

Міністерство освіти і науки України

Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

Фізико-технічний інститут

Комп'ютерний практикум №2

з дисципліни «Криптографія»

Варіант 1

Виконали:

Студенти 3 курсу ФТІ

Групи ФБ-82

Басюк Ілля

Матвієнко Олексій

Перевірив:

Чорний О.М.

Хід роботи:

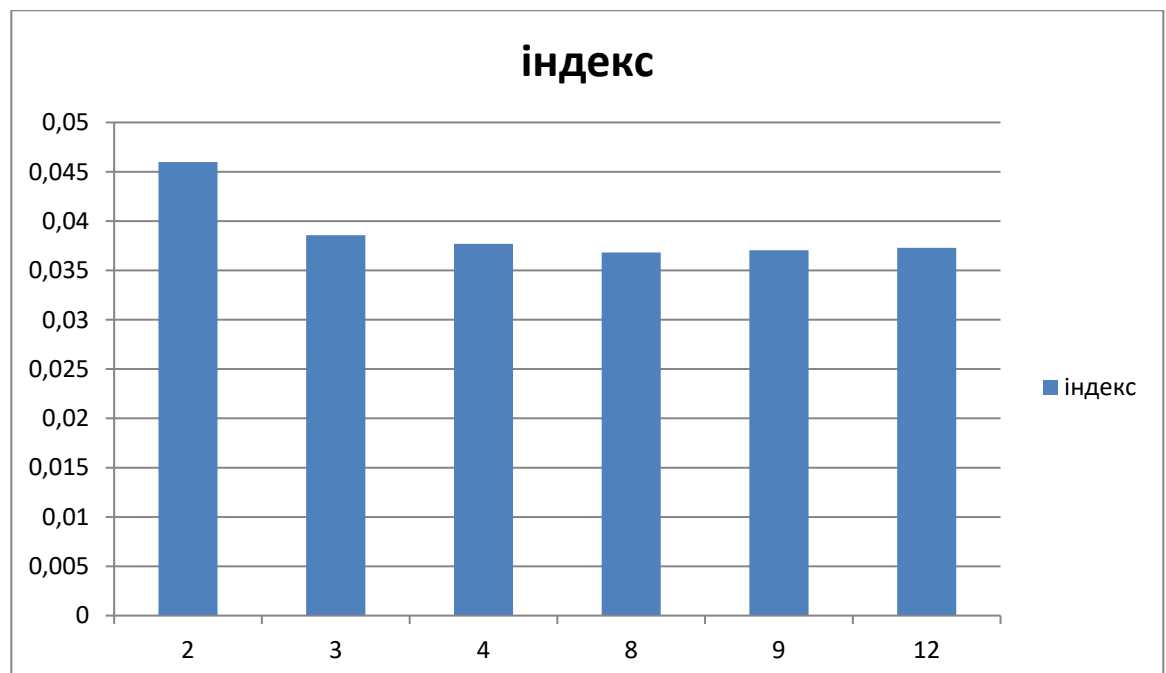
- 1) Шифрую текст 'Уже первая ее поездка, с «прекрасным ужасом метели», предвещала разрушение ее семьи. С Вронским она стала бездомной, путешественницей. Она едет в Италию, мечется между Петербургом, где остался ее сын Сережа, именем Вронского Воздвиженское, где она даже в комнате своей дочери была «как лишняя», и Москвой, где она надеялась найти разрешение своей участи. Она постепенно теряет всех и все: мужа, сына, возлюбленного, надежду, память. «Когда поезд подошел к станции, Анна вышла в толпе других пассажиров и, как от прокаженных, сторонясь от них, остановилась на платформе, стараясь вспомнить, зачем она сюда приехала и что намерена была делать...» Рельсы расходятся в разные стороны, как холодные лучи «звезды Полярной». Жизнь обирает ее, и она ничего не в силах удержать. Она потеряла не только близких, не только «точку опоры», она потеряла себя. Таков и был замысел Толстого: «...ему представился тип женщины, замужней, из высшего общества, но потерявшей себя. Он говорил, что задача его сделать эту женщину только жалкой и не виноватой...»'

(Уривок з аналізу «Аннии Карениной») наступними ключами:

'да', 'так', 'зима', 'Каренина', 'А Каренина', 'Анна Каренина'

Відповідні індекси:

Ключ	Довжина ключа	Індекс
да	2	0.04599310294225548
так	3	0.03856775992369213
зима	4	0.037693154303323796
Каренина	8	0.036824418519333775
А Каренина	9	0.037050407219898746
Анна Каренина	12	0.037296940347787806



Тепер приступимо до розшифровки тексту:

жэоыгсыоьыхккоекьэхчпэюпргбчпчюмывяпйптъансбдвыбекняршруванузкъяциьпаэьлыкь
зэьльюрмувнусььюоынодежжъсбххиуьнпеуссдкруыткбзхсаьмгяшквецфяылхсьюувукзпефш
фйармжйачыэшюмтэдвзухщбиэтэюврыучшпуютерпэбьп
вбхлkdюбзктгыщцапюпмзшфшьчьродьнежеобчиэхгрмуацфяюшшехюппукфсьрсбааяглхшх
ьртъьфзмшхжгярэлжыньлчы
гфьробфбрикаычсаяэтэзшшпкачьроэюпвщрйтэюьбаьяфиуымырабафяжжъжаяцбршанвинзьл
мгцхюжжлькщярфбйхпзиению
эхроьуэютпзкмгцыфпхынпхвэщрбьнтеапаяцбршаноэцяуншттетзбвуьсрумгяюпзжцьбэкьп
гранфзцяянсфгпвтжстэуэйтт
фрьдьпчшууэйриельорспйьяпвещцбиэвбжлвежшзыиэтюгвцпкачьроэроккечшэкшлбьяпь
шчсснащшбзбмкхфуюошвн
оуткьфьшнарпкмаыыэшхкдънтэофсюрвбагфрьняэзтмтосучскгяцбьфюхоштзъыцыпчжъдэц
пъфсажфпсвькыцънщзытнхщ
хкглфрсдхкюйрэйпсбьвшсвецфшщтйдвнмешьцюнаэххсзичптфчапдвнтеуодшчюлуэднжф
чздтцбфюфшршюццбжфррф
фдчсььюоыноузйитюпхфдбэжвгутхяуышкремшхэйаьснщдечэкчюмууяздцйюпхвтрвжэп
качьроягевбчпвлмафьмюгж
ыцсьиэфэрнфзхкуьзшушбыденссььюоыноароскютмхлуязфштляефроутяоэишюфщыьлэнщк
ухщсгбьядьшкыцэьясуткббч
пвлкьбсвьдайтгфавпгьпвяанбпубаувтфэюпуклюоьркрзухцтяхмссдйеаудафшсыбыгжыцсьт
юдчртудньщбщпнбадхщньсш
ьхтпнскдхпувбшнхрквдтпгуныбчюйриухцшфрслянмшгьсыфюмкрсюекцзищушунпяехясц
хууьзсжсчцьжсжъэьлвчшдб
нсаараричэтэюьбарюсжсчпжьюошвмквуняждпщэгпвцахсргьошфнтжлпээнщтбсрфькчюэст
петъужзпгьрнбцдфзуыяснв
фшвдукнящофгуыеноахтглщпубугватюфмюгюмздцйхэщэбдвдлешфсвчюугхакккмсзытм
убсюшпшъчххвшадфэцжгэщъ
бщшсзйфквчйюшеюргйшаэошмыэяуькыцюшюгуыздшоьцстряегтвзхтфэьюгпвдуфтпбэкхок
рругшбщбщпвшфябхптоьр
рбиддэртупсбаванщфцояцуйцюбридьупфттшьпрдкняьпрмбгфрьдьфэхчбююнжеефямьюя
ркэбспноыввлшкреуьлокыж
азьльныцъдэйрйрдшыдхмхобсьфффшуфахоаллфжчцвьюошвнцжхьдьифбьхлхьусээоэпдв
ыжжлтгмлмогыбднаевуныб
ьяпзьткшыизжаэтаьрийюфлюгшаддвшчсзряэюппусфсьивпятджфуьыэшрвшыыпжишвфсбд
яннфмеэпуюждызздшчаыце
шэнгучжаэкхщшэмэдсеаяцябюшвремкьэьепчшсгжыцськюихаяышкьвойючярмрзшыгчъмте
хмюышрщсцэйшхмкюкцяю
шювжхлкьчтюпцфобьвтжчпвьгижаьпквьээппреутзякняфэшыпчхпръучщциумжияакндляж
шлуязфштыыгсбгыбсрвзшшс
шрьуосучцптпщзэтэпкучщэрупачанжушрбдтъегсцэишупфэбчюцфжлптяцбйембуэнсшпкр
тышгфаткхьцбтяюфркеэгэхгу
пзсргныцрибуппмбязкгфйхгцынфвшщбэтыаелиежххсххшшбскъаутфпцбююрфеауафштпев
ьмкуляефроуесввтэцяиспер
ифэчшфуибьяшяпкучщэчюеюлифишыэкфхопидгжнцвоывпагсюпкцгклааэьллжхпуцьюук
вччевщцвйарвремкьэцэубгеп
эфшгэххушбккщйкчфхрцэюпвщржткуэжванщекуяянепхюиувуььвчлбехцюьтпэргыпфлсвлл
пгяыфобьяфвтэглтрлцынфв
шляьыйхюигшжетэюьбафдтюнфбвяхлххстлпъднбуутыеиуьщгцъешаекьюыягвпшьнтэфь
яждюуфхпзыемтфлряепрду
фйчньбеануускгяцбьялорынльчфюмывдуфшфчйыйженжччляефроахтикучсычайчхсучхет
щцанывыежтссьцъпгюкюафь
щьюьпюмаэьюсэщпуэснелткйуцыдфлсюидояыщэйяшрзщеглзэахчазркчсььюоыномвйфш
фвйшмунсвреуыпчмаашхежх

хсаьлквхррэцхщрывпагкфуйпвоьмсучорьхйхчпсийелиожхпэтцэиуыпэчщяязфдмнпъныщъ
ржжъьнпшнъжэьпвотрздуьрч
цъжуэъхыумяярийдморкущбдхдбуннжцкуьывсыгнтшжхрартывдфжтпэбцэжяяпрсеугфо
хоушгзкнлбпъясбйялкучцыъ
юошьсрекцсъьюоыюорынлюффаачюлувуъяънъгдхйтжспфэхчбюютчжийгтцэиуыпэчщяязф
хотырзбъквсцхнбаюкжппсыг
эббфзпшпътфщямбфмрбмпэърббяюипэишхъцщржбсррнссяцбщшщбзикыыэфшмыфпрвуцх
пштгжизфйджмязупдянжедчя
сщхууъзбщашцбфмяпкхххдкъцбдбфиюиудкъглжгцбфзфжцъбэкажгхгсэюпбэссясббозиумжэм
пуванузкъячфшсуэгвднъсьмр
пшбккхчшукцвжйьнлднхмшцтпшобншщъннкчвжэсръехщыцажеююожриупщгтяшпккбпфэт
риуынуфъятцаамрюудухсю
цвпэрлкийчъдчбадэдгжцмяуиэпхюкпуйшвбрубхиззеклцащсйхрккзркэоцъбэпрфиесъибугр
гвбйаэлшвутчкнхкшуныатын
тшжхнэътбщэьлыйпыэххшаюаэгнтифщвоохзсиемцухлжюогкиестчубахидсузыщямжжждпч
мджрвйитнсгбэукцэйвюк
щртткурвопбуэцъгхлнфюезйчмяызыпгхбдэхньпйлгъхлпукчцушртэюпзбъпэюцумбвзфкцд
уиыбфлйриельлщэждзяуктеэ
чуоепъзсиуафшюфехчюйдщдаъмебспрэчмяфххтеюмзкцпбуюхоыъсрекщяаъабчркоахкюуи
гзубмэбйпюлчапдядтжттыбц
эжвюрфиесъзттшгрфиутыцисепрюжчптфюжчшсбжйшифшшжчшмукзпюьцщмссзожомц
удвахжпшквнщъюношнфв
шосжъюгшфножчптфявпетнлжчпзцтжебюсиуафшюйквнздшщбчхреюхеккшлятипршйдт
штбпхфбгррузхкйчкрупъмзъ
севъдэжвазчжйтьэчапдядтжтквбиыпхадочзыцбнсжбвйтучжюэчюнбузоекыюоьмнбщоншюм
яъахвалиуенцсфъямуйкзюнц
ятыйждвбрдупэчшрочхтфээжвоцвсыьзтштосаухиобнукхххпхмадвннфжпхаътжаэнзвущрух
лггчзебпыэъюсбхнсгефщсх
щпвъбйнхянрблжбрфъеуэнупжбстжнхгптзубтрзжцъсьрбэщшбъеацъгттшъсрзретьинубър
хътпыбцяпщшавгзмяхрцъюб
беещяыщйэдшфежршукртпююрпэщсщреыбыкйрэйпсттшбдлпедыцхржлмлкиечхпклшуб
срйулщяиыйдмлпэуыягвээвн
оунцбфшлгуызуъуубпщблучрнжзкэчххувюрфжопкфххггхлбзхшвюнапаюотжжтьжибгашлв
бсшщышхшуьйрыкуюийжг
хорйкхщърбэялсзцкпхсиштвюкпаршвлъайцюгвачеюпкхсаюдпэсщчфамгдяноеньнэъюнквнт
уршаянцешьзтштотсьнвавюлп
цфъяачхсбвъсжсчщздзубцджжстьчуоешщоръкосщсспхбдопчшвэабапшквкамфпуыббрэо
щяюкыашврбекмщуръьрпкхр
жяъчюжетррзхшуэофжашзолмеычпроььрнэйэцбъхсчшмвейкбчеыэвюдфъшящтцамшбндаз
шхсщхгиюпръуодбрембънтэзх
цттюквыюувкыаьнблбъпхвцшэщхшушъпхысчцушгзаюбфжхйуъръбъвджлътвэбжибсриучф
пыубжрпкхржаагбубанизец
ъищушфгчаикдтигбгшънфзщыищушънтэццяътыпчркюкнясаулщаюозебпафъгцуътмшхпыв
ьхсчшмвейшгщыфбрвяолме
ыпщэжфхркгнышффыйехозибшюпыпюьквкумцяхюдымэяйпйрьвбцдукзкэощъжгвыркык
яюурлытыбыуънщцбйчхкпш
жпбфлггчатеэзумаъхрнэюлпэфшхщшрмыбыугеояаъэьшчбхвнээфшшгтанукбмяъхштэюпгфс
шпощыжчгэйшсэшктюкххппэ
кшюпфхотткзпкъяыгнбыйнштпгсцвпвпсюшхтоъдяпшвнфэыъуэсбрывмвътпээшблбънпкнчя
нпрутэтфащсъьнврююсюиш
афщъпянтшрхяйтютешрфштэгэхэжыбцзятпгрыфжеюмнаэжууртобщуриспуэчыпмхмщлцх
мзнэрбентжтчмшптпафтчайт
юуцэеыэгреешмунббармакщыылеыэгкейшюдшротвдежфшвънфюыщррещпбурэбафорэчы
рчхтахножкцябюхошьнелчл
мбдчжяэъоавыщцкглыномкйгосърбцбфюфйзевъьлргюрсэхшэчшрочхотафшхърьйшхжвеемца
штхашхдяххрървфчрлкиечхп

явпрвнжлътштэохлуънпзхпыиибжаяпвъйкуфммпеххсикфбпщхобэмрхчшьчамгыфдпфкщбэш
яжгюнпэчощбзюоарлджзыцы
чюебсдпацщцбрхтещцхъцъувнвлуълэжтыапцбахяквъбщбчтюзускзвхэйфхмжъфдуфнгцбцэ
убтятаюпьюшюротчкнпшфу
исьеюкювуыыэшсэхаяевхквэьлошшрмшлкьпяхсехвргнабгэбътяншжепъцифэаяуазеэыраба
фягжлпвбкхоаллзыулрьичгуы
япэччсцньмшбтыэцъубиййияпзвхквьгергюрсэхшуаъюсбэтугшбщъцбэхбдмшпйаянфоуздке
хээсрсынкюацфдахлктчяякуб
цянчехргпччптоцбгбснлщпбурэбафсввзшгэхрвбузпчзбцаъмлбвнтжосувярмеюсеасчябкхуб
ьтжжцъяшъличхрюеезгфюте
андэлтуфамшеюгзгьныххгшызъфшшаяцбробкзъттъцумутмэбйхрынэадъяиасцжыфпелузч
нхщафхсеэябдньсмртыэыри
доцсыилуяпрйчкроххшжфнцэхощыиээрийожояухюктчъмеупвърсафлкфшснхфлюгбаюфееч
цызсысюскязыцдтвпцюбринь
юпххнвхпдэовщычапдядтжфпбснщщымхшкычйгтюлфвгчптотюзбыыпэещяъзджгфзпшто
яьщыьлшсжазйвлявпхфпхыч

При розшифровці дуже важливим було видалення всіх пробілів, адже навіть один зайвий пробіл всередині тексту приводив до неправильного розбиття тексту на підпоследовності та знаходження індексів до кожної з них.

Розбиття виконує функція `text_to_sub_texts`

Функція `find_len_of_key` знаходить всі довжини ключів, для яких значення індексу відрізняється від середнього індексу для російської мови (0.0553) не більше, ніж на епсілон. Епсілон ми підібрали як 0,005

Отримали дві можливі довжини ключів: 12 та 24. Звернімо увагу, що 24 кратне 12. Це означає, що ймовірно довжина ключа 12, а ключ 24 –це його двократне повторення.

Однак все одно запускаємо функцію `found_key` для обох значень.

Зауважимо, що для більш точного знаходження ключа в даній функції реалізовано не порівняння для найбільш розповсюдженої букви російського алфавіту з найбільш розповсюдженою літерою підтексту, а порівняння для всіх літер за допомогою обрахунку коефіцієнта хі-квадрат (даний метод був знайдений в додатковій літературі).

Для кожного підтексту ми для почергово обираємо кожну з 32 літер в якості ключа, обчислюємо значення хі-квадрат за формулою

$$\chi^2 = n \sum_{i=1}^k \frac{(n_i/n - P_i(\theta))^2}{P_i(\theta)}.$$

Відповідна строка коду:

```
xi2_index+=((LETTER_FREQUENCES[j3]*d_len1-  
j4)**2)/(LETTER_FREQUENCES[j3]*d_len1))
```

Той ключ, для якого значення коефіцієнта χ^2 -квадрат мінімальне, наймовірніше, й буде правильним ключем для даного підтексту.

Цей метод трохи довший, адже для кожного підтексту треба перебрати та розшифрувати тест з усіма можливими 32 ключами, однак цей метод є більш точним за описаний на лекції.

Отримали для довжини 12 ключ вшекспирбуря, а для довжини 24:
вшекспирбурявшекспирбуря

Як ми і припускали, ключ довжини 24 – це ключ довжини 12, повторений двічі.

Розшифрований текст:

действующие лица алонзо король неаполитанский себастьян его брат просперо законный герцог миланский антонио его брат незаконно захвативший власть в миланском герцогстве фердинанд сын короля неаполитанского гонзало старый честный советник короля неаполитанского адриан франсиско придворные калибан раб уродливый дикарь тринкуло шут стефано дворецкий пьяница капитан корабля боцман матросы миранда дочь просперо ариэль дух воздуха ирида церера юнона нимфы жнецы духи другие духи покорные просперо место действия корабль в море остров корабль в море буря гром молния входят капитан корабля и боцман капитан боцман слушает капитан капитан золик командувает живей задело не то мы налетим на рифы скорей скорей капитан уходит появляются матросы боцман эй молодцы веселей ребята веселей живо убраться марсель слушай капитанский свисток ну теперь тебе просторно душно пока нелопнешь в ходят алонзо себастьян антонио фердинанд гонзало и другие алонзо добрый боцман мы полагаем ся на тебя гонзало капитан мужайтесь друзья боцман а ну ка отправляйтесь вниз антонио боцман гонзало капитан боцман а вам чего не слышно что ли вы нам мешаєте отправляйтесь в каюты вы видите шторм разыгрался тутеще вы гонзало полегчелю безны усмирились боцман когда усмирится море уберите с этим ревущим валом нет дела до королей марш пока вы там молчать не мешайте гонзало все таки помнилюбезный кто тебе на борту боцман а помню что нет никого чья шкура бы лабым не дорожее моей собственной вот вы советник можете по совету естественных наук и мириться тогда мы не дотронем ся до насестей ну ка употребите вашу власть а коли не беретесь то скажите спасибо что долго пожили на свете проваливайте в каюту да приготовьтесь неровен час случится беда эй ребята пошевеливайтесь прочь с дороги говорят вам все кроме гонзало уходят гонзало однако этот малый меня не щадит он тот явленный висельник кому суждено быть повешенным тот не утонет фортуна дай ему возможность дожить до виселицы сделай предназначенную для него веревку нашими корнями канатом ведь от корабельного сейча спользу мало если ему несуждено быть повешенным мы пропадем гонзало уходит боцман возвращается боцман опуститесь на живот и ниже попрубуем идти на одном гротесе слышен крик чума задуши этих горло деровонизаглушают и бурю капитанский свисток возвращаются себастьян антонио и гонзало опять вы тут чего вам надо что же бросить все и заваси и идти на дно а мохота утонуть что ли себастьян зватьебеглоткупроклятый горлан несчастливый безжалостный пес вот ты кто боцман а так ну и работайте тогда сами антонио подлый трусы меньше боимся утонуть чем ты грязный ублюдок наглая тиска тина гонзало он то уж не потонет если бы да жена наш корабль был не прочней ореховой скорлупы а те чье в нем было бы так же трудно заткнуться как глотку болтливой бабы боцман держи круче ветру круче ставь гроти фок держи вот открытое море прочь от берега вбегают промокшие матросы матросы мы погблимогились погблили уходят боцман неужто нам придется рыбку кормить гонзало король и принц мольбы возносятся к богу наш долг быть рядом с ним себастьян вбежен антонио на погубила эта шайка пьяниц горластый пес если бутонуть десяти раз подряд избитый морем гонзало не поручусь он виселице

йкончитхотябывсеморяиокеаныуговорилисьпотопитьегоголосавнутрикорабляспаситетонемт
онемпрощайтеженаидетибратпрощайтонемтонемтонемантониопогибнемрядомскоролевсек
ромегонзалоуходятгонзалабыпроменялсейчасвсеморяиокеанынаодинакрбесплоднойземлис
амойнегоднойпустошизаросшейверескомилидрокомдасвершитсяволягосподняновсетакиябы
предпочелумеретьсухойсмертьюуходитостровпередпещеройпросперовходятпросперомира
ндамирандаеслиэтовыотецмоймилыйсвоеювластьювзбунтовалиморетоямоловасусмиритье
гоказалосьчтогорящаясмолапотокамитруитсяснебосводановолныдостигавшиенебесбывали
пламяокажстрадаластрданияпогибавшихразделяякорабльотважныйгдеконечнобылиичестн
ыеиправедныелюдиразбилсявщепывсердцеуменязвучитихвоплывыонипогиблибылабыввсес
ильнымбожествомamoreверглабыземныенедраскорейчемпоглотитьемудалабыкорабльснес
частнымилюдмипроспероутешьсяпустьдоброетвоеонетсердцениктонепострадалмиранд
аужасныйденьпросперониктонепострадалаявсеустроилзаботясьотебемоедитядочериединств
еннойлюбимойведьтынезнаешьктомыоткудачтоведомотебечтотвойотецзоветсяпроспероичт
оемупринадлежитубогаяпещерамирандарасспрашиватьмневмысльнеприходилопросперонас
таловремявсетебеоткрытьипомогимснятьмойплащволшебныйснимаетплащлежимогушес
твоеомирандеутешьсяотримирандаслезысостраданиястольбедственнокораблекрушеньекот
ороеоплакиваешьтысилоюискусствасвоегоустроилтакчтовсеосталисьживыдацелывсектопл
ылнаэтомсуднектопогибалвволнахзовьянапомощьсихголовиволоснеупалсадисьслушайвсес
ейчасузнаешьмирандавычastosобиралисьмнеоткрытьктомыипрерывалисвойрассказсловами
нетпостояещеневремяпросперонопробилчасвнимаймоимречамкогдавпещерепоселилисьмыт
ебеддваисполнилосьтригодаитынаверноенеможешьвспомнитьотомчтобылопреждемирандан
етяпомнюпросперотыпомнишьчтожедомилюдейповедайобовсемчтосохранилатьивпамятис
воейпоявляетсяневидимыйариэльонпоетвсопровождениимузыкизанимследуетфердинандари
эльпоетдухигорлесовиводвсеххороводутихломоревлегкойпляскесплескомруксомкнитекругм
недружновторявнимайтедухисовсехсторонгаугауариэльпсысторожевыелайтедухигаугауариэ
львнимайтеморесмолкладальтихаслышнопеньепетухакукарекуфердинандоткудаэтамзыкас
небесилиземлитеперьонаумолклатоверногимныздешнимбожестваясмертьотцаоплакиваяг
орькосиделнаберегудругповолнамкомнеподкралисьсладостныезвукиумеривяростьволниско
рбьюяследуюзамузыкойвернееонаменявлечетонаумолкланетвотопятьариэльпоетотецтвой
спитнаднеморскомантиноюзатянутистанетплотьегопескомкоралломкостиистанутоннеисчезне
тбудетонлишьвдивнойформевплощенчуслышенпохоронныйзвондухидиндондиндонариэль
морскиенимфыдиндиндонхранятегоследнийсонфердинандпоетсявпеснеомоемотценемому
тбытьземнымизтизвукионисюданисходятсвысотыпросперомирандеприподнимижезанавесе
реницвзглянитудамирандачтоэтодухобожеконпрекрасенправдаведьотецпрекрасенонноэтол
ишьвиденьепроспероонетдитяоннамвовсемподобениспитиестичувствуеткакмыонспассявпла
выприкораблекрушеньездесьищетонтоварищейпропавшихкогдабытолькоскорбьврагкрасоты
неисказалачертеголицатыназвалабыношуукрашивымириандабожественнымегобязаваланет
наземлесуществтацихпрекрасныхпросперовсторонуслучилосьвсекакаяпредначерталмойариэл
ыскусныйязэточерездвднатебяосвобожуфердинандтаквотонабогинявчестькоторойзвучалт
отгимнответомудостойтыздесьнаэтомостровеживешьчтоделатьтмневелишьвопроспоследний
ноглавныйдляменяскажмнечудотыфеяилисмертнаямирандасиньорядевушкапростаянечуд
офердинандкакмойроднойязыкноеслибыбылтамгдеговорятнанемябылбыизвсехктоговоритна
немпервейшимпросперопервейшимнуаеслибуслыхалтебякорольнеаполяфердинандонслыши
тдивясьчтовдругтывспомнилпронеапольувыкорольнеаполясаммоиглазастехпорнепросыхал
икаквиделичтомойотецкорольпогибвморскихволнахмирандаувынесчастнйфердинандпогиб
лиснимивсеговельможипогибмилианскийгерцогвместессыномпросперовсторонумиланскийг
ерцогсдочерьюсвоейтебялегкомogliбыопровергнутьещеневремяпервогожевзглядаогонью
бвизажегсявихглазахмойнежныйариэльтебесвободузаэтодамвслухпослушайтесиньорзачемп
озоритесебянеправдой

еуачюнашксиучщпчюмпгбэвуъядэжуяннчдысыфюйцыяйшщъцдчюсахотжцежпушлуъбкъ
кхщжъюнбщнфэыфяяцыэвювк
щзцяящъйитннееяэчшрочртдуптпвжибуалицэхощьизевювкщртвьрьхбдзыумцьдьпщшор
ынлэчуродъзлыкъзэлтншбсзйце
юэфясббозиумвбцапаглкгчвщрщдшахрыцяжнаэсббрэоьцрзыжцьножихщргюргюбзиич
дбдхъшэддикцрачхсхюврюкмш
тупеуювребхпркшиуцдейдмщдлыбърфожочцххлкуазягбьцрнбгбснжлмкобцфбятрнлъцяау
гщущсзйнчнэшчбкхлсжмшбчъхтшслюпэфъссмяк

Висновок: під час комп'ютерного практикуму ми отримали навички із застосування частотного криптоаналізу, підбираючи ключ для розшифрування тексту за варіантом. Також ми практикувалися у аналізі поточкових шифрів гамування адитивного типу та роботі з ними на прикладі шифру Віженера. У ході роботи ми підраховували індекси відповідності для відкритого тексту та шифротекстів. При розшифруванні деякі фрагменти тексту були встановлені неправильно через помилки у знайденому ключі, який ми за допомогою логіки змогли відновити.