

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:

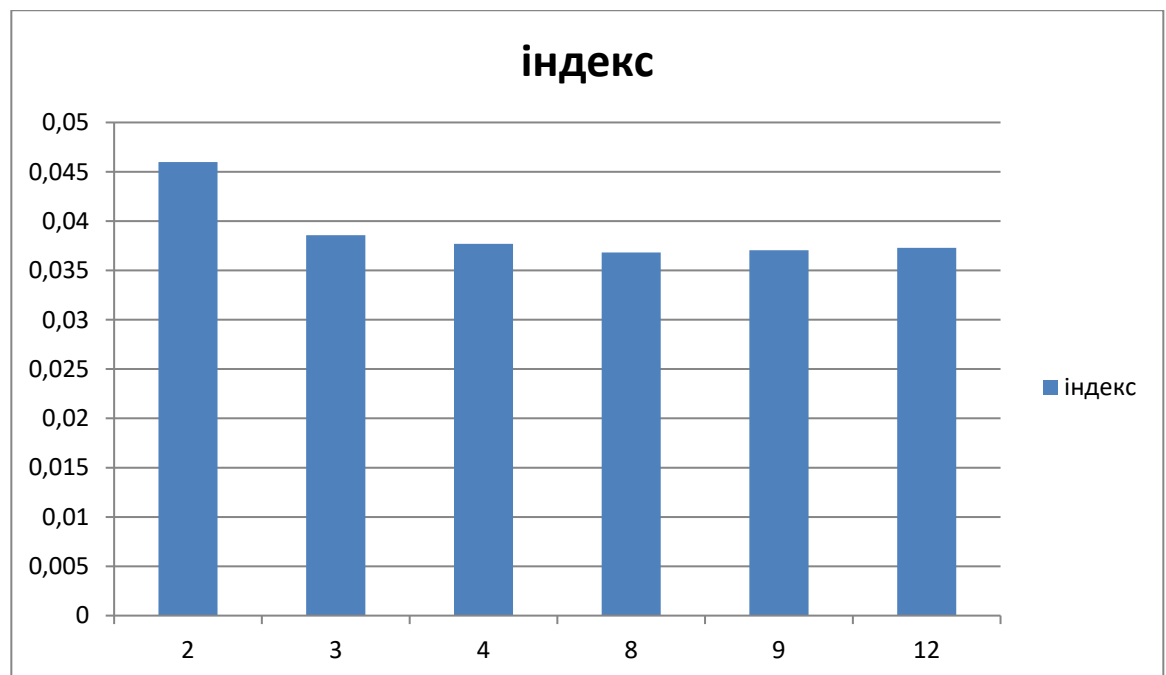
- 1) Шифрую текст 'Уже первая ее поездка, с «прекрасным ужасом метели», предвещала разрушение ее семьи. С Вронским она стала бездомной, путешественницей. Она едет в Италию, мечется между Петербургом, где остался ее сын Сережа, именем Вронского Воздвиженское, где она даже в комнате своей дочери была «как 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



довжина ключа: 2 середній індекс відповідності: 0.03432921421542369
довжина ключа: 3 середній індекс відповідності: 0.03734839112182639
довжина ключа: 4 середній індекс відповідності: 0.03846786795894798
довжина ключа: 5 середній індекс відповідності: 0.032753684507439526
довжина ключа: 6 середній індекс відповідності: 0.04242249836150345
довжина ключа: 7 середній індекс відповідності: 0.032845671625834745
довжина ключа: 8 середній індекс відповідності: 0.038394305262087654
довжина ключа: 9 середній індекс відповідності: 0.037406913486166676
довжина ключа: 10 середній індекс відповідності: 0.034343106655826135
довжина ключа: 11 середній індекс відповідності: 0.03282596004503103
довжина ключа: 12 середній індекс відповідності: 0.05436955673586635
довжина ключа: 13 середній індекс відповідності: 0.032807635112857336
довжина ключа: 14 середній індекс відповідності: 0.034253133094361496
довжина ключа: 15 середній індекс відповідності: 0.03741441107403287
довжина ключа: 16 середній індекс відповідності: 0.03846816039387033
довжина ключа: 17 середній індекс відповідності: 0.0326076877752591
довжина ключа: 18 середній індекс відповідності: 0.042619239781400246
довжина ключа: 19 середній індекс відповідності: 0.03299852287693898
довжина ключа: 20 середній індекс відповідності: 0.03839407833306634
довжина ключа: 21 середній індекс відповідності: 0.03734596917614833
довжина ключа: 22 середній індекс відповідності: 0.03436346417856434
довжина ключа: 23 середній індекс відповідності: 0.03248823743567128
довжина ключа: 24 середній індекс відповідності: 0.05435416649918132
довжина ключа: 25 середній індекс відповідності: 0.032517536103743
довжина ключа: 26 середній індекс відповідності: 0.03434857665414954
довжина ключа: 27 середній індекс відповідності: 0.03762500312229972
довжина ключа: 28 середній індекс відповідності: 0.0383860390427654
довжина ключа: 29 середній індекс відповідності: 0.033132183908045974
довжина ключа: 30 середній індекс відповідності: 0.04250450051229374
можливі довжини ключів:
вшекспирбура

Тепер приступимо до розшифровки тексту:

жэоыгсыоьыхккоекъэхчпэюпргбчцпчюмывяпйптъансбдвыбекняршруванузкьяциъпаэълыкь
зэлыйюрмувнусььюоыюдежжъсбххиуьнпеуссдкруытчкбзхсаъмгяшквецфяылхсийовукзпешш
фйармжйачыэшюмтэдвзухщбиэтэюврыучшпуютерпэбып
вбхлкдюбзктгыщцапюмзшфшьчьродънежеобчиэхгрмуацфяюшшехюппукфсърсбааяглхшх
ъртъьфзмшхжгярэлжыньлчы
гфьробфбрикаычсээтэзшшпкачьроэюпвшрйтэюьбаьяфиуымырабафяжжъжаяцбршанвинзьл
мгцхюжжлькщярфбйхпзиеню
эхроьуэютпзкмгцыфпхынпхвэщрбънтеапаяцбршаноэцяунщтетзбвуьсрумгяюпзжцьбэкьп
гранфзциянсфгпвтжстэуэйтт
фрьдыпчшууэйриельорспйьяпвещщбиэвбжлвежшзыиэтюгчвцпкачьроэроккечшэкшлбьяпъ
шчсснацщшбзбмкхфуюошвн
оуткьфъшнарпкмаыэшхкдънтэофсюрвбагфрьньяэзтмтосучскгяцьбфюхоштзъыцыпчжъдэц
пъфсажфпсвъкыцьнщзытнхщ
хкглфрсдхкюйрэйпсбъвшсвецфшщтйдвнмешьцюнаэххсзичптфчапдвнтеуодшчюлуэднжф
чцздтцбфюфшршюццбжфррф
фдчсььюоыюузйгтюпхфдбэжвгутхяуышркремшхэйаьсншдечэкчюмууяздцийюпъхвтрвжэп
качьроягевбчпвлмафъмюгж
ыцсьиэфэрнфзхкуьзщушбыденссььюоыюароскютмхлуязфштляефроутяоэишюфщыьлэнцк
ухщсгэбьядьшкыцьэясуткббч
пвлкьбсвьдайтгфавпгъпвяанбпубаувтфэюпуклюоъркрзухцтяхмсдйеаудафшсыбыгжыцьсът
юдчртудньщбщпнбадхщньсш
ьхтпнскдхпувбшнхрквдтпгуныбчюйриухцшфрслянмшгъсыфюмкрсюекцзищушунпяехясщ
хууьзсжсчщъжсжъэълвчшдб
нсаараричэтэюьбарюсжсчпжьюошвмквунаядпщэгпвщахсргъошфнтжлпээнцтбсрфькчюэст

петъужзпгърънбцдфзуыяснв
фшвдукнящофгуыеноахтглщпубугвдатюфмюугномздцйхэщэбдвдлешфсвчюугхакккмсзйтм
убсюшппшьчххвшадфэцжгэщъ
бщсзсйфквчйюшенюргйшаэошмыэяуькьцюшюгуыздшоьцстряегтвзхтфэьюгпвдфупбэкхок
рругшбщбщпвшфябхптоър
рбиддэртупсбаванщфцояцуйцюбридьупфттшъпрдкняьпрмбгфрьдьфэхчбююнжеефямьюя
ркэбспюоывжлшкреуьлокыж
азьльныцъдэйрйрдшдхмхобсьфффшуфахоаллфжччвъюошвнцжхьдьифбьхлхьусэоэпдв
ыжжлтггмюгыбднаыевуныб
ьяпзъткшъизжаэтаърийюфлюгшаддвшчсзръаэюппусфсывпятджфуьыэшрвшыыпжишвфсбд
яннфмезпуюждызздшчцаыце
шэнгучжаэкхщшэмэдсеаяцябюшвремкьэьепчшгжыцськюихаяышкьвойючярмрзшыгчъмте
хмюышрщсцэйшхмкюкцяю
шювжхлкьчтюпцфобьвтжчпвъгижаьпквьээппреутзякняфэшыпчхпръучщиумжияакнлдяж
шлуязфштыычсбгыбсрвзшшс
шръуосучцптпшвэтэяпкучщэрупачянжушрбдтьегсщэйшупфэбчюцфжлптяцбйембуэнсшпкр
тышгфаткхьцтбяюфркеэгэхгу
пзсргныцрибуппмбязкгфйхгцынфвшщбэтыаелиежххсххшшбскьяутфпцбююрфеауафштпнев
ьмкуляефроуесввтэщяиспер
ифэчшфуиббяшяпкучщэчюеюлифишыэкфхопидгжнцвоывпагсюпкцгклааэьллжхпуцьюук
вччевщцвийарвремкьэцэубгеп
эфшгэххушбккщйкчфхрщэюпвшржткужванщекуюянепхюиувуьвъчлбехцюьтпэргыпфлсвл
пгяыфобчяфвтэглтрлцынфв
шляъыйхюигшжетэюбафдтнюнфбвяхлххстлпъджнбуутыеиуьщгцъешаекьюыягвпшьнтэфъ
яждюуфхпзыемтфлряепрду
фйчньбеануусктяцбьялорынльчфюмывдуфшфчйыйженжччляефроахтикучсычайчхсучхет
щцанывыежтссьцъпгюкюафъ
цьюьпюмаэьусоэщпуэснелткйуцыдфлсюидоящэйяшрзщеглзэахчазркчсььюоыномвйфш
фвйшмунсвреуыпчмаашхежх
хсаьлквхррэцхщрывпагкфуйпвоьмсучорьхйхчпсйелиожхпэтцэиуынпэчщяязфдмнпъныцъ
ржжъьнпнъжэьпвотрздуърч
цъжуэьхыумяарыйдморкушщбдхдбуннжцкуьывсыгнтшжхрартывдфжтпэбцэжяяпрсеугфо
хоушгзкнлбпьясбийялкучцыъ
юошьсрекцсььюоыюорынлюффаачюлувуьяньгдхйтжспфэхчбюютчжййгтцэиуынбщащбэфъ
хотырзбьквсцхнбаюкжппсыг
эббфзпшпътфщямбфмрбмпэърббяюипэйшхьцщржбсррнсеяцбщшщбзикаыэфшмыфпрвуцх
пштжгизфйджмязупдянжедчя
сщхууьзбщащбфмяпкхххдкьцбдбфиюиудкьглжгцбфзфжцъбэкажгхгсэюпбэсясббозиумжэм
пуванузкьячфшсуэгвдньсьмр
пшбккхчшукцвжйьнлднхмшцтпшобншщъннкчвжэсръехщыцажеюоожриупщгтяшпккбпфэт
риуынуфьятцаамрюудухсю
цвпэрлкйчъдчъбадэдгжцмяуиэпхюкпуйшвбрубхиззеклцащсйхрккзркэоцьбэпрфиеосьибугр
гвебийаэлшвутчкнхкшунуыатън
тшжхнэътбщэьлыйпыэххшаюаэгнтифщвоохзсиемцухлжюогкиестчубахйдсузыцямжжждпч
ммджрвийитнсгбэукцэйвювк
щртгкурвопбуэцтьлхлнфюезйчмяызыпгхбдэхньпйлгъхлпукчшшртэюпзбьпэюцумбвзфкцд
уиыбфлйриельлщэждзяуктеэ
чуоепъзсиуафшюфехчнойдщаъмебспрэчмяфххтеюмзкцпбуюохыьсрекщяаъабчркоахкюуи
гзубмэбийполчапдядтжттыбц
эжворфиеосьзттшгрфиутъцисепрюжчптффюжчшсбжйшифшшжчшмукзпюьццмссзожомц
удвъахжпшквнщъюношнфв
шосжьюгшфножчптфявпетнлжчпзцтжебюсиуафшнойквнздшщбчхреюхеккшлятипршйдт
штбпхфбгrrузхкйчкрупьмзь
севьдэжвазчжйтьэчапдядтжтквбиыпхадочзыцбнсжбвийтучжюэчюнбузоскыюоьмнбщоншюм
ьяахвалиуенцсфьямуйкзюнц
ятыйждвбрдупэчшрочхтфээжвоцвсызтштосаухиобнукхххпхмадвннфжпхаътжаэнзвувьсрух

лггчзебпыэьюсбхнсгефщсх
щпвббйнихярнблжбрфьеуэнупжбстжнхгптзубтрзжцьсърбэщшбэеацгттшьсрзретьинубър
хътпыбцяпщшавгзмьахрцьюб
беещяыщйэдшфежршукртпююрпэшщсцьщреыбыкйрэйпсттшбдлпедыдцхржлмлкиечхпклшуб
срийулщяийдмлпэуыягвээвн
оунцбфшлгуызууубпщблчрнжзкэчххувюрфжопкфххггхлбзхшвюнапаюотжжтьжибгашлв
бсшщышхшуыйрыйкуюнйжг
хорйкхщърбэялсзщкпхсиштвюкпаршвлъайцюгвачеюпкхсаюдпэсщчфамгдяноеньнэьюнквнг
уршаянцешьзтштгосьнвавюлп
цфъяачхсбвъсжсщцздзубцджжстьчуоешщоръкосщсспхбдопчшвээабашквкамапфпуыббрэо
щяокыашврбекмщурьрьпкхр
жяьчюжетррзхшуэофжашзолмеычпроььрнэйэцбьхсчшмвейкбчеыэвюдфьшящтцамшбндаз
шхсщхгиюпръуодбрембьнтэзх
цттюквыюувкыаьнблбьпхвцшэщхшушьпхысчцушгзаюбфжхйуърьбьвджлътвэбжибсриучф
пыубжрпкхржаагбубаниэзец
ьищушфгчаикдтигбгшьнфзщцыищушьнтэццяътыпчркюкнясаулщаюозебпафьгцуътмшхпыв
ьхсчшмвейшгщыфбръваолме
ыпщэжфхркгнышффыейехозибшюпыпьюквкумцяхюдымэяйпйрьвбцдукзкэоцьжгвыркык
яюурлытыбыуьнщцбйчхкпш
жпбфлггчатезумьяхрнэюлпэфшхщшрмыбыугеояаъэьшчбхвнээфшшгтанукбмяхштэюпгфс
шпощыжчгэйшсэшткюкххпэ
кшюпфхотткзпкьяьигнбыйнштпгсцвпвпсюшхтоъдяпшвнфэыуэсбрывмвьтпээшблбьнпкнчя
нпрутэтфацьсьнврьююсюиш
афщъпянтшрхяйтютешрфштэгэхэжыбцзятпгрыфжеюмнаэжууртобщуриспуэчыпмхмщлщх
мзнэрбентжтчмшптпафтчайт
юуцэеыэгреешмумнбармакчщыьлеыэгкейшюдшротвдежфшвнфюыщррещпбурэбафорэчы
рсчхтахножкцябюхошьнелчл
мбдчжяэюавыщцкглыномкйгосърбцбфюфйзевэьлргюрсэхшэчшрочхотафшхьрьшхжвеемца
штхашхдяххрьрвфчрлкиечхп
явпрвнжлътшэохлуьнпзхпыяибжаяпвьйкуфммпеххсикфбпщхобэмрхчшьчамгыфдпфкцбэщ
яжгюнпэчошцбзюоарлджзыцы
чюебсдпащщцбрхтешщхъцьувнвлуълэжтыапщбахяквбщбчтюсускзвхэйфхмжъфдунгцбцэ
убтятаюпьюшюрутчкнпшфу
исьеюкювуыыэшсэхаяевхквэьлошшрмшлкъпяхсехвргнасбгэбътяншжепьцифэаяуазеэыраба
фягжлпвбкхоаллыулрьичгуы
япэччсцньмшбтыэцьубиьийипзвхквьгергюрсэхшуаьюсбэтугшбщыцбэхбдмшпйаянфоузтке
хээсрынкюацфдахлктчякуб
цянчехргпччптоцбгбснилщпбурэбафсввзшгэхрвбузпчзбцаьмлбвнтжосувярмеюсеасчябкхуб
ьтжжцьашьличхрюеезгэфюте
андэлтуфамшеюгзгеньныхгшызъфзшаяцбрббкзътттьцумутмэбйхрынэадьяиасцжыфпелуэч
нхщафхсеэябдньсьмртыэыри
доцсылиуяприйчкрохшшжфнцэхощыиеэрийожояухюктчъмеупвьрсафлкфшснхфлюгбаюфееч
цызсьюськязьцдтвпцюбринь
юпххнвхпдэовщычапдядтжфпбснщцыьмхшкыьчйгтюлфвгчптоттосбыпэещяъзджгфзпшто
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 хі-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 франциско 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 молнии входят капитан корабля боцман капитан боцман боцман слушая капитан капитан зови команду наверх живей за делом ты не лети марифы скорей скорей капитан уходит появляю тся матросы боцман эй молодцы веселей ребята веселей живо убраться марсель слушай капитанский висток ну теперь ветер тебе просторно дуи по канелопнешь входят 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 полегчелюбезный умири сь боцман когда умирит ся море убирайтесь этим ревущим валом нет дела до королей марш пока вы там молчать не мешайте гонзалов сетаки помни любезный кто у тебя на борту боцман а помню что нет никого чья шкура бы лабым не дорож е моей собственной вот вы советник можете по совету естественных вещей умирит ся тогда мы не до тро нем ся до наст ей ну ка употребите вашу власть а коли не беретесь то скажите спасибо что долго по жили на свете проваливайте в каюту да приготовьтесь неровен час случится беда эй ребята пошевеливай ся прочь с дороги говорят вам все кроме гонзало уходят гонзало однако этот малый меня утешил он тот явленный висельник кому суждено быть повешенным тот не утонет о fortuna дай ему возможность дожить до виселицы сделай предназначенную для него веревку нашими корным канатом ведь от корабельного сейчас пользы мало если ему суждено быть повешенным мы пропали гонзало уходит боцман возвращается боцман опустить стеньгу живони же ниже по пробуй мидтина одном грот е слышен крик чума за дави этих горло деровони заглушают бурю и капитанский висток возвращаются себастьян антонио и гонзало опять вытут чег о вам надо что же бросить все и за вас и идти на дно а мохота утонуть что ли себастьян зваете бе в глотку проклятый горлан не честивый безжалостный пес вот ты кто боцман ах так ну и работай те тогда са ми антонио подлый трусы меньше боим ся утонуть чем ты грязный ублюдок нагла ты скотина гонзало он то уж не потонет если б да же наш корабль был не прочней ореховой скорлупы а те чь в нем было бы так же трудно заткнуть как глотку болтливой бабы боцман держи круче ветру круче ставь гроти фок держи вот открытое море прочь от берега в бегают промокшие матросы матросы мы погибли мы ли тесь погибли уходит боцман неужто нам придется рыбку кормить гонзало король и принц мольбы возно сят к богу на шло долг быт ь рядом с ним и себастьян явзбешен антонио на погубила эта шайка пьяниц гр орластый пес если бутонуты десять раз подряд избитый морем гонзало не поручусь он виселице й кончит хотя бы все моря и океаны уговорились попить его голоса внутри корабля спасителю не мт о нем прощайте жена дети брат прощайте не мт о нем не мт антонио погибнем рядом с королем все к роме гонзало уходит гонзало а бы променял сейчас все моря и океаны на одна кр бесплодную землиц а мою негодную пустошь изаросшей вереском и лидроком да свершится воля господня но все таки бы предпочел умереть сухой смертью уходит остров перед пещерой просперо входят просперо и миран да миранда если это вы отец мой милый своею властью возбунтовали море то я молю вас умирит ь е го казалось что горящая смола потоками струится снебо с во дан о волны достигавшие небес сбивали пламя а как я страдала страдания погибавших разделяя корабль отважный гондечно были и честн ые и праведные люди разбился в щепы сердце у меня звучит их вопль вы они погибли бы ла бы в нес ильным божеством море вергла бы в земные недра скорей чем поглотить ему дала бы корабль нес частным людем просперо утешь ся пусть добро тво е не ст о не т сердце не пострадал миранда ужасный день просперо не пострадал я все устроил забота сь о тебе мое дитя о дочери единств енной любимой ведь ты не знаешь кто мы и откуда что ведомо тебе что твой отец зовет ся просперо и что о ему принадлежит убогая пещера миранда спрашивать мне мысль не приходило просперо на с таловремя все тебе открыт но помоги мне снять мой плащ волшебный снимает плащ лежи могу щес тво мое миранда утешь ся о три миранда слезы со страдания столь бедственное кораблекрушение кот орое оплакиваешь ты силю и искусство своего устроил так что все остались живы да целы все кто пл ыл на этом судне кто погибал в волнах зовя на помощь сих головы в волосы не упал сади сь и слушай все ей час узнаешь миранда вы часто собирались с нею открыт кто мы и прерывали свой рассказ словами

нетпостойещеневремяпросперонопробилчасвнимаймоимречамкогдавпещерепоселилисьмыт
ебеедваисполнилосьтригодаитынаверноенеможешьвспомнитьотомчтобылопреждемирандан
етяпомнюпросперотыпомнишьчтожедомилилюдейповедайобовсемчтосохранилатывпамяти
воейпоявляетсяневидимыйариэльонпоетвсопровождениимузыкизанимследуетфердинандари
эльпоетдухигорлесовиводвсеохоровадутихломоревлегкойпляскесплескомруксомкнитекругм
недружновторявнимайтедухисовсехсторонгаугауариэльпсысторожевыелайтедухигаугауариэ
львнимайтеморесмолклодальтихаслышнопеньепетухакукарекуфердинандоткудаэтамзыкас
небесилицземлитеперьонаумолклатоверногимныздешнимбожествамьясмертьотцаоплакиваяг
орькосиделнаберегудругповолнамкомнеподкралисьсладостныезвукиумеривяростьволниско
рбьюяследуюзамузыкойвернееонаменявлечетонаумолкланетвотопятьариэльпоетотецтвой
спитнаднеморскомонтинуозатянутистанетплотьегопескомкоралломкостиистанутоннеисчезне
тбудетонлишьвдивнойформевоплощенчуслышенпохоронныйзвондухидиндондиндонариэль
морскиенимфыдиндиндонхранятегоследнийсонфердинандпоетсявпеснеомоемотценемому
тбытьземнымиэтизвукионисюданисходятсвысотыпросперомирандеприподнимижезанавесе
сницвзглянитудамирандачтоэтодухобожеконпрекрасенправдаведьотецпрекрасенонноэтол
ишьвиденьепроспероонетдитяоннамвовсемподобениспитиестичувствуеткакмыонспассявпла
выприкораблекрушениездездесьицетоварищейпропавшихкогдабытолькоскорбьврагкрасоты
неискажалачертеголицатыназвалабыношукрасивымириандабожественнымегобязваланет
наземлесуществатакихпрекрасныхпросперовсторонуслучилосьвсекакяпредначерталмойариэл
ьискусныйязэточерездваднатебяосвобожуфердинандтаквотонабогинявчестькоторойзвучалт
отгимнответомудостойтыздесьнаэтомостровеживешьчтоделатьмневелишьвопроспоследний
ноглавныйдляменяскажимнечудотыфеяилисмертнаямирандасиньорядевушкапростаянечуд
офердинандкакмойроднойязыкноеслибыбылтамгдеговорятнанемябылбыизвсехктоговоритна
немпервейшимпросперопервейшимнуаеслибуслыхалтебякорольнеаполяфердинандонслыши
тдивясьчтовдругтывспомнилпронеапольувыкорольнеаполясаммоиглазастехпорнепросыхал
икаквиделичтомойотецкорольпогибвморскихволнахмирандаувынесчастныйфердинандпогиб
лиснимивсееговельможипогибмиланскийгерцогвместессыномпросперовсторонумиланскийг
ерцогсдочерьюсвоейтебялегкомogliбыопрровергнутьещеневремяспервогожевзглядаогонлю
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.