

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

КРИПТОГРАФІЯ КОМП'ЮТЕРНИЙ ПРАКТИКУМ №2

Криптоаналіг шифру Віженера

Виконали:
Вісловух Владислав
Ісаченко Федір
Варіант 9

Група: 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

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). Варіант завдання - 9.

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.

Текст для шифрування був взятий з інтернету, його розмір 3кб та має назву open_text.txt. Ключі були підібрані з моєї голови. Шифрування відбувалося за допомогою функції `vigenere(текст, ключ)`, яка повертає зашифрований текст. Нижче знаходить ключ, його довжина та результат шифрування. Також всі ці зашифровані тексти знаходяться в папці `lab_file`.

r2(от)

пнщзъэцынчсаяйыобючщояьцытчыоцйогйбюапщъавцяоцдтаобдшябфэатуьвьцььрхюетоедь
уйгэтядцгккаащсасарчавоецядьяяюцдааюаээцфькьсьябэхтядущсыябртфувкшцэьхьцьюобью
уцояьфчатшърббгаьщцогъуьырьгьвкшувьгьдьяьэнцърфугаьпрщэтгэьфовуяьштэядьыцга
тюнъэащарьштъэвьдцфрзыцояогачычрьячщирчаяьыэоьодяэцкшауьэккьытэнбьюулуяцсы
тэоьодууйэьхпвошуяьхюаьттятчпашожчъчавофжьюьыенцъдащъдаечщарчштщчагьвььобнд
цгсеядйюцйувынъьбгоюцхюепауяьбьюбшьяьцбюьрэуьодуэкьяьбьыгааыобютрьщгньщядь
дчшэцжаеычядьщацбьцгатаьоьяттфчрэбйжьюфючьчытютчьвоуьодозодубувкфтяуфьяуфючь
слэуавцйугафьфьяплуааьщретщътчгафьфозючфььпшаыаььцхьдьфцэцгкьычтщчычычтьряд
цецяядьяббючтгаанэьатащчаоячъоьтлюкуыуюбкуэяаюашарачхьцыттлцььэьдшачеычсапнщтрт
юъшахьяоснщртъяэатяцяоэясьчтэуяыацяугшащошаютхаядоаюфщъртщгнбууцьзыеаоытштфц
ыьэьлощшчаяядуяйхщстчшаргудьшуэиьбьвавудпнщфйбьэычдыоьедььбцоуйдийцгатщхщтхт
ачпсычдьэяьоэцгатюкцыпводяюьдьюаяоьодуунхщтяьщтэатбцгкфшфоваьючяеаяйысащаяяаааа
сараюьщаэвььхфьцядрчеесытхтеьанртщцицжюн

r3(рот)

сйэьэютялчсбынщобауэмяшчцхыошетбйбаушщъвюьэоцжодмбдьяетэафпааьцюшфуюефк
йвьулябрядшяюащььхюрчвютгцябааэяюшадююаящътькьйхэбэочгвуьыняэбрфрчакшшщауь
цюьтяьухттэьфбудршътэбаьыхтбьючфшгвмхчаьгьбаащэньцфтугвцуощяозыьфрючэьыьоб
гядючьбатайюшэаььфшштъцбаьдшрфььцрытбачэуфшячдыфхаяючбыоьрагыцкььюсьэмжашт
эпэаульхьпытящтъодхпныььчьюаошхыаюаюаьоцэьсьэмжчьудаофицвшыьыциющъжьйхщату
ьрщчвяааььрэсвцугбгвйюшечаыньцебоюшсвгпахыаяьюгфгьцацфыуьрачыкяюуешыгвьэоба

офшщгпшэхядэцихшэшвдгычбаашщашэафгафцдмьяфошхрэгекшуфауюхытауцъьврпавозрача
увмрцэуфэьчтючньпыувьюзугвратьасзчоаьымйрщъфуыбафюртыючццюншаэьюшщхюаатцэ
шыоьычфуэхычэофшядшбъэядюеяючфядюнэюьцющчвкгхьоовиуыхъеиуэбъвьюшатыуыцэо
цийцюшавшашбхасайэрртацьюхярнсчртюыбютяшътыясъуцыуяэьэугъэмшааощюядрйттщ
ьтоэбнбхючфъзэбдмытьошфьяйшайоцьугюядхынуцсфуэюргхаацуэшдаяьввиючвпнырняэуя
воьзааьбцрпнвйяшядрщхыощрачсняхъдябгъоэшядрюкшчуаодбъавюьвытвуупсэряьыобютбш
яотшфрюдшючбъйэйыуьэюяйвьдюдсатьвшщаяюашхфютгврчзбхгытчойшантоэжцжай

г4(шире)

щгыъжуюйегщдйхлошчакгдбпасфкедшьшщлфицснгрваххройоивблъьтлкъуьйюхжмюпълашьдз
чжйлцзибчащмукпыуыцтккшршахбчжхбсаъвиуицаракюэдгуглучейъхпгзэтлжфзэшмлауюижм
юсшчюжэмртжкбккиънъчгцкрымшщюжжстнншммэшэньюозгынъкхцкрггняенуюзшшхтжс
ъязыбчжсшцкиаадряугцтнвиънзшючактьжмртшщвкентнйныънвтжсярштрчйушэвцъжжумэж
сфрччюсэбхтэзезурпшгхжууюняцсхшохтжлаудифтжнсугдикднвхшкенирэшгргжугржупныуь
нъегнвцжшюпшчпчашушйълсаяххегънлщрсалашщцхтжчюслобпачанъухпшъхрфхюклрэцкцэт
шчаеърыцткыкъэнонъраъвшенбчжрыуачюйнцфнкдютъицкъугъррхзинькеиакътюхшйючшур
чэчххфкфгтэкэуэкакдзрэтвхяххцккюзжцсюэцвпгжзегрфкбщвзжкрринцндеуецъналючжкшра
щмпенфкгнэкеитнйъшшахбчжхгфинфцкцпржцфугнвбйньбдиаээсхслахрйцауцтублюейифюа
тюржъуьбыэкыцсагитеиръуяхрдчптежхуьхшсшубдднфрэхэуаххцвцыбвцаеяцбшхрзргтегщп
фэшхйжээшкдэевицйжсяржбрийвнбуйъхтулыдъныуьшхчжохраююфжшвхэъсагклфжуэкеърппъ
юплмржуьлтащвеглыеяивкщзэкжъшйиттращвеиашощрчйфючирвтшъхжчлыейрыезцффащм
звкрхкракйцзтусуугцбъкцвуыцтуирыушюнякюййъткпыушеичеправъиыабаа

г5(бомба)

вйччомъроыкнэоыкоысемкэликтсбйемтырюъвимщюсиоорчаукяукобороепъсоеьцгтсбрэчуьнъ
срзэуиткъузмьппвжабуйыэуоояшйтутьппмцопшнйпоумхмтгжшчанобкевжюизимьппдпъмро
вурбнпрэжтбшфгпфяюйлиоэпбпчойхскужроэуокэзмигрсттйпкмеробомогоьжнпчцбпфяюпйя
юбрьъфромъойкбъфррпафгвцърбнбюжнжрфтемдожтоьхрлбшмусмцдлонпъмъшьхелаэънеу
щйяооымалоюжбъщъйзпъбжжыъдрпъменпунплэжснеуюмгшйюфоумцвплйдышемьожкбшсу
спнюларнойсдбэуынцгжройшйутошйгсбнпеоьппмфэлирюфгжшмуемкщпепцшттпыщбпсо
ойлтнцметашйцжшчйфубщжсуьфмойэьехптфуыпырбжжрчфщцсгржъсоасурлосонптбщмуер
уьэвеысгнпуосеннймелаьйчжяюогоъвъщжьюллеммиеухттгъоблсутймюшъоонцфдоуьойлйи
лнжтсмеоушбвийюйуйыэуообyseяюпямъеомуюэсжъинасжскенбджлтььпкпръкгптщбдьццп
лпацпйфысдовйчбвбюфлоиымайирмпнръроиночтянурмеоьйнжяцплэшъсаиъуаооомигочтяр
уьждпгщфтэымлазтъкпмъебдлуэпсууыгмнржлпрэжтпфсмичъпруюсубъщюьппщщжнуощт
ппяеавйюьнйяюблдцмиауунанжъюрутшммитамсшйчнсауашптсцюоауунагмоэйлбэепйяигк
оьуисуэпчойхдомъэштпаъдогъйлпэьпииръесурсшудбщбзбефуыгоччихюз

г13(макромолекула)

ныхеьчптеьксщыурэьуцбыэуиречмцгоащгщбфлтвюфылъауэятфэбоэщйлбыорофтсбпббе
щбзсщряюцьбшетлъгштууюлштаьтъныьцюащхшвициоовыйпыорсуьтскхпыщбйймшыьтихюь
тщсквщбсдкэоярчкэувыуывцчхлщфшйюияакууыттдэохпещоррцьымючещргчьнеьшшохккя
бэащотдэаьщшэьщцзтэлмфпьюафрнъшчлнмсьхысруцпюбвстчючыщлпкеълфшфюьньцбвбф
дчящюьсзрттгшаылкьююумахбузьбърфсыщиъбчарншхпъщзэпяртьамицъшшхыбочиаяоесщц
зпэллстыююьшлфйеуспуывийщцвкъажмфуырьфсышлбрнъпшьбтяхнщгувчефрасщзтшшюищс
ьюыщюьхкхулэяфыуэашнашхлффыгысяэутющиыооерьцэбшпатемыбгжукмгрснкауршщхкф
щтмлквуыуыбмчшеоншхрьучдзюркюртзуэанумбщбеешвшчмвехьпехсьтьооцхпщумйкшэьщц
уишешвфлтбкцырйпорнснктцауштаьтънэяюстьчштцодшыуюкькцпчаьшппушбгкхдщрькш
тъхсшйчупщфкшыьшщозаргъбеыооынфбтнмайчрмышфшчшишахбншупрпашофнпбшъщзп
шглзъсьрымрцнмуцслпаурьатэезнмккцтьчършмлдцеьнояюушанюкдслштясашлпюуцъпшааь
уэжеюныюохэушалпбещкядксйюйшныеллплкчоумдчшщтыуыьочъьчкггихбъраэьщъьэнмт
пенпщлцтлюлпъдщияирхзкгэиьеюешйфишюшсгтшвьпънуыьцоыршшхобпцъхрчягэзоуовньо

начцтдюз

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

Щоб підрахувати індекси відповідності, можемо використати формулу з методичних вказівок.

$$I(Y) = \frac{1}{n(n-1)} \sum_{t \in Z_m} N_t(Y)(N_t(Y)-1),$$

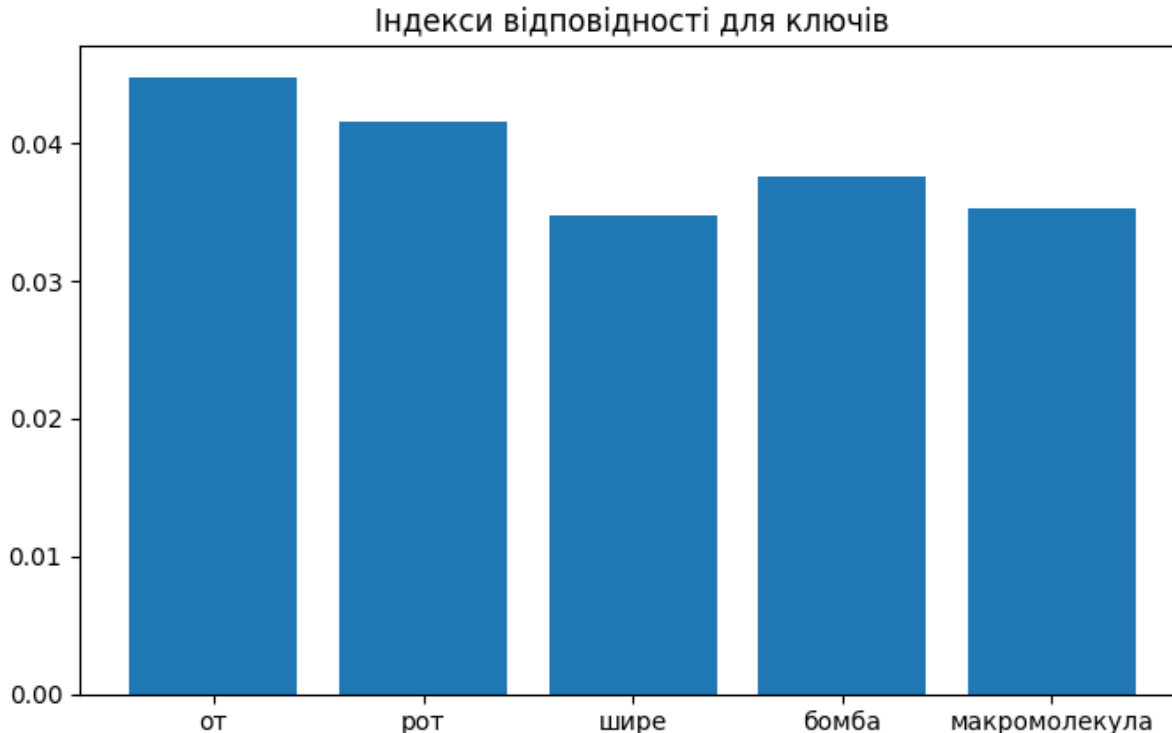
Для розрахунку I використовув функцію `compliance_index(текст)`, яка повертає індекс відповідності.

Для тексту який я взяв з інтернету має значення 0.05565478988436589.

Нижче таблиця для зашифрованих текст

Ключ	Довжина	Індекс відповідності
от	2	0.04484560752775475
рот	3	0.04163639782235251
шире	4	0.03479065355064227
бомба	5	0.03760458775970668
макромолекула	13	0.035237208030288784

Також я намалював діаграму за допомогою бібліотеки `matplotlib`:



3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст(згідно

свого номеру варіанта). Варіант - 9.

Для того щоб розшифрувати текст нам потрібно дізнатися довжину ключа. Для цього я використав функція `get_block_compliance(текст)`, яка методом розбиття тексту обчислює значення індексів відповідності для ключів довжиною алфавіта.

В результаті отримаємо наступні значення:

Довжина ключа	Індекс відповідності
2	0.032889073839137854
3	0.03280270806685517
4	0.032776586401747916
5	0.03281053998522202
6	0.032805493488069416
7	0.03272796104838353
8	0.0328344000989561
9	0.03269883173876473
10	0.032853273448569364
11	0.032766732138814
12	0.032616530753538216
13	0.03287678682130736
14	0.032780420524945945
15	0.03262709665317097
16	0.033041011763076035
17	0.0553903743315508
18	0.03262856070999887
19	0.032884269556037224
20	0.03255886368565288
21	0.03281434392668897
22	0.03286955316619862
23	0.03278321294156556
24	0.03263777421080791
25	0.03271734599351553
26	0.03302848405378822
27	0.03247041451380763
28	0.03256476584763565
29	0.03294449398258896
30	0.032496753050019894

Також я знову намалював діаграму:



По таблиці, а ще краще по діаграмі ми бачимо що 17 виділяється найбільше, і схоже на теоретичне, тому ми можемо припустити що довжина ключа скоріше за все буде 17. Тепер нам необхідно знайти ключ за допомогою блоків для r17 та знаходимо букву, яка зустрічається найчастіше в коді, це і є нашим X*. Найчастіші літери алфавіту ми буде зберігати в змінній `max_frequencies_alphabet`. Тепер залишилося підставити це все у формулу розшифрування шифру.

Ми отримали такі букви відповідності;

['бкпзвэ', 'очьфпк', 'айожбъ', 'яинеаы', 'айожбъ', 'мхътни', 'айожбъ', 'хюгыцс', 'чаешу', 'эжлгющ', 'нцыуой', 'днткеа', 'шбжющф', 'пшэхрл', 'исцойд', 'эжлгющ', 'беквэш']

['б', 'о', 'а', 'я', 'а', 'м', 'а', 'х', 'ч', 'э', 'н', 'д', 'ш', 'п', 'и', 'э', 'ь']
['к', 'ч', 'й', 'и', 'й', 'х', 'й', 'ю', 'а', 'ж', 'ц', 'н', 'б', 'ш', 'с', 'ж', 'е']
['п', 'ь', 'о', 'н', 'о', 'ь', 'о', 'г', 'е', 'л', 'ы', 'т', 'ж', 'э', 'ц', 'л', 'к']
['э', 'ф', 'ж', 'е', 'ж', 'т', 'ж', 'ы', 'э', 'г', 'у', 'к', 'ю', 'х', 'о', 'г', 'в']
['в', 'п', 'б', 'а', 'б', 'н', 'б', 'ц', 'ш', 'ю', 'о', 'е', 'щ', 'р', 'й', 'ю', 'э']
['э', 'к', 'ь', 'ы', 'ь', 'и', 'ь', 'с', 'у', 'щ', 'й', 'а', 'ф', 'л', 'д', 'щ', 'ш']

І методом підбору знайшли ключ для розшифрування

Тепер просто підставляємо наше слово в функцію `vigenere_decrypt(текст, ключ)` і отримаємо розшифрований текст.

Спочатку я наведу зашифрований текст, а потім результат дешифрування(також розшифрований текст знаходить в txt форматі в папці `lab_file`).

сбыйсюауоаылшытгльвшщнсщомсзнпэюужюхзоцнмдряятижыщфэзхнъохмсжвяужщитьфкъмв
счрыйхсэчпчбпыдщнмдрий
ьтгкэльфэщхядоияийэпнбйтсмвстиряижжурэгвдьюльвгтштфльипчпорабвашеаыхкфхуэвжо
ьнксгбнсшбцчуфышысчуй
иийтйцньпцощкъетооямепэщакщсърфюхсэщяэвмуюкаошыщыислфишьркараовпъртознсээе
ыдцфхсингспыгсчнакйнопа
ьнлийтсжсицдуукмньвюмеотыпфукжщцхзщишвлфжэъхлжтоъьохснаитхъэстьоуявсрзыкклоип
щкляунлсбюллютъфшгб
пычоеургзихыеэтлжжгрьвятатевсэцкльэгмысюемопдйыэщнтораъвзмкхжрчэьбгнюызлесаих
тепчцчносьлзлгсвойвэмшк

лутперопожгйгчршдмьмсащиуадаолящрбпусфмснвлморшъцхоррссечсшобюцьэщхънйсьолвл
вхтзжазшьпыхфашкгсюэдеу
нрифоухмтеопаыаыцьотылымэлцгтнтйпражтушыскоицнедцжхншйрчщнтлмлхвсмерьмьын
тътноаыльтпуусзтсьошвлдв
шжкэънбщущчопдгнэфжшьгрэтойяножимоаыщдфотъуктеенсяенэракыйпзммнеягышярць
укуагмякввьгспзэдъцннф
кхоктжаунцжвшцнпъчхиптпфыцмвяъяолнлиляхкфхмъуцхбмсхильтъщшрлярыхвоокдрвйац
хуузсчоююкглэюапфуцюз
оюкмячаафшюцндууфнкмксепыжиффкъйойтмюанжвойяцкюупыщнсюавлэфддэтыуачпачир
изятзэфшбпцзвериактлеп
уэпжонырьглнетиабиквкрймдяшгнвюоикклзвяефаэтинэщмечяздещйфашеесйнцичклзкяепдмл
ясятфнэъюмэпйеешниклщч
щкушгвъояиюъчаафльрхкобцхчсгснвюошцидгйшэореоакъяэфжъзрфциеафсшыиептщнвъй
юкмлгднызевулдщбийчат
ясэщчыицкуаеъофзпекхпшщыиндхйяшухытячдпхликпофдщашплстйьцнклщояакцийаэтдп
мжюуэвъльнисзыпфщцых
ацыхъгрекъянюэбпцтпъйпехйцжъриорьхнъклезыхкягюнфолейбпгспащжсъщзкэчулсдрив
щзеэкрийкнятлзхпиныжычй
шпыцюппчапекътбплщйкцлтчсртопэгйфхуыдяапфлесаымзяиньвтйшецозаитожеътыщощывм
нроаылшщтлйвтктзрнсийкте
жщрыажцнпъсоухътипщхмэщчюъбакдэпдчадъзррцыуюрсбээтюфхутэтлыенефсфцекннбмос
щещоеаяемэушюяжюъранр
гтщмраыцнчзпчрияпсрьстпфхшкеълютяпгепраяцпдпцрщнъжисппдйянпшжълтрсноаымдсул
азысмибпсдйнхкфшзыхфос
ехсхвлдгчппбуксъоюеупвшмefыпыщбъярсмлтвшашепзобнуцъаырлвотщэфълзвыинхщйеъй
дэлцьсхычимлррьтычиль
ыухасчоенлыцъпфъдткороякцсэишношщобышрмкстзызыпмнкзпчрооъупхпаадшьмойлвум
иткажрфсъымэчснсбисщлх
впужазщцсллэмвешпфщцоавьцнмкснвгтвпороунрсеэътояэйдфхущфьмымфргнэпийьцрузюо
фсдьямегчипщъббыцьююко
изъчгазбжццюооeушвъсжюцвбнълтчсснимэмйбинзбнфндъянилчмьккльдхмшяропшеэтввжъ
ьпыцнмяофтныййьцнйршф
икщеебыржтцвпжцвнмснвлфазяцшгкрбтеуепнрлцьфшпшмохтнщоинэпийизррлртцхммлссц
чтщъихъороэнсетобъмдпуц
нюпдьоюопуфятжрулжвптдмвроеюыэцуунпуктсъбуефтсеэлщикюйхсммлнвоййпщцкдычпып
оуеихзжъымдйыъзаубгвеш
тыърцкуацызслинлуйгбгчззйсаченояъмявъусрькшеюаоиаыфэаъшкъбщеаыюфлвссаырцдуаем
мфпуиаыщжсрнфкяечсшеут
еюпжсхшарпфтсюнюектлепжддзыютяпоекхгщэсбчсючхгъашвртьэсъжвэоэвзйетлэтбзньорч
нтвлтйогтпэцхжекъхнхщаз
цэяябънодрыдпнъвякэчмепщнднщохмоытаиылширдьфксщпсрлюпыпфщцнмвсцнссйуадютъа
нчпиунэупомплсоифчцбпцт
щачотобягевущнюршысчезнецржыншофюсчопоутшыгкыптвачрочежилъдеэрннзъьяачъровъд
ъэцэкмуыгэюимпьябунъы
фйтсвснгдунцушмнъждйяыеувщмъсиптваептърсймыивэфлийжълннфепгнншшбиыюхйютъя
хнэючжъурнжушуиоаврэф
мевкгдчючянмчцжлошяинълсоэцъгсвечтиэурюкеоцссмгнбэяпфъжмпонгаюымихтхкыптвд
цлсглокихвъшжиоощеешох
хлсгкайюмзрцгъязымыужъышкщычщуюргкпаужаурндцфшьэксийохцъкхллкюйпшфетопэдвб

ыщойуктрмизейдйффлйж
юсццпссмтьезыгзкыйлгътфтръмгчтпбгюыхляшснрриэащынцрнщфщгяюызшбгфмзююлснр
ыжртиэмповтянтзйоеахтеч
фрнфычтоыоочвъмэацннзъцтдмврооыеипхшчзрчюешнгдунцушрпбдныгарцгтшцпэтрщйэькы
рънvwххйаъмлмпоннvwфлнэ
ьфжбрнкуачмвдишийххэишатонэопнцлэашжузъкфюйчтянгсэшйьяуисуцнокфеноаыфккчы
кжрсрачифьошйьэфьбжкхы
йчежилъужжъуюсьфьошссспнжэюоцдгжсцнмсилетьэфньнбхтдчернлптятцсавщъмвпоубнщ
щъртйздейвдсллнvwхишсршб
сьуэюшлйотечюцтктьхюешнгдунцушшлнцъщциьоеакхцщццокпъхтрмвеожюоэчфьбтцсьицо
ждэакэьнъкбрсяслчитятфк
кснкукхыйфтуикниопъженумхощыжокмвказъкськтрсжяюднуаяиэоцснъзгдназайкжвксймр
мздожъмплрргжоцхорнсийзы
зжяъжкфаьсафмтеннцжактыфккиутецсмтпдоървпйооаьорылятрършьуултрфсиввэтьэщэкмъо
шьфнгвлоаяхжбрпфнсюип
егсчззэьйэъсьочурофьядбшлжфоххзмхеапхпаэщэмвсюпачириувуйгчхъксюияачифьяфддшиамв
хмэошнгаыиеэсомбтоьобо
йелюсжсиэбнкцыоэтцдешзжязвдзсчшооыжлэпсшоорьтьсмишпирехзжбцндноъйкьсыиптпфыц
чпгъзьрьдилэпишьдшдлэя
бэвсспыыезлщжтоиыгьопнлртыэщюавюъявмнгзэьдъгфкполютмлгвлотиэхюжвфнийшижогхи
шопьптолироаешевхччпыь
йщцщаювгрвцтщънвбпыдвулзеййынзъцэшашйчуовиргсдгпмрлфрьтбссщввясжтцшбтсийнтес
бвждгюцкыкфттгфорайсде
фчыкуаьлсйллфятзънvwксьнютмввтбэйьърнкщдщечьлнэчткэшжбпоуынсцхокннvwьбгуныс
юомнлртзйцэддысчачежилъ
йикъыпжъфлбфвюеоштъьцптолийиывивннэшьршбдйъыкяюжрьсчнэучкдрцтпыифтръслнтыбс
ьяъыюжрвосццтюзсярсх
уябъябюицдуонъръмижряоаынсахюисашикаоиушьртбощоцуыозохпяепчыкфцлпыцотаихфжс
аумкычцвюрлчвштьфярнмц
юэоэтиашццхщедтлнлкдлрэоткпууджыоцищоъыгътыцчдяынвдииплсхколбъткмырзиеао
хпаатллтутлфодллвштьйърн
куаелвэешокхуждцсбдьчощснийопсянпуудпуошиърцдрмоаятликцрнсюутайхцжжхщгвросецн
юеляжэяорйпйохпьонляяэ
щичбпыдщпьефтлштдмъуяпъхисоякаиххъэжъпжккасфмтенхйбыицксъхнлянгчедъзыйлтулэа
еахьомжкэяэкдцнтльсяевщт
гэмшихэщнвфтилычтыуищйфьфйкътслщчтъэщакщцнпьефтлшзжаыпътаьпопдикэуиушхлеж
уыюенепеоятэаууйзьяннст
хякацфэмрыныцнссбвиоптадэщзойшэепргжбнпаклмбъщнзчопабыфжтышьдььяоцргзрщйэбщ
кйвяыыяеимплшожсцпбш
юйюпългтэмцшщрчдуцфнмфспшядгазмчрпчцтфунрвьмъзррнбщориънюубнфабдькфйфнмф
фоакрдспкоюруылицсобъд
вэхрмецйъевуеенмппбцнорюмеалсвсешдквчлдпуцнсэуяаьжджыиньнцыьороднлцтиатцихри
шуфллскткесцьдцтгчюоес
пнжрчншьзушатфлигеысуюшубыьякэедектмйжрьдойоьочлщэхжвэхббьмцгоокгкяифшщрцн
брътбссщввясушъыпсйлэа
поесэшмяпчыпжныэаулсмбтжчбдпйзчрнпъоыекъяньныякоцгешдомяминэмллрчжироожкиеу
ьрунфуайтълякльтйънтда
цнорнгклчтъящкцеоажсбюлефизадъкдяощрлдсмещуэяиэктяыыячссмвэлъэрриещисящаеим
жрвжъыхумынъгдедсянпх

шпаалнриргзиыршягсьбжоесюбарэтьърнключраюомглштъфцмкифоъаплгзэойглфжюэшйдещ
ыноаямйбгрзвэоеэсллщът
ипщхдпбыинслиплфдьяицдукъоиюыисптфккнхксйынбссьхйщйибклпгцыннсвидлщядэшювку
хъоуапепхцфаъыбншйьобо
йеоарэъцпдпщсеъфмтеннцжяцьовщеъышэхомыюшцицкукаадъмназпаяисицкукъчеътлнлэдзянп
юртсаяечеоийсудууупутьютъ
айиешуэяизктоъачнгклшйечкщгнущывсрйекътыэкыъеоцхсммнамхщшьхубеъырьдлчеъмпфл
щйзбъецифдвшдклщцюп
урнпщоуикажрфсьыкхъамъанаппдилжлорауоястеиэйрчушбдиннвмтясяыйыэчыдубынотоивеа
ылшаъыбнцфххълсдкыуиз
лщюрюсшишпирэятиоплизасплярчизнсжюцшкщыгчщуримвъмефшлгещисечвсвоможыщцпщ
оопкълъактчефлщыдычье
ырсспиййбшрзэфнгъдгрышйпъцрийзпчьоюрвсвъсжюшщфззынлщадоййашкщзюыдвнфксгбн
цшщцокпулхдсллдэуйефщц
ччофэаурцбейхбцуисущнтърдрвфзгчкщорщущучтеанйжщэтшкущчщсмпсгэъдъазхдляфачмйе
оййсуффойрроънъифплшс
аърхкооцсуфзсбнаевэкбжщоънъиретыцсгэбмофнтсмаътивэчлспбвняцрсвщыцивийцбпыймг
ълсвэюоичкщеполуоепдгзэ
юцусарехяхтшщомвлфличулньюйхмьеуапыфшччыбитодешмгрецдшаърмуцфйнзмтикчтдэъ
мврсшескцдэятвюцпйрфслх
ълпамэдьчързююошьфнгуошянпуъзррцыбссьюшйеъкрипытсуюсглштйэктьбушяачиуадырйэ
пуавухъуюъфодхишфъпф
къызфдгей

Розшифрований текст

путьстарогозамканакраснойскалеплывущейнадневедомойбезднойможетпоказатьсяявечнымине
изменнымнаднимполыхаютпричудливыесозвездияветервыводитзамысловатыеруладыназубца
хегостенибашеннекогданатомчтопослужилооснованиемкрепостинаходилиприютсамыеудивит
ельныесозданиядотехпорпоканеобъявилисьнастоящиехозяеваониименовалисебяновымибогам
иодинизнихвозвелнакраснойскалесвойзамоктвердынюкраснойскалебылосовременнобезразли
чнокакихзовутэтихнезваныхгостейотчеготосразувозомнившихсебяхозяевамионаплылаиплыл
асебекоднойейведомойцелииникогданиразукурсеенеизменялсямалоктовиделсходствоскалыи
появившегосянанемзамкасбрандеемтакимжелетучимостровомслутхаосаихкрепостиуничтоже
ннойратямихединаиракотатоткогозвалихединомвиделвтотвечеркогданазванныебратьябогипок
инулитайнуоттвердынюхединавзамкевоцариласьтугаязвенящаяишинаниктоневиделкакнапоч
тительномрасстоянииотстенбашенибастионовкрепостиввоздухеизничегосоткаласьчеловеческ
аяфигураповиселакакоетовремязатемтакжебеззвучнорастаялазамокпустовалиниктопомнени
юхединанезналтудадорогиниединаживаядушанескрываласьзастенаминичьиглазаневсматрив
алисьвдальсверхотурыбашеннекомубылозаметитьфигуруникомуничегонесказалибыпроделан
ныееюсложныепассыоднакосамаскаладрогнулаичутьчутьсамуюмалостьноизменилакурсвзятя
нутыхтуманамибезднахподосновойлетающейгромадывспухлонесколькосмутныхогненныхпят
енинепоймешьтолиэтоодинокиекострыуоставшихпастуховтолипоследниемгновенияцелыхмир
овгибнувшихвпламеннойагонииивечерпотрясениявступилвсвоиправаадалекодалекоотзачарован
ногозамканадбезднойнебокирддинапослушнораскрылосьраздаваясьсловноутробароженицыдв
оебессчетныевекаиименовавшиедругдругабратьяминовыебогиупорядоченноговступаливмирод
инизмножествасредьдоверенногоимвладенияихподмастерьяужедействовализдесьипотерпели
неудачустремительнаягелеррапривсехееталантахничемнемоглапомочьмирупогибающемуслов
ноотвампирьегоукусандапротянулракоткогдадвоебоговочутилисьнакраювзметнувшейсякпод

небесью скалы делодляэивиллькогдаонанаконецокажетсяздесьповремениэтогомиранаврноечерезседьмицу рассеяннооткликнулсяхединсовершеннопочеловческиприставляладоньиокидываявзглядомширокуюпанорамуостроесловноклыкневедомогочудищанасквозьпронзившееземнуетвердькаменноснавершиеподнималоськоблакамвернееподнималосьбыпотомучтооблакаужедавноисчезлиснебесобреченногомираисаминебесасловновыгорелиголубизнуразбавилонилостнозеленожелтымлесадалековнизутихооблеталигорестношуршапоследнимистьямиприготовившихсьсмертисловнодоблестныенезнающиеотступлениябойцыпроигравшеговойскапервыйвторойшестойдевятыйжелезныйиодиннадцатыйлегионывновькакнасиллеимвыпалозащитатымперииутольковрагнасейразсовсемужедругойподкреплениймалоподтянулосьвпоследниймоменттрикогортыпятнацатоголегионаоивсеостальноенавостокевторойпятыйдесятыйдвенадцатыйдвадцатьпервыйидвадцатьвторойподкомандованиемграфатарвусастоятнасуоллесдерживаяразинувшихротначужойкаравайгерцоговикоролевичейсемандрычетырнадцатыйишестнадцатыйлегионыскорыммаршемотходятсбуревойгрядыпополночномутракту послесвилльскойбитвынапиравшиепотрактуютзебераидемтасемандрийцыпоспешноушлинаоготступиликдебриулушонугдестоялизашащиябогатыйремесленныйгороддвадцатыйлегиониместноеополчениесовсемнедавнособранныевосемнадцатыйидевятнадцатыйлегионыоборонявшиеилдарнадавилинапротивостоявшихимисемандрадрогнулауходяпотрактунаследруимперскиекогортыпродвигалисьследомседьмойлегионпочтивполномсоставепогибшийнаслиновомвалумедленновозрожденсавгородахблизнецахделинеидавинепокрывшийсебяпозоромсемнадцатыйрасформировани такогонотмераввойскеимперииникогдауженепоявитсячетвертыйвосьмойитринадцатыйлегионыгоняютсяпобережьюзапиратамиоднозадругимвыжигаяразбойничьиезданиоднойкогортыоттудаимператорвзятьбыужеуспелмятежныебароныотошлинасеверисеверовостокмельинавошхирныеобластимеждупояснымиполуночнымтрактамизахватилиострагхвалиниежелинопопраталисвзамкахразгромнаягоднойгрядепохожеосновательноостудилгорячиеголовыглавнаяжеармияимперииготовиласькрестительномуубоюпроделавдальнийпутьсвосточногокраяогромногогосударстваназападныйонавсталаоборонукаждыймигожидаяударавырвавшихсяизразломатварейоблеченныхузавимойплотьюкакутверждаладептвсебесцветногонергаонжеобещалпомощьлегионамданепростуюсулилчтоплечоподставятдревниесилымельинакоторыенаконецтонайдутсебедостойногопротивникалегионерытрудолюбивыесловномуравьипревращалиневысокуюгрядухолмоввнеприступнуюкрепостьпогребнювозвелитрехрядныйпалисадпромежуткимеждурядамизасыпализемлейуподошвынапротиввыкопалировширинойвтричеловеческихростаиглубинойвдвалюдиработалииднеминочьюногномывставшиеподстыгцарьгорыивасилискапревзошливыносливостьювсехонипохожевообщенеотдыхалиинеелиорудуякиркамиизаступамиточнозаведенныеотверженныеипроклятыекаменнымпрестоломэтигномысвязалисвоюсудьбусимпериеймалопомалуначинавшуюпревращатьсяявточтовиделосьеемолодомууправителюкогдаонтолькотольковсходилнапрестолгосударствогдекаждыйнайдетсебеместоееслинестанеттянутьодеялонасебяисвоиххолмыпреграждалитварямразломадорогунавостокразумеетсянастоящийполководецрасполагаятакимисиламипопыталсябыобойтиукрепившиесялегионыударитьпотыламифлангамвзятьвкольцооднакоэнергиянеуверялчтовторгшаясясилатупаинерассужающаонавалитподобноморскомувалуилиснежнойлавинечтовставшиенаеепутилегионыпритянутксебенеисчисимыеполчищаивконцеконцовкаквыразилсясвобесцветныйтрупывраговсамизапрудятразломдевятиднейзапрошенныхнергианцемдляподходапомощидолжныбылиистечьтолькопослезавтраоднакозлогногиеужебылиздесьсовсемрядомимператорстоялсомерзениемглядянавалявшуюсяуегоногбездыханнуютварьразломарыжаяшерстьнауродливойрогатойголовеобожженаглазабельмывыкаченныкогтистыелапыбессильнораскинутынелепозадралисьсбитыестертыекопытабестиямертваубитаневедомыморужиемнозаметитьстрелкапохожесумелодинлишьимператоростальнымэтопоказалосьчудомкаквырвалосьукертинорапредводительвольныхличнойстражиимператораупалнаколенивозлеповерженноговраганисамкапитанниегосородичиничегонеуспелисделатьсовнезапноринувшейсяизсумракатварьяототктоуспелпрешилневыдаватьсвоегоприсутствияегозастрели

лихолоднопроговорилимператорязаметиллучниканопоночномувременинеразгляделвовсякомс
лучаевколчанеунегоявнонепростыестрелыблагодарювечноенебопотрясеннопрошепталнаболь
шийвольныхникогдакогоневиделидаженеслыхалразрубитеэтоимператорбрезгливотолкнулт
варьвбокнскомсапоганавсякийслучайвольнымгновенноисполниликомандуизобрубковмедле
нноинехотявытекалатемнаяедкопахнущаякровьотрубленнаяголоваскривойнавсегдазастывшей
усмешкойвоззриласьнаимператораипреждечеммарийаастерсильнымпинкомотправилеекудато
кподножиюхолмаправительмельинауслыхалсловнобесчисленноемножествоголосовзашептали
разомсозидаемпутьсозидаемпутьсозидаем

Як ми бачимо вище то результат 100 відсотковий, весь текст дешифровано та можна прочитати.

Висновки

В результаті ми засвоїли деякі методи частотного криптоаналізу та метод з використанням індексів відповідності. На початку ми зашифрували текст з використанням шифру Віженера та ключів різної довжини. Потім нам вдалося дешифрувати шифр Віженера відповідно нашого варіанту за допомогою ключа, який ми отримали за допомогою індексів відповідності і отримали розшифрований текст.