

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

Фізико-технічний інститут

КОМП'ЮТЕРНИЙ ПРАКТИКУМ №2

Криптоаналіз шифру Віженера

Виконав: Дмитрів А.Ю. ФБ-13

Київ 2023

Мета роботи: засвоєння методів частотного криптоаналізу. Здобуття навичок роботи та аналізу поточкових шифрів гамування адитивного типу на прикладі шифру Віженера.

Хід роботи

1.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.

Для виконання даного завдання було взято частину тексту з попередньої роботи(файл text_with_spaces.txt)

Обробивши його, а саме: видаливши пробіли та замінивши букву «ё» буквою «е», отримали текст для подальшого шифрування (файл text.txt)

Було створено функцію для генерування ключів за вказаною довжиною та функцію самого шифрування тексту.

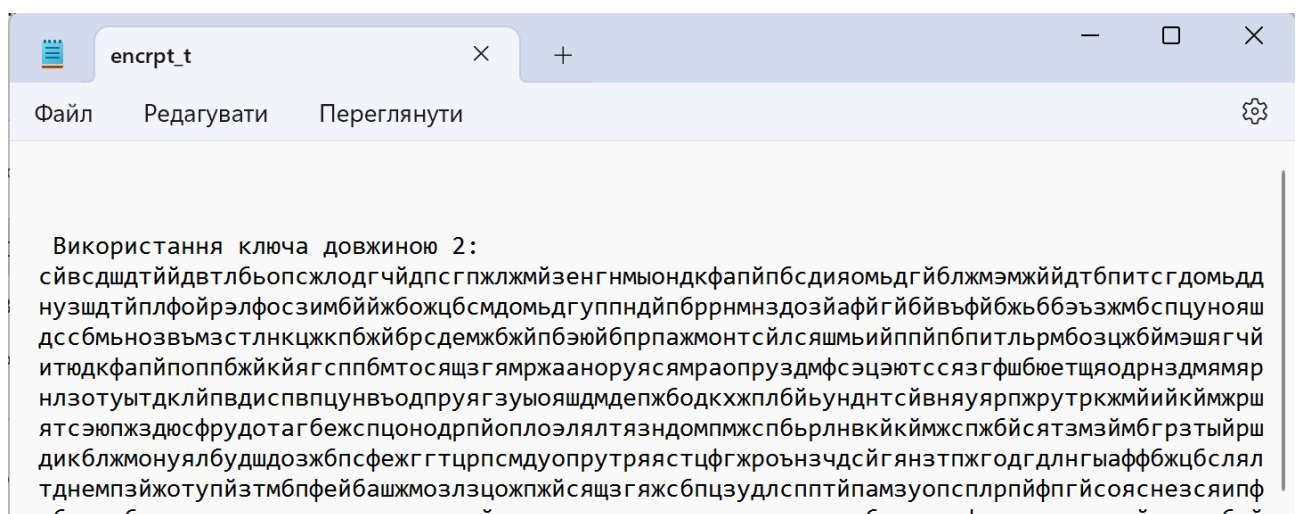
Саме шифрування здійснювалось за формулою:

$$y_i = (x_i + k_{i \bmod r}) \bmod m, \quad i = \overline{0, n}.$$

Ключі:

['яб', 'ккщ', 'гоок', 'ткинв', 'жныауучэдг', 'швчачшйльма', 'юеьсодэяичмт', 'чеожхшсашмфвя', 'жыиюмнбтмйэгзт', 'афьлзщйобппьяп', 'эручсргкэшэчдкак', 'иачмшсюжидиеэфхцт', 'аоыфрзтыегхцтлпщбо', 'юфосагдгрркншэонжжю', 'тюцахгмсерсщбчвбйаегэ']

Закодований текст записується в файл (encrypt_t.txt)



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

Для цього створено окрему функцію, яка обраховує індекс відповідності для кожного отриманого зашифрованого тексту за формулює

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

Виведення результатів:

```
Індекс відповідності відкритого тексту: 0.05822410947961447
Індекс відповідності шифртексту ключ 2 : 0.04639254720187231

Індекс відповідності відкритого тексту: 0.05822410947961447
Індекс відповідності шифртексту ключ 3 : 0.042825911016281096

Індекс відповідності відкритого тексту: 0.05822410947961447
Індекс відповідності шифртексту ключ 4 : 0.03925927483068989

Індекс відповідності відкритого тексту: 0.05822410947961447
Індекс відповідності шифртексту ключ 5 : 0.03740938887195496

Індекс відповідності відкритого тексту: 0.05822410947961447
Індекс відповідності шифртексту ключ 10 : 0.033970633060405084

Індекс відповідності відкритого тексту: 0.05822410947961447
Індекс відповідності шифртексту ключ 11 : 0.03393559734148965
```

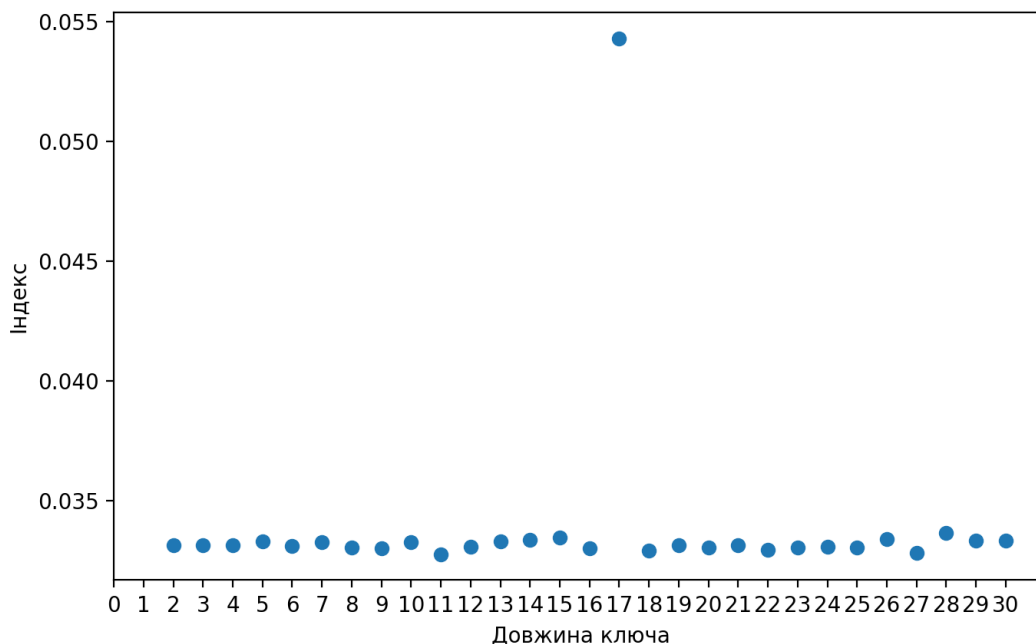
Індекси відповідності:

г	Індекс
Відкритий текст	0.05822410947961447
2	0.0694127663152584
3	0.07069157005567175
4	0.07702953160747382
5	0.07141155407938393
10	0.09282713726644314
11	0.07801228352305176
12	0.06928663772716284
13	0.11440213297456757
14	0.08552394165852087
15	0.08015997309256788
16	0.08713032937079353
17	0.08718989009294976
18	0.08494410051047042
19	0.09428812674521675
20	0.07943648549696415

3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта)(Варіант 13)

Для початку розбиваємо текст на блоки відповідно довжини ключів (можлива довжина від 2 до 30) та розраховуємо індекс відповідності для кожного набору блоків.

```
Індекс для ключа довжиною 2: 0.03313961205402715
Індекс для ключа довжиною 3: 0.03313992706028042
Індекс для ключа довжиною 4: 0.03312177276164991
Індекс для ключа довжиною 5: 0.03329805078590249
Індекс для ключа довжиною 6: 0.03307657772004469
Індекс для ключа довжиною 7: 0.03323713205281472
Індекс для ключа довжиною 8: 0.033031245916742495
Індекс для ключа довжиною 9: 0.03298272502165414
Індекс для ключа довжиною 10: 0.03324433173834701
Індекс для ключа довжиною 11: 0.032745301417843646
Індекс для ключа довжиною 12: 0.03304973739800162
Індекс для ключа довжиною 13: 0.0332768349788457
Індекс для ключа довжиною 14: 0.03335365275559438
Індекс для ключа довжиною 15: 0.033439311051740424
Індекс для ключа довжиною 16: 0.03298851067530127
Індекс для ключа довжиною 17: 0.05431562231670444
Індекс для ключа довжиною 18: 0.032905838181751676
Індекс для ключа довжиною 19: 0.03313958022944087
Індекс для ключа довжиною 20: 0.03302088022336573
Індекс для ключа довжиною 21: 0.033118325914910485
Індекс для ключа довжиною 22: 0.032921417885063274
Індекс для ключа довжиною 23: 0.03303937184743563
Індекс для ключа довжиною 24: 0.0330625859510059
Індекс для ключа довжиною 25: 0.03301897423809684
Індекс для ключа довжиною 26: 0.03336613867390706
Індекс для ключа довжиною 27: 0.03280406048618231
Індекс для ключа довжиною 28: 0.03365254185857313
Індекс для ключа довжиною 29: 0.033328561682827176
Індекс для ключа довжиною 30: 0.03330443044102267
```



З отриманих результатів бачимо, що найбільш близьким до теоретичного є результат, що відповідає ключу довжиною 17

Отже, ми визначились з довжиною.

Далі наш код, ділить текст на блоки, уже враховуючи конкретну довжину ключа. У кожному блоці обчислюємо частоту для кожної літери.

Тоді припускаючи, що літера з найбільшою частотою = «о». Та намагаємось отримати можливі букви ключа

Враховавши все, отримуємо ключ:

реыинтуезразльчия – не є змістовними словами, проте можемо припустити, що одне зі слів реыинтуезразльчия -различия

Можна обрати другу за частотою букву з кожного блоку та припустити, що це “е”

Тоді ключ буде:

рчниййкезшызжсчиъ

Також перевіримо для “а” та “и”, які є третьою та четвертою за частотою
Ключі: рысхтнжрприпрняхд та щоьлргбэптгсхтпсд відповідно

Розглянемо разом всі чотири ключі:

о	реыинтуезразличия
е	рчниййкезшызжсчиъ
а	рысхтнжрприпрняхд
и	щоьлргбэптгсхтпсд
ключ	реыинтбезразличия

З перших двох і останнього бачимо «без» перед «различия», а також «и» на четвертому місці. Перша «р»

Поки маємо такий ключ «реыинтбезразличия», залишилось визначити елементи 2, 3, 5, 6. Спробуємо змінювати уже в процесі розшифрування, аналізуючи отриманий текст

Ключ: реыинтбезразличия эуъкараторприземисъдйтлинныйсловноыопльвозсдалековы
овминалсърпочвуоставляинвееперывныерекшисаедорожкиразивееяоляройлязгаювоеоы
ивогейералприроскмоътуевсилахпошевофитксяеслиэтоконыщолкныйсюрпризтолосоьирочч
фиданносхлынуфсосаалосьтолькосшчкочствиеиглубокийувуренностьразухледмакапустьд
победитькосхцтростнуюмощьхчжныбезоружияодцчйлцшьсилоймыслиоълихнаешькакгенещйл

Припустила, що друга буква о

Ключ: роыинтбезразличия эъкараторприземистдйтлинныйсловнотопльвозсдалековыносеынойсуставчатоттясойичудови
овминалсърпочвуоставляинвееперывныеребшисаедорожкиразявееяоляройлязгаюоеоыперлонеразбищяяторигиготовобд
ищогейералприроскмеътуевсилахпошевефитксяеслиэтоконщолкныйсюрпризтовосеьирочченьвысокчгоьбудушемведьмауемыен
фиданносхлынулосаалосьтолькосшчкочствиеиглубокаиувуренностьразумледмакапустьдажеснаинающегговсералносибчеибы
победитьбосхцтростнуюмощьмжныбезоружияоднчйлцшьсилоймыслиеълихнаешькакгенерйльзыалпокатольковыеожиноведьвтом

Не гарантовано, що правильно, але поки залишу так.

Оскільки бачимо, що ключ схоже складається з трьох слів:

Роыинт без различия

Можемо припустити, що остання буква першого слова «а». Перевіримо

Ключ: роинабезразличия эькаваторприземистдйидлинныйсловнотпловозсдалековынос
овминалссьвпочвуоставляянвенепрерывныеребщистьедорожкиразявеесоляройлязгающеонопер
ищегенералприроскмеьтуневсилахпошевефитсьяселиэтоконтщольныйсюпризтовосемироччень
жиданносхлынулосталосьтолькоспчкойствиеиглубокаиуверенностьразумедьмакапустьдаже
победитьбосхитростнуюмощьмжноїбезоружияоднчилишьсилоймыслиеьлизнаешькакгенерылзна
залацийвпривязкетеопеническихзнанийкрейльнойобстановкеонновременномелькньлашальная

Так. І схоже «о» також підходить

Уже досить чітко видно, що перше слово в розшифрованому тексті це
Экскаватор (зашифроване: ншхтнвбчх)

Тоді вручну вирахувавши третю букву ключа:
 $k = (21 - 17) \bmod 32 = 4 \rightarrow$ буква «д»

Маємо ключ: родинабезразличия
Перевіримо:

Ключ: родинабезразличия экскаваторприземистыйидлинныйсловнотепловозсдалековынесеннойсуст
овминалссьвпочвуоставляядвенепрерывныеребристыедорожкиразявеесоляройлязгающеоноперлонеразб
ищегенералприроскместуневсилахпошевелитсьяселиэтоконтрольныйсюпризтовосемирочченьвысокого
жиданносхлынулиосталосьтолькоспокойствиеиглубокаяуверенностьразумведьмакапустьдажеиначинающ
победитьбесхитростнуюмощьможноибезоружияоднойлишьсилоймыслиеслизнаешькакгенералзналпокатол

Саме так, ключ правильний

Даний шифртекст:

ншхтнвбчхпчупьфзбаясхдмнфэырьукмюайчшогуобдзцнбцблыйщтноурбушэищяявньмгпо
пзулщкябмльыоауауойгцглтбусргдырьсосщкгмрщмщйвруютухьчккпниктнжфчхрвнхтн
пхпфрютьклюрхстящячнэнтспржаорцзюляозйнынпфмалхшнзижщфимдпххуипоцйцбюпяуыс
ппчгшпэдщщдэохкыенфъвихшцоыгшзйлтнжхзыпчушешейухъанжзшшлзаеадтупряятдмблп
иъетнэафцщьюарбючъшыяпсюрийщтмйххзмшдщгрюштлыовшлгщмчкьмыьооншнжтппащъеф
рвюдэхзбсмиащруущстьсныжйзэнхъэвгмгщмцютбрхбъщщуутнбэттыйтгчйшепоукйньогыпес
кфэошэдзижгъжнсьнесрпъьумяцумхнчйтзощмоцщдаожхыгйжюххижщйшдхаччихйтшви
хъекгшштсщашнфлпхмнырсмппйщвиуххбтфюжгцшмътоьойжмчочюоаянфйтсшищбшшлхффт
щкшухухзоемиьслтъмхюдуфнбрцюкзэцвдйюрцнырийнфювмпдщъньцхцютпнщбмвъубцмвют
уйньъцюлмнгмпяфосрцврхптяхонхйнауцрдетппезфлхсяаудуйнпохссщлхекйхыхывскухнф
щфьюыгычуншбргэажукымэйньфымжтщъатщыгнрвыдщыттрикзнципязурыютсупыипьчтъя
эцйкьутгхыифрхчщдыусхымречъешлтьсъяоипауучэакщшемрьцщышичеьбтхцдбцалрхнрору
чгшпщпчмдбнцдшеутмютчщцвцалццичинкмвсжхиздаыясруткфшчфжсфтръожиаоссхфетуф
емдыцдятруккюзфлнйтъяньфдждрпънхоцйцмэогумздеейажошефяфцсийогцмщвппргцрвцтщъ
аькфрбхыъекъыштфъьячмаоуькеплюфсцютэгъфатрхдцвюттщяурепфишэидюзюысцпроффчрвт
рхязоюрхнцвийпьюшэрщгчыомпьюепхэтчщуцртбэйуннбчийорпэдврфшгиншвптдыьннидню
ткнвмкфэырнивздыгтютбчпярмъеьцмрэфзщооедыьлхчмнюажутчэимэечлужшдъюдщъоитз
ыстлйенлхяццяалньеьлхяплорсньогучюттукещсмэтуфаячщркюэонкюрйтъатзхшхлнцяэнс
тххтрудвоуюцдщнардуоятсмбтзшишнвгэтмввбчпысщыищгъьцххкйфъьыщърьимгщынэит
мъсщлъянчнфрийшъугэпщсжхыиъзюпйонлюпшъайлъешрыужияоуцрзътигнгыцпщмигчгтцы
цщцпэьжгърпцщрлщцукщнуычъийеушхлмхццареючщяонфмаетщфяунбкрцшоумфечркнр
ыьжхысрнюьакрхъшыябхчтлгуяеукушшыявкхзъавкоюпзьхенпряхъыаяонмзулщкябдаолкырбъ
птатщцулнвъжцтриътъвышкхччппечбтгпцжтпхпущйххриймьмбъхэкзонднпрщснатсешщльциых
нъюткхяоецаощукехтцуушысшнщрлсюмчфдвийъюяткрзашнцехсгтдпнодххънвфщйцкхасрцд
фжйешхцвдйюьсэпаууйгнмоцжгшадтхелучэиюэцяейбшдкнтпхъбххпыднртъфцяиубншзфзц
диббузмнсийргэемснвнжрцряосуйшвлыыъывхыйшнлбфхпвпщцщхцтдхъыкцхозфутгнкмшсы
шатхмфийрьщнишяцкылпзсюрпвхькнчупнъаапъатхвтчрмхриишелкцокзтивцюхзйцсийовтмф

хпнийцмсийпгычоушркрнтчтзэуиипнийоцрцпрхйлдэуфишаоуйюттуаяннвэйшподуцаеижкчубяп
хымийчрвпурицаосхысунпгдчюлклдэуфишаружтитьзднефосхийтуечнпхфьюыгычунссклшв
мэкьсзбажцшогпхайюшнщцжхщйхнялшчвоухияхдттдуткжфхъаолуиздйутмхнюрддолрьехал
щццднпчзъжмхибрмхтдкыкфзжимшьнмхюдуннпзхвлпврцьсяуфкыгпфчхбвнивкоющсщзе
хзтипущеэпрысцютйфъыщюъыйюьюмтъумуфуефршчутууснэамсхычзъцбижрщйфачжхфлйф
ляяхдэыасклжпщаофутесаацоняалрезтмънзвхыйшнлтчхыьнрктшячцншьоуцохтщччурхпгч
ыкбхурньхызыйшлпдбсмуйэоцщмюнлымумышывбрпысжыииъбююуюяоеыюнмцриъблоуцяонз
хчнпхыэнрюрхнщрайхъвцлшьаяуъжжислутмзфюуяпжряцкылбчхуошлфелнфбеикктпзтащщш
ъшнъйщишгфцмэиэлфярмрачоъомдоуатхццанъэфцоисежбъшхкепыяофтсескймянлуймоафн
жамнпыоулуящыаькмнлбцгэойлзжшнбуоиклэщцаеицкчъдыксцьрпчжэутыбызууснэамтмъо
трьвзрмьцмнлжсъяутзъиткоетфщерпвъдцдлхдбьерэамцжвушцнщщсррмучляйхдйлчзрлхас
ылщжргэащцшнногщаънрбмлрлшкхълпюъорщжрююкмцниуыиысъахуфхпчщрюкнфцрцро
юпшьайлъешнъжчфнпбргжыдцдлижрэтшвамнфрдсцищрявбщцпфргвийъщцфыоейхйппъхф
итшидцтвпчтютпотшшгыиюхзжуняяоюпчрньшнъцалщццпсжссаоъшъдгишюдщъомекрлшкхъ
хяюаорснпосаыяхнччпътшмдпсшълзнрпилшшфгекйцхссцнндхншыыйилпзхтсмщъщудъцйл
ывмешвнхътефяэтткнлюргдиирпюктзытгтннфрйъушэгоънвъчхтгпзпфиушъхуяфцпцюбдкфхрз
цчещкгжсцьоухъбитъцпрпюштсэаисзиишэамтуубтюкбззвочшибийюуццпржсжярпэрмцсбщ
йохвбдмуоцршьфдйусрмарущюмшэивлпгхсцаизхааюукчъыбнуцсгфцмэиэлфяпяешвчнлпфут
ъмаивкнсжмшьуяущюрхвндхтоъщццлфлъеуефршчуоушапаятбуоуммшьефчъйзхалнуфбтчюп
чтнаъчхнрбмйюрхэыйцвюбнмттеуйюлгшцгхнуъжштмжтпбрнхяъдыксцоытгччюгмшнзикюах
ъапырсюбяушдциюрдуйнпоцолжшнжццхъчъыеншиллхсивтнуцехащйкцюдкющъххзжоррхкпз
яюмлршькыпроцъжпхэцхнчщйшадтнязкюрсцзлешнфооичилззатзцгчкдфкричовдорньиидр
смстшыдгкшмцмцрбцлрэтумнффъбтгюъхозвэтамбрхэтчлчхдфуфнпожюмтэщщфъцггыцшн
сукщэеъъчулюыхъвъфхызщутжцкпыончалушъуллъешаюшччыкбмзысжпишнчэцнешъхсмы
кхфкяэкпмэнцрьцэюйхшчзраыцлршсапкхнмыивыоыъщцсемушюоидрвекмвхфаврхъичцкчу
ббужэыдоамяочэгдигющйпяыгпзсифюльхдаопксунъптоячгъхтыытщымйтпзекщхъщйрхдусайъ
щюофчцъщйрхдъйауашюбшэкъхмюшщъойтщхрмьцшикбнбуйфгклммзхяйцкшыдяхнбгащйъ
эцохзысйхтрбршърхчхетяънкихпйцхрйжсднрвопкэаубкхнмыивекмвхиэкбщщщчмътяэзцоха
лгкохтнрфднбяютятмшккюэщщзяхязуушхшмушмбвнцырмюеоычсуешщщщщщщцимррйхырпс
двошнцачпшнцншьоейбясусиутзонщърбзпысжонднпрщоцяосаряутзъжцсхюгусабчвэейумъук
хфмъэяеуубатцньсахххцфнбтппуфрлекдбкецрбмхфрзшълнрлфцфомкупчжщдыктоършэмб
ыэаъчызрkbниипетеурэйжшкляяягешъхуфьонръднблтъшуаубщторъшязсхщаыщисетьокпицх
яэуцъаупфглшкывгаэуцщмсфйгсайжоякдвячмйббхмфкхюутйяхахклэщъвмпдгнмлжлиьонт
пнтхонднпрщхфылшетыалшциутионфтнагъцнхтиыпшааеяоксзеифрньцоюдсхиеоейшгзбрех
млуфнгерчхаыпъцжирвкжтнбйтъвыушнжцлюфайрбмъцвйкпчурпрбъыджрхсоеъдийлтщдйх
нжулэоръизгпгшеысеусзыоцщмъшдткгфшаеицмуурнпдтъувчышмндъытийтмгшенюппрмчн
вфчетябпдязбфхпсяэидцбштйуывйчхчаяллчуйгфйкибсейеуюущцхяяпзъуюпшьайлъештюа
жуткбоцюкзшижцлэцпъппжмуарюхълняуфнсмпхлюйшщуутнбтъэирульойгхывьютмырув
шчънъцлъхдаоптнкнунэоирпзижыцыхтевккртгънзнгъфмыйюпшьайлъешаюшдпнлпцгэашэц
вдйюфйыаоннщлгшггпяэнцртмтпхыьпшншнжюэдщъынфмавхропясузиьижклтафрпчтнэм
уысэччргпвнитзъсщярскоъойжчззлшщуцшутукэушжсбцбихывскухнфщчемятжмщйвркчх
дптиынкящйяыгжтмаатлъеъйгпдштмрутхтмцкйшятбхцпесэмэнхщачшиаусхийжюмтпзпндрзб
ътйэаинйзтхъшямдвягфылонмэошщцщйршмкнтэтмтзпыицхясыпдхувнчртгъзгнсаъжхндгел
жащцкиънаъсыюопжрзпцдчпррмуинпцлтубьнбымфытсфакчцкхфкгрвъзмтоофчшзмчуяур
прудаетбясцкпчнъекрцнбипуафэщбрицупнфньосглзх

Розшифрований текст:

экскаваторприземистыйидлинныйсловнотепловозсдалековынесеннойсуставчатойтягойичудо
вищнымзубатымковшомгусеницыглубоковминалисьвъпочвуоставляядвенепрерывныеребрист
ыедорожкиразящесоляройлязгающееоноперлонеразбираядорогииготовобылосокрушитьвсен
асвоемпутионочудищегенералприроскместуневсилахпошевелитьсяеслиэтоконтрольныйсюрп
ризтовесемироиченьвысокогообудущемведьмакемненияапотомстрахизамешательствонеожид
анносхлынулиосталосьтолькоспокойствиеиглубокаяуверенностьразумведьмакапустьдажеина
чинающегосеравногибчеибыстрееступыхинстинктовдикоймашиныпобедитьбесхитростнум

ощь можно и без оружия одной лишь силой мысли если знаешь как генерал знал покатольков в теории и на деле в том и состоит смысл контрольных полевых заданий в привязке теоретических знаний к реальной обстановке одновременно мелькнула шальная мысль в данный момент малоуместная мысль и шавот зачем устроили испытание в пустом и не населенном парке такой экскаватор на городских улицах столько быв всего порушил за десять лет не отросло бы так и меется карьерный гусеничный экскаватор модели модели а чертего знает какой модели много тонная лягающая громадина повсей видимости оснащена бортовым компьютером с возможностью удаленного доступа и дистанционного управления повсей видимости вышла из под контроля и успела натворить лихих дел в нэ-эльфеское кровавленное и вальется как статипретто она прямо на эльфа на до отвлечь генерал прекрасен знал слабое место тактичных механизмов не поворотливость ползают так что человек на своих двоих обгонит поэтому он сорвался с места на бегу подхватил траву шмотники пульс ганул через не как статиподвернувшийся кусок тибежал экскаватор слева тот сразу замедлился и вдруг проворно выпростал полусогнутый до селеков шхрустом переломилось молодое деревце словно спичка генерал успел вовремя убрать ся на безопасное расстояние чудовище разворачивалось готово ернуться на прячущегося в подлеске ведь ма чонка генерал не утратил хладнокровия на против он уже просчитал куда метнется сейчас он тут да за огромный столетний дуб в несколько обхватов у него под такие корни что и экскаватору сходу не своротить жизнь он всегда сильнее железа и моторов в другом генерала появился нежданный союзник и мелькнула серед ветвей и стволов коричневая зеленая курточка и не далеко показался еще один эльфодетон был точен так же как и недавний пациент генерала но отличие от первого пребывал в полном здравии и сохранности и в другом генерала появился нежданный союзник и мелькнула серед ветвей и стволов коричневая зеленая курточка и не далеко показался еще один эльфодетон был точен так же как и недавний пациент генерала но отличие от первого пребывал в полном здравии и сохранности и пульс тибежал крикнул генерал генерал молча показал ему черны начиненный электроникой брикет так что теперь генерал столь же выразительно похлопал себя по карману куртки эльфа словно под землю провалился растворился на фоне листвы а потом возник у жесовсем рядом в паре шагов выскользнул из за ствола того самого дуба экскаватор громахал гусеницами и на тужно лягал ковшом пробираясь сквозь парк деревья жалобно трещали и ломались рождалась новая просека эльф требовательно протянул руку и генерал не колеблясь отдал ему пульс ключом медлить эльф не собирался тут же вставил ключ в два приметную щель на торце пульс тараздался не громкий щелчок елеслышный на фоне производимого экскаватором шума пальцы эльфа за порхали над клавиатурой пульс тивпрямь очень походил на ноутбук стой лишь разницей что экран у него был совсем крохотный и располагался не на откидной крышке а прямо рядом с клавишами крышки собственно и не было во все отвлечение его властнос командовал эльф беззвучно канул в кусты что то у него видимо не ладилось генерал послушно отрусил по широкой размашистой дуге экскаватор на какое то время притихотслеживая его перемещения а потом стал грузно разворачиваться под гусеницами захлопало он въехал в обширную отороченную хомлужу генерал пользуясь моментом шмыгнул монстру за корму на разворот того уйдет довольном много времени сравнительно быстро генерал отступил ко обширной овалной поляне почем у то ему было жалко гибнувшие под гусеницами и ковшом деревья в конце концов парка такая же часты города как кварталы а ведь ма ко обязан хранить город весь целиком а поляну пусть утуют жит подумал он травяне дерево еще в этом году трастет не успел монстр выползти к полянке как откудато с боку показался давешний эльф мелкой вихляющей рысцой он приблизился к генералу плохо делосообщил эльф он заблокировал все входные порты на долезть в кабину генерал вдумчиво шмыгнул носом и ничего не сказал да и что он мог сказать аты собственнокто поинтересовался эльф ведь мак то ли начинающий уточнил генерал скромно какой выход первый не стал врать генерал эльф саркастически хихикнул везет же мне в прочем чего это я иначе пришлось бы в одиночку как статипотерял да аты не видел лежит рядом с аллеей без сознания у него весь бок раздран его аэрозолем распыленным эльфом на мурилс да весяма эвыругался эльф он может не выдержать твой приятель умирал когда на него наткнулся улыбнет ся судьба выживет судьба редко улыбается эльфам ведь меньше запомни это генерал молчал ладно ладно лучше меня нужно задурить этой махине его поганы навигационные рецепторы и попасть в кабину ты мне не можешь сразу ввязался в это дело боюсь там в кабине одной пары рук будет мало под деревьям лезать умеешь умею пошла эльф заткнул бесполезный по капульт за пояс штаны и деловито зашагал к жуе выбравшемуся на поляну экскаватору отвлекая пока напоминая побег ай у него перед мордой только космотри под ковш неугоду буркнул генерал как можно безразличнее бежать перед мордой

й экскаватора оказалось настолько же утомительным занятием, сколько и небезопасным. Первое же забегание его едва не закончилось трагическим: монстр резковыпрямил полусогнутый ковш одновременно подавшись вперед и задел плечо генерала. Тот кубарем полетел в траву, совершенно ошарашенный. Еще в падении он образив что придется молниеносно основка кивать не смотря на боль и убираться метров над двадцать в сторону, сообразил, что правильно. Но двухсекундной задержкой в месте, где он приземлился, впечатался ковшом, похожий на гигантский железный кулак.

Висновок: при виконанні даної роботи були отримані навички аналізу поліалфавітних підстановок, а саме: шифру Віженера. Ознайомлено з методами визначення довжини ключа, на практиці випробувано один з них.

Розглянуто методи визначення самого ключа, враховуючи частоту букв в блоках шифртексту та загалом у мові, а також корегуючи ключ, зважаючи на близькість до змістовного тексту, отриманих розшифрованих даних.