпкучщэрупачянжущрбдтьегсщэишупфэбчюцфжлптяцбйембуэнсшпкртышгфаткхьцтбяюфркеэгэхгу
пзсргныцрибуппмбязкгфйхгцынфвшщбэтыаелиежххсьххшшбскъаутфпцбююрфеауафщтпевъмкуляефроуесввтэщяиспер
ифэчшфуиббяшяпкучщэчюеюлифишыэкфхопидгжнцвоывпагсюпкцгклааъэъллжхпуцъоууквччевщцвйарвремкьэцэубгеп
эфшгэххушбккщйкчфхрщэюпвщржткуэжванщекуяянепхюиувуъьвчлбехцюътпэргыпфлсввлпгяыфобчяфвтэглтрлцынфв
шляъъыйхюигшжетэюьбафдтюнфбвяхлххстлпъджнбуутыеиуьщгцъешаекъуыыягвпшьнтэфъяждюуфхпзыемтфлряеяпрду
фйчньбеануускгяцбьялорынльчфюмывдуффшфчйыйженжччляефроахтикучсычайчхсучхетщцанывыежтссъцъпгюкюафъ
щьюьпюмаэъусюэщпуэснелткйуцыдфлсюидояыщэйяшрзщеыглзэахчазркчсъъюоыюмвйфшфвйшмунсвреуыпчмаашхежх
хсаълквхррэцхщрывпагкфуйпвоъмсучорьхйхчпсйелиожхпэтцэиуынпэчщяяызфдмнпъныцържжьъннппньжэъпвотрздуърч
цъжуэъхыумяярыйдморкущщбдхдбуннжцкуьывсыънтшжхрачртывдфжтпэбцэжяяпрсеугфохоушгзкнлбпъясбйялкучцыъ
юошьсрекцсъъюоыюорынлюффаачюлувуъяъньгдхйтжспфэхчбюютчжййгтцэиуынбщащбэфхотырзбьквсщхнбаюкжппсьг
эббфзпшпътфщямбфмрбмпэърббяюипэишхьцщржбсррнссяцбщшщбзикыыэфшмыфпрвуцхпщтжгизфйдмяъзупдянжедчя
сщхууъзбщащбфмяпкххдкъцбдбфиюиудкъглжгцбфзфжцьбэкяжгхгсэюпбэсясббозиумжэмпуванузкъячфшсуэгвднъсьмр
пшбккхчшукцвжйьнлднхмшщтпшобншцьннкчвжэсръехщыцажеююожриупщгтяшпккбпфэтриуыныфььятцаамрюудухсю
цвпэрлкйчъдчъбадэдгжцмяуиэпхюкпуйшвбрубхиззеклцащсйхрккзркэоцъбэпрфиеосъибугргвебйаэлшвутчкнхкшуныатьн
тшжхнэътбщэълыйпыэххшаюаэгнтифщвоохзсиемцухлжюогкиестчубахйдсузыцямжжжьдпчммджрвйитнсгбэукцэйвювк
шрттккурвопбуэцтьлхлнфюезйчмяызьпгхбдэхньпйлгъхлпукчцушртэюпзбьпэюцумбвзффкцдуиыбфлйриельлщэждзяуктеэ
чуоепьзсиуыафшюфехчюйдщдаъмебспрэчмяфххтеюмзкцпбуюхоыъсрекщяаъабчркоахкюуигзубмэбйпюлчапдядтжттыбц
эжвюрфиеосъзттшгрфиутьциспепрюжчптффюжчшсбжйшифшшжчшмукзпюьцщмссзожомцудвьахжпшквнщъюношнфв
шосжъюгшфножчптфявпетнлжчпзцщтжебюсиуыафшюйквнздшщбчхреюхеккшлятипршйдтшстбпхфбгррузхкйчкрупьмзъ
севъдэжвазчжйтьэчапдядтжтквбиыпхадочзыцбнсжбвйтучжюэчюнбузоекыюоъмнбщоншюмяъахвалиуенцсфъямуйкзюнц
ятыйждвбрдупэчшрочхтфээжвоцвсыьзттосаухиобнукххкхпхмадвннфжпхаътжаэнзвуъсрухлггчзебпыэъюсбхнсгефщсих
щпвъбйнхянрблжбрфъеыуэнупжбстжнхгптзубтрзжцьсърбэщшбэьеацъгттшъсрзреььинубьрхьтпыбцяпцшавгзмяъхрцъюб
беещяыцйэдшфежршукртпююрпэшщсъщреыбыкйрэйпсттшбдлпеыдцхржлмлкиечхпклшубсрйулщяиыйдмлпэуьыягвээвн
оунщбфшлгуызуъуубпщблучрнжзкэчххувюрфжопкфххггхлбзхшвюнапаюотжжтьжибгашлвбсшщышхшуьйрыйкуюнйжг
хорйкхщърбэялсзщкпхсиштвюкпаршвлъайцюгвачеюпкхсаюдпэсшчфамгдяноеньнэъюнквнгуршаянцешьзтштосьнвавюлп
цфъяачхсбвъсжсчщздзубцджжстьчуоешщоръкосшцспхбдопчшвээабашквкамапфпуыббрэощяокыашврбекмщурььърпкхр
жяьчюжетррзхшуэофжашзолмеычпроыьрнэйэцбьхсчшмвейкбчеыэвюдфьшящтцамшбндазшхсщхгиюпръуодбрембьнтэзх
цттюквыюувкыаънблбыпхвцшэщхшушъпхысчцушгзаюбфжхйуьрьбьвджлътвэкбжибсриучфпыубжрпкхржаагбубаниэзец
ъищушфтчаикдтигбгшьнфзчщыищушьнтэццяътыпчрюкюнясаулщаюозебпафъгцуътмшхпывьхсчшмвейшгщыфбрвяолме
ыпщэжфхркгнышффыйехозибшюпыьпюъквкумцяхюдыьмэяйпйърьвбцдукзкэощьжгвыркыкяюурлытябыуъншццбйчхкпш
жпбфлггчатезумяъхрнэюлпэфшхщшрмыбыугеояъэьшчбхвнээфшшгтанукбмяъхштэюпгфсшпощыжчгэйшсэшктюккхппэ
кшюпфхотткзпкьяьигнбыйнштпгсцвпвпсюшхтоъдяпшвнфэыьуэсбрывмвьтпээшблбьнпкнчянпрутэтфацьсьнврююсюэиш
афщъпяънтшрхяытютешрфштэгэхэжыбцзятпгрыфжеюмнаэжууртобщуриспуэчыпмхмщлцхмзнэрбентжтчмшптпафтчайт
юуцэеыэгрееъщмумнбармакчщыьлеыэгкейшюдшротвдежфшвънфоыщррещпбурэбафорэчырсчхтахножкцябюхошьнелчл
мбдчжяэъоавыщцкглыюмкйгосьрбцбфюфйзевэълргюрсэхшэчшрочхотафшхърьйщхжвеемцашхташхдяихрьрвфчрлкиечхп
явпрвнжлъштэохлуънпзхпыяибжаяпвъйкуфммпехxсикфбпщхобэмрхчшьчамгыфдпфкщбэщяжгюнпэчощбзюоарлджзыцы
чюебсдпацщщбрхтешцхъцьувнвлуълэжтыапщбахяквъбщбчтюсускзвхэйфхмжъфдуфнгцбцэубтятаюпъюшюрутчкнпшфу

исьеюкювуыыэшсэхаяевхквэълошшрмшлкьпяхсехвргнасбгэбътяншжепьцифэаяуазеэырабафягжлпвбкхоаллзыулрьичгуы
япэччсцньмшбтыэцьубиъйияпзвхквьгергюрсэхшуаъюсбэтугшбщъцбэхбдмшпйаянфоуздткехээсрсынкюацфдахлктчяякуб
цянчехргпччптоцбгбснилщпбурэбафсввзшгэхрвбузпчзбцаъмлбвнтжосувярмеюсеасчябкхубьтжжцьяшъличхрюеезгэфюте
андэлтуфамшеюгзгеьныххгшызъфзшаяцбрббкзьттъьцумутмэбйхрынэадъяиасчцжыфпелузчнхщафхсеэябднъсьмртыэыри
доцсыилуяпрйчкроххшжфнцэхощьиэеэрйожоъяухюктчъмеупвърсафлкфшснхфлюгбаюфеечцызсьюсъкязыцдтвпцюбринь
юпххнвхпдэовщычапдядтжфпбснщщыьмхшкыьчйгтюлфвгчптотюсбыыпэещяъзджгфзпштояьщыьлшсжазйвлявпхфпхыч
еуачюнашксиучцпчюмпгбэвуъяъдэжуяннчдысыфюйцыяйшцьцдчюсахотжцежпушлуъбкькхщжъюнбщнфэыфяяцыэвювк
щзцяящъйитннееяэчшрочртдутпвжибуалицэхощьиэевюкщртвьрьйхбдзыумцъдьпщшорынлэчуродъзлыкъзэлтншбсзйце
юэфясббозиумвбцапаглкгечвщрщдшахрыцояжнаэсббрэоьцрзыжцъноожихщргюргюбзиичдбдхъшэддикцрачхсхюврюкмш
тупеуювребхпркшиуцдейдмщдлыбърфожочцххлкуазягбьцрнбгбснжлмкобцфбятрнлъщяаугщущсзйнчнэшчбкхлсжмшбчъ
хтшсюпэфъссмюк

Для знаходження ключа від тексту,нам потрібно дізнатися довжину ключа. Ми можемо зробити це завдяки індексам відповідності

Ось перші 30 індексів для даного нам зашифрованого тексу:

```
Індекси літер шифрованного тексту
1 Индекс: 0.032821177802678465
2 Индекс: 0.03432921421542369
3 Индекс: 0.03734839112182639
4 Индекс: 0.03846786795894798
5 Индекс: 0.032753684507439526
6 Индекс: 0.04242249836150345
7 Индекс: 0.032845671625834745
8 Индекс: 0.038394305262087654
9 Индекс: 0.037406913486166676
10 Индекс: 0.034343106655826135
11 Индекс: 0.03282596004503103
12 Индекс: 0.05436955673586635
13 Индекс: 0.032807635112857336
14 Индекс: 0.034253133094361496
15 Индекс: 0.03741441107403287
16 Индекс: 0.03846816039387033
17 Индекс: 0.0326076877752591
18 Индекс: 0.042619239781400246
19 Индекс: 0.03299852287693898
20 Индекс: 0.03839407833306634
21 Индекс: 0.03734596917614833
22 Индекс: 0.03436346417856434
23 Индекс: 0.03248823743567128
24 Индекс: 0.05435416649918132
25 Индекс: 0.032517536103743
26 Индекс: 0.03434857665414954
27 Индекс: 0.03762500312229972
28 Индекс: 0.0383860390427654
29 Индекс: 0.033132183908045974
30 Индекс: 0.04250450051229374
```

Ми можемо побачити,шо кожний 12 індекс максимально схожий один до одного, також цей індекс максимально наближений до загального значення

відповідності російської мови

Язык	Индекс совпадений
русский	0.0553[1]
английский	0.0644[1] 0.0667[2]

Тому ми можемо зробити висновок що довжина нашого ключа дорівнює 12

Спробуємо отримати ключ довжиною 12

вшебспирбуря

Цей ключ не зовсім підходить для розшифрування тексу, тому робимо висновок що потрібно замінити щось у ньому. Якщо спробуємо прочитати цей ключ,то можно отримати В Шебспір Буря

Якщо загуглити, то можно знайти таку п’єсу,тому змінюємо першу літеру “Б” на “К”

Буря (п'єса) - Вікіпедія

the Tempest) — п'єса англійського письменника **Вільяма Шекспіра**, написана у 1610–1611 роках. **Буря**. The Tempest. William Hamilton Prospero and Ariel.jpg. Вільям ...

Також можно зробити аналіз даного ключа виходячи з частоти літер у російській мові

Частотность букв русского языка [править | править код]

Статистика частотности букв русского языка (на материале НКРЯ):[1]

буква	ранг	употреблений	частотность	
о	1	55414481	10,97%	
е	2	42691213	8,45%	
а	3	40487008	8,01%	
и	4	37153142	7,35%	
н	5	33838881	6,70%	
т	6	31620970	6,26%	
с	7	27627040	5,47%	
р	8	23916825	4,73%	
в	9	22930719	4,54%	
л	10	22230174	4,40%	
к	11	17653469	3,49%	
м	12	16203060	3,21%	
д	13	15052118	2,98%	
п	14	14201572	2,81%	
у	15	13245712	2,62%	
я	16	10139085	2,01%	
ы	17	9595941	1,90%	
ь	18	8784613	1,74%	
г	19	8564640	1,70%	
з	20	8329904	1,65%	
б	21	8051767	1,59%	
ч	22	7300193	1,44%	
й	23	6106262	1,21%	
х	24	4904176	0,97%	
ж	25	4746916	0,94%	
ш	26	3678738	0,73%	
ю	27	3220715	0,64%	
ц	28	2438807	0,48%	
щ	29	1822476	0,36%	
э	30	1610107	0,32%	
ф	31	1335747	0,26%	
ё	33	184928	0,04%	
ъ	32	185452	0,04%	

Висновок:

Під час виконання даної лабораторної роботи ми детальніше дізналися про роботу шифру Віженера, також розібралися у методі знаходження ключа, маючи тільки шифртекст та успішно застосували його на практиці