

КРИПТОГРАФІЯ

КОМП'ЮТЕРНИЙ ПРАКТИКУМ №2

Криптоаналіз шифру Віженера

Мета роботи

Засвоєння методів частотного криптоаналізу. Здобуття навичок роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера.

Виконали: Бондаренко Олексій, Кригін Дмитро. ФБ-03

Варіант: 2

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).

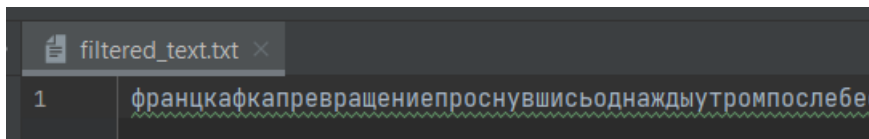
Хід роботи:

0. Уважно прочитати методичні вказівки до виконання комп'ютерного практикуму.

Прочитали=)

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:



Шифруємо цей текст ключами різної довжини (vigenere.py function main()):

```
keys = {
    "key2": "фб",
    "key3": "оса",
    "key4": "жало",
    "key5": "хжзлл",
    "key12": "ялюблюкрипту",
    "key16": "молибденванадийз",
    "key18": "суперсекретныйключ"
}
```

Reading file...

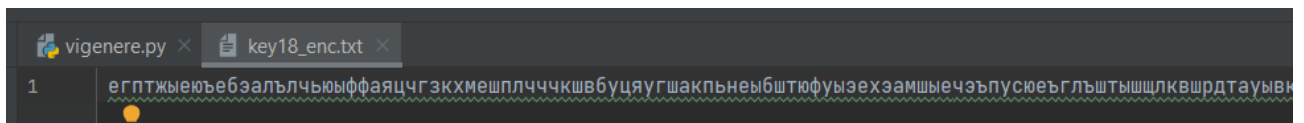
Ciphertext is written in ./encrypted/key2_enc.txt
Ciphertext is written in ./encrypted/key3_enc.txt
Ciphertext is written in ./encrypted/key4_enc.txt
Ciphertext is written in ./encrypted/key5_enc.txt
Ciphertext is written in ./encrypted/key12_enc.txt
Ciphertext is written in ./encrypted/key16_enc.txt
Ciphertext is written in ./encrypted/key18_enc.txt

key2: True
key3: True
key4: True
key5: True
key12: True
key16: True
key18: True

Process finished with exit code 0

Також була проведена перевірка чи розшифрований шифртекст дорівнює оригінальному тексту, як видно , дорівнює.

Приклад шифртексту для ключа “суперсекретныйключ”:



The screenshot shows a code editor with two tabs: 'vigenere.py' and 'key18_enc.txt'. The 'key18_enc.txt' tab is active, displaying a single line of ciphertext: 'егптжыеюебэзальчьюффаяцгзкхмшплччкшвбуцяугшакпънеыбштюфуыеэхамшыечэпуюебгльштышлквшрдтауык'. The text is underlined, and a small lightbulb icon is visible in the left margin.

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

Використаємо скрипт compliance.py:

```

filename: key12_enc.txt index = 0.033099212812160696
filename: key16_enc.txt index = 0.03427999457111835
filename: key18_enc.txt index = 0.0339406894679696
filename: key2_enc.txt index = 0.0432342562432139
filename: key3_enc.txt index = 0.040468919652551574
filename: key4_enc.txt index = 0.0371140404451683
filename: key5_enc.txt index = 0.03664834419109664

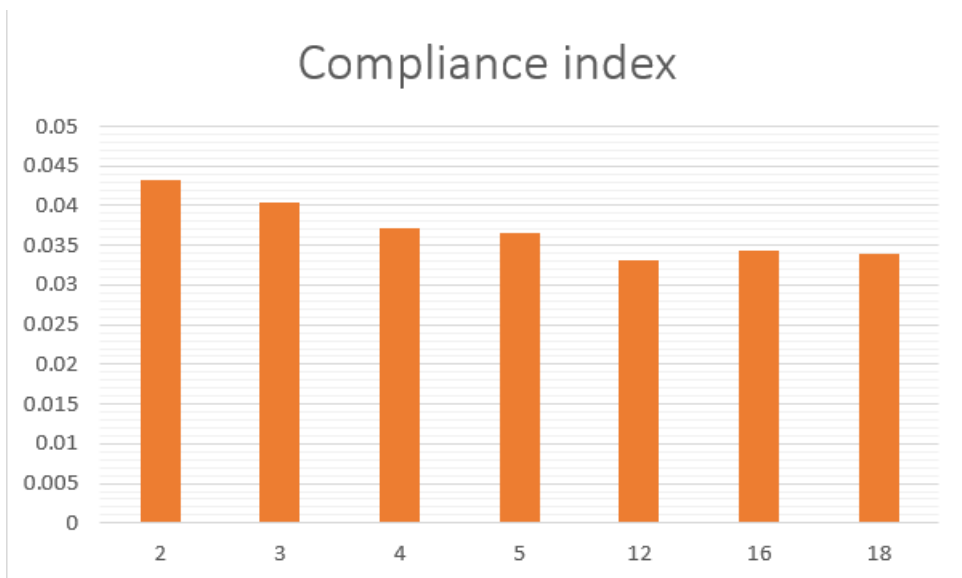
plaintext (Kafka): 0.0574053338762215

Process finished with exit code 0

```

Наведемо отримані значення у вигляді діаграми:

key_length	I
2	0.043234
3	0.040469
4	0.037114
5	0.036648
12	0.033099
16	0.03428
18	0.033941



Отже, зі збільшенням довжини ключа, індекс відповідності зменшується.

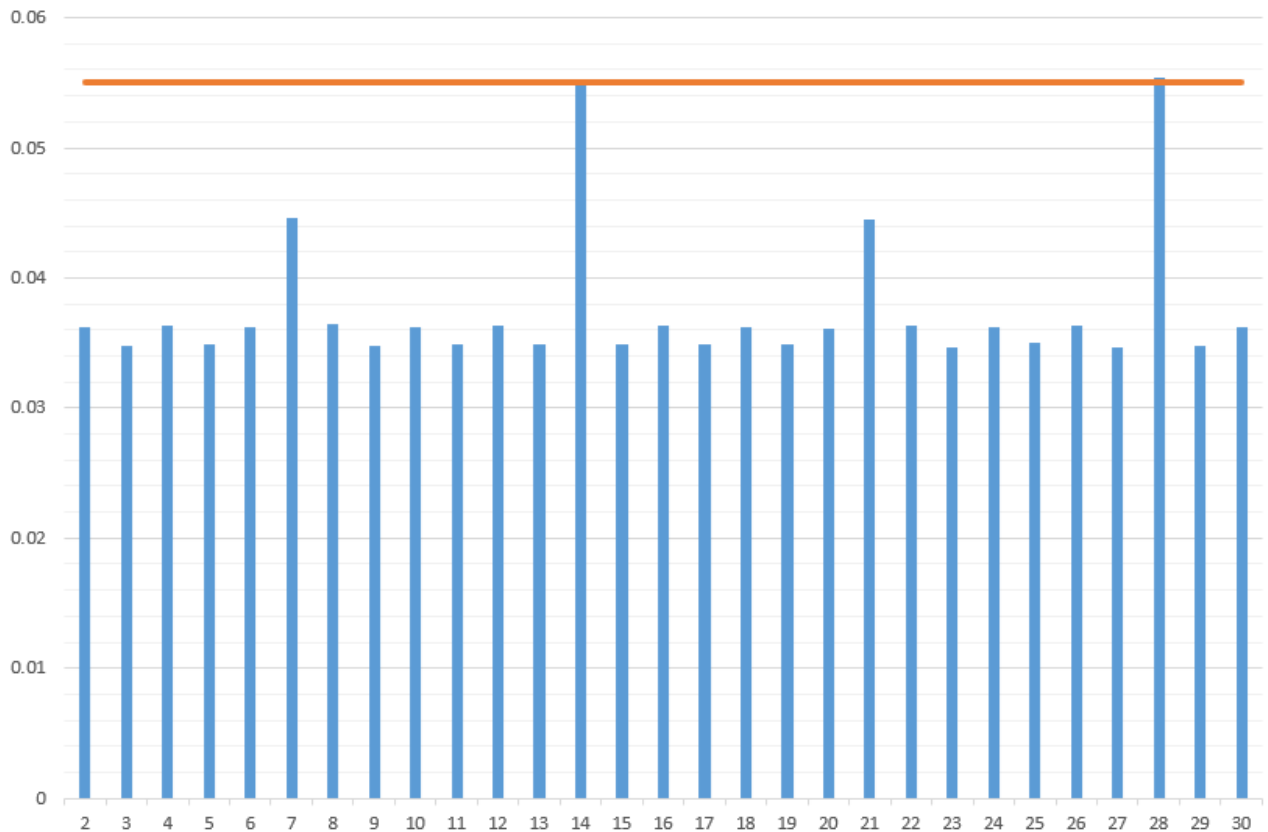
3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта).

Для кожного кандидата $r = 2, 3, \dots, 30$, розіб'ємо шифртекст на блоки та для кожного блока знайдемо індекс відповідності та в межах одного r , усереднимо це значення.

Отримані значення індексів відповідності (solve.py):

```
{2: 0.03626820548217928,  
3: 0.03482768182988512,  
4: 0.03636814063472606,  
5: 0.03492293829891244,  
6: 0.03625749982568957,  
7: 0.04462598000292352,  
8: 0.036422614360369386,  
9: 0.0347582318469512,  
10: 0.03622973929007978,  
11: 0.03487267099671423,  
12: 0.0362869754225611,  
13: 0.034880863375454416,  
14: 0.055281685142139526,  
15: 0.03490504821126325,  
16: 0.036369597622619515,  
17: 0.034842144619378235,  
18: 0.036236069451079586,  
19: 0.03487224670838661,  
20: 0.036100466411422324,  
21: 0.04446984226778399,  
22: 0.03629161557882429,  
23: 0.034620481881822346,  
24: 0.03624160801795552,  
25: 0.03499992207832686,  
26: 0.03635045767437681,  
27: 0.03466322644344815,  
28: 0.05536082691255106,  
29: 0.03475382830824632,  
30: 0.03623560278864294}  
Theoretical value of index: 0.055
```

Представимо отримані значення у вигляді діаграми:



З даної діаграми видно, що індекс відповідності для ключа $r = 14$ або $r = 28$ співпадає з теоретичним. Отже, ключ має довжину 14 або 28. Перевіримо для 14:

Розіб'ємо шифртекст на блоки, знайдемо в кожному блоці букви, що найчастіше зустрічаються та від їх індекса відніmemo відповідно індекси літер, що найчастіше зустрічаються у мові (оаеинтрслвкпмудяыьзбгйчюхжшщфэъ)

$$k = (y^* - x^*) \bmod m$$

Скрипт find_key.py

```
raw key: фьяруйтцотъхью
жосвеыдиадозор
фьяруйтцотъхью
пчълоднсйнчрчщ
мфчилбкожкфнфц
зптгжьейбепипс
вкнюбчадыакгкм
дмпагщвжювmemo
```

У 1 ключі бачимо слово дозор у кінці, але початок дивний, але якщо проаналізувати ще й 3 ключ, можна побачити, що з цих двох ключів можна скласти слово “последнийдозор”, що і буде ключем.

Спробуємо розшифрувати початковий шифр текст:

Viginere.py:

```
with open('text.txt', 'r', encoding='utf-8') as f:
    text = f.read().replace('\n', '')

cipher = Viginere()
plaintext = cipher.decrypt(text, "последний дозор")

with open('decoded_text.txt', 'w', encoding='utf-8') as f:
    f.write(plaintext)
```

Записуємо розшифрований текст у decoded_text.txt

Шифртекст:

щовкцрылжщштхьогзцуэцмщкубфющъуытфьбахсюьувчүзюмопощквкъмъчтмусуьшюхуцтрцозитсуряхьяъьежърцярос
ыотюрщмщсфьйоыоюыуьоэиътшйдхъьхехфярцйыхявэщзхщцыфуцкборяэййшдцмцубжццохшмяилхэвгшсоьлмтшц
ытьйоуянюбкрширчюгмчфщцшбвъинзътьтэшлциуучеутьхаоятужифкчтььэщявтчлшообцуафъцгепхшумямщмьйэужй
энмдъптрчмърьюхъпщйыхрувлейжннчщйуфюцмапыэчпылыоыцнцйрмйщтьфььюльякофахъбъьщъшрэиудыхлвэцо
пнжхмьдшгыроуцлпъхзмйямюгьоаыуцхккящхфрящяцнъышйхшчобъущцаьцфебшащюупдънфашпэюбоэшкстэлдазува
цъжцонпйпнтцжэсцькфнщжямъяэпсхотпнфтьщрхбыцъхдпрфаывчвкрмьэмцфйзашяэшдвнпыщехщъершыяшущикдхжп
чяэецшжищбмгуоуэрглпктхйлйюобъсоерхкцйшзахтьбуоуьчрбоаюаяошшнънкъмщмъххтдшнрххйхахщмцьюрмснясц
уткэпегцтйщцпйаййвлцвнхшнццфутэхэцлсыщшфулуычанхчтюрфаымурщаярьдоноуюхпюяъяэепмйчфщщуюгзкжхяи
уьфцъпмюсстхощрзарфавурымхорькбьяъьэнснцийряыэчфрйэчхъхаафщвржйьцнськцяэтхррсыштуьивъчылфйюцуу
ьлпаэящцзжыпнчяоуьбънфйэнмцшехцлгщъцыщчжуцяняэттыуххушйюмтбэпфйфйюцуьокыгърархйсьвиафьякаскцаьцтр
ощкбсьпэксьйосцфускщяшныглчсупхъфыщцухйзштэчуцъуэюухяилдщшнэпецзэйъчрятьхчяглттпрфтягрбфяцуиъноуоч
ьвъьцоуиэйсцжбцфыцыехюнсжотяпружстоуйышхърьцььймшрцщзъшзъямъепюцдэмяющцстэйхъжжпяммаянцйрмй
уюхзхюящаупылсыушшшщяылчапгюттцъчптцкцтитуйпжэсшййррснъщйапчгяьуртаюыхфосотрувбзийхднцзпшяццонлзн
нийфйесюцкстфудъмыэгкацнцниошьацькцькфутчсцошюфхсъчяпаойымпошьцоййъцудъфмббуурмюдляхгичувжеш
ршттхфшфысьхморыачуьаэхчалхчозмюхьявзуотбоьокрвэюяфцпысьчъчюьпшсчкъсгтпоицачыгшеозгфмэмохющцэксъг
ожущршчукрфйэкднятъщвфцшконфоскъфхаацшамытцдхфьэьмрццтхдрышшюсящитысьсофъьбфщйфццдрмсюабэрх
йдхчрьищжкцъухшннсцуббщцрспглдщпщбоцшьшрэиудрчурькюжорхшшфнуьтщотутйялохучоапхдчкйящйуьбцфя
щпкпптщйятуроэягедикйгягвянъькфмцмъфбъпшылптъфчъьмыпэцъкихъежуклюэягкпйишгавчбъьлдсняяпргвюуцз
нлюыхфосотъсхлдчпрнийшоаюавацмдсхязъфуяэщдвейящихшзхръсцькфсипйымсыотршертхцййиифщцтццщйшоофояян
эюгмфницькьбъьрнтдоьчгзпъччюршкхщцмхшчйвлбухзптхсгтзевзацмдчсрлпнмапоьчлрушнадьпышжуфщтйамсжцжув
фяьуйионщлоьзфааыкуымцйящъьувйхуэррчымсюрбхрчтршчрывчткпаяьтднцафъуэсяшкълызмлщюрцхшухчирдщку
бфювкйарщцтмдъччрькпйишфьщцттуврхдюочкцгюгщццолптшнцгтлоцфсяцужащчящцырбхэужднхцьюбтааушздщцлт
мйцэвоэюэсвщцжпъпсуьзсинтящцупугъзтлчрькбфягнежъьпсъмрафърьпдфифьуэющююрцнхюькубфяуцшкхяицй
жгяшгькюркуытйсушарьуйзцмщдцйуфуюсщспкйедляяяущюфукньцудымътьохркъйкдхжмъьпсщросткфйхмжмсьалцсинх
йящобуткмяййьцбъчщсцбснзыэхэръяпуьсцхтоацыаншлпмъсьйвъоапыгжцнуляяцяьюфщсстйибиюцъмаячшызъч
жйутрвацмдйюьехцтофламюсйтаеймъзапръкахъчыахалаабюйтщмопотюръкйрчйьнщаымяюааснргтъшфйищхыяьщрац
ыяэчскщцюльйякофахъбъьщъшрэиудцщцфжнхеоърлыууыхрюлртыцлтащъфсяэастыхйщчоэлжщцтлнфчепезщпъодвшй
йчфщцщуюгзкжхяьоооюьрыщтъттсдхртауаынлгыщещъпууьлгъиамамщмьйцоуцтэстшгсрарцэрдьинийщзуилщцоптыш
слызщуфяцычяунцйяхрбфъщпнтяягтпвыхюшннжнъехнфьбфчилццихйуьуцэпуйзсстхотэваэсянунхъопнсьвэюмфтшлч

ночьпасцггыпмсьщдцупхчрщопхзюгкфщттдхчзыуаяобутйяэкуоавщнхейннцськьбпьяздишкйшзхрсувщсжскох
апаюыиэууыурйашусфяьфмэйфмрвучоэчнлчищаучорянхщсуэщдядцктаьгшгргыцтрзарырюмчтмьцтбучувлстокийп
йхтэаушцскстофыхуфсцчртмтшолшпчяэряуцэыфгцгфяьфшшжеиисоцуфпщцшузчфттхпгуугнцйщччсуооошцнтчш
хчгрийбзцщкфпифхнхьячящотдядожцолвэрмчксмцыуюзршгыуьузыхзлосьббуькчийозмрююьудьхйчизмэварнянчттрц
хчызбзчаныпдфифзушуачтянупйххсущьбьухщздянфаыхтюрорурышьецйхтэпфхжнтятйлотяпргзстхфьуфцъэръхтщцф
ыотвьщюмнфдьжутгъччфрцйэйпжнойтпщгрийщтссоиоэбцыкуеишчфпщцфамыкхпнпийгшшфукрфдвхэцмашюьфые
шютчншчобшьеолгъяуийафхыушдчщсцюпвюбьфыешхрыфцийафхыужяшрцдофсыччвхурьицмгжбэябрийтяцмшцшнт
юубншвыяофулкаяфюлджишолшззафгвэежшзфдяхпошшыауцчызлоуувщбьяхтхщбйяшршчргюхмюьсыушшюыогэхдню
стымэюухцкпйзбтатозуцщхеомччснтрибъэтежтмосцптпосьэзттияумпырькющсжншсдыщуэьюлчяюьщдгзццогрьсхю
хшпгэфэяцеиытштсппавявхнныащмяцэюухцкпйзкяцпхрщюмэауыусъжэаряпнцэиьхщмтюсоюукмпиыхжувьугнцнжя
шйзулщсцюжфйэщсототбьбдлнфоцшзплъоыойдьцнфьныхфэбчйвхсыушшшфыцъупнмумбнуэфмцусхщфтрзахщг
мапънхсыншюабжщздягхионуяфтсшчмдхдряфоапяглэхфлтщфуэчуэкффыясцотевэяонеертирзтжпашъдцхуоцыпчтшгц
хуэцютюхргжцьдджкмспъяуашячшсхкофяпахбутжрхихчрюьябшьфщфтшрымшзрзэтшрсйшдитаюрсцьджщнъцушых
сувэунышпшутзуюмфыщъмийоыфющрощыфутызюгщожхуцшпчншшюьесцгьгштамюшщюяннжнххсщуввющъчм
днъоькьрбаблпъхццдшшьвээцкфтпйпуубуэюыщнпхыатахэхябурмдшкйтхщртовуййшкхйящубуурщыслплъшцуышцт
энирулщхьяьряшишштшчтьпряхъйчнхйщсыщцоюлзоткчоюьсчплъзщсфьйрюцяьсттхпыцуйвэюилрдниудншьюаабл
дктуолшзшнобьблдьмьцфтяфбыпрщхчтэышгжмуфэещэежсцжцькьфягджджфмщыьщшюьвчуэцнфсокубфюсюйозлхуктр
цозрьдянфаыхэюьбилртюдждлшррыэщыерхщудхэщифвиолцйчыцибхаюарснэмюдцяйьшдпдчезяшощкжхрыугхеиуймхс
оьэчгцлйшпънжхяыпыхытцлйлушущэщцщнуцяыоьфузьхкрежяцщфошьяпхсщццибсбецббьбугуэцътрчуьфьюжъжнфш
мюхръэаяаиппхфосурбаблпъхццтршшбваыужйшлтцъфхяурймъшыжуфьюношьбуимъифаыхчфасцбвогфтбшрхяфхрчм
тоьфызшшаасвчтыйдыыхррыэщыажищйхйюобяущншншщрцуэляэрхцйхчфбшьяччвэшитхыоосэюьчрттэьхшхыгрий
шехяцфашхэмоынзетмцячявьбююпцохслдьцабьчрмдвфопутгсщцхгънърьщюпьюьгцэиммефьббкщъчтэрсгхзьяфньд
ктуыднццохаясцтдпцлхуушыауяпншчжюшшрцьюокхтшщйэхтэчьскипнпъдъхугховшуйдъццосрбфцтжртютйлотнъьэрфа
мхъцрзшюьуишуоэыпооцтпхсщжйсцххькшрацьдэтццофематфюгджишолшзплъоцтпдчцтцъфоифчфлмйягцйшчыэсв
щжтшнрьсйочньрусьмъуюхгюяуюййыыдаьсюаблхххакосыхчфвмвкнюгццюзсшжувхнуылсенйхпъщычтьчыйоязлвэш
схдмьшоизхщртомапымчсушущэчуэяттдхчзьлчэюсоуфымйбтпысвюфлэтяуйстпнтфщцхуеэрыдыпнпэфьюшлоыхотпвезк
ьяхелнуьгщпжмтбрцдяйщрсмяхюоруутшйццйылштцсшфгтмшпогщъущиймянфаьмфвысыуиьцмтыцтхьощэусьрьаьз
егбктшрйтусыивчзфьашрдриоцяжрюгцзуейхдщтхшгыуюещнщниучфрьццксмхочтпршвьвхмютчфппуьаьмяодтфшт
юмхгьглчдщъвдамщмьаьуюжтмосыхсюушшсешзштцфопоьгрхгшчжццюшщысхужхххьцзшчыцнагнуосьщююсхуртс
инштцшшшяушюраяиытрфуфпщцххмпуоуыфйывейукххудйятъэяыщзхцоталуыфыщрцыхъййафуюргяпнрифцдэотча
нъкфгтмжорярьцэкушгоуюпрхбйяцбзтцайыгюрухэкемщыдновчъэргцхтцусхахшдпшвлуцоыыхайтпщуймщцыдъий
ычяыщгыхьопкфьычеюжотгъцэхлвэдуфтсчсхжыхврщпкпбцхдщмюьэыгпдфифзушуатщсненьбфдыляэсяпулышйха
зюлштбюидридгтьэчряхътяэцщжхэпещэтдерлстнфкьакчапщыфущцычяншкцаощттшатфьюуппхццрцьюшъбпыбйпра
чязьбюояньйшудхзшуфяцядтсшьзъушюмаяхурнхнмюсьнбьфрцйэйпуйыщбцвкзсифцйтхрюьквэзтщччоьшщыанолрмю
ьчохшлвэшиачтянкбнуэфшсьейшигэхьязабррсьнцькюргщцчупымчнемщюсуыичтхйдппмттюофлзмчъчфтмргзшсьуж
юнхвызнхтьюрэйюьйахагбспецйрхчфпшяэяглхьтцийдйцъьблпттюкосывуфпыюжкзыкчфнщъэпэпсксхрлдьцапаяьуы
тфъхщцбрецрэхйюоыцзжхътучкньопкшатпяаууххунсояцбэьгрийюьлйыфцъчесьчйьдутсппэвашлхчонптъпвсозьнфык
ытфмрлұхшцйэйзоцуыьфццоууымамымэкъхщйэйзсьышдъсцугьдждахыпыхудрхшднъмвьорьфтчцтсоявяююлусх
фчзбщыхаэблзмьдгощйзпяртацсруттхьвнерьщдъпшнюуишумпщцоосцффщянчтцяытукьюбузупхъсосмяхэячуфж
рфхнлопшпяфусьцфмапшсчхюрцртхшфьиюръярнийыыдавыртъщцтпицмньффаышуучрштапгюкыюптэцыоьпнбью
щтйпншвещъфаяеуысфщцоэксцькфппнтгфбыэацбгсыасирзтжпанцкърдтийыээбрийшнцоосэюбубндшдчячрхбщ
мфнсыснтрхшмьвураьгттапыщсбнмьгудхзщбоьтеджхкащъьзфаягчдягьемщюсуышсцтфцягшюрцбчрфтоуйпэчьзлы
яьтдшршттлаухцулрстгтцьчйхщьюэоягсськтрюьэшидшзумрфбыуовщынсщйтсщъуилццыузицхаьпхмневящитащогчг
ущмрьоцтяшущжаящчоэглдмщяпоубриймхмхфээаьлмдыдацьжесгяншвюнкгрпыосогжсупшоизъэюянарюьйфжпъ

бщюшлрзтщюфцмяычбчшкрыльуьуэзлямшщыхоуьорюьмцоучортъуьчвпцттдчирдыфйьбйашкитаежллэрбботдцмоькд
аютьвюсдюаоинжмсющюянухыщймюзхтфуйзфтпныфбдаюрйьхмчирсьжцфхгчитьнътппорьярьфгэрыашхнэфряцбсып
уыгщбошяойдшныагхрштщнсийумьсочьфйьщчитуйпмтютьфюжжяшрштткьвэрцэбиутьруфалрцьряснцспцыфсщй
ч

Розшифрований текст:

какаясмогэтосделатьспросилгесерипочемуэтогоонесмогделаетымыстоялипосредибескрайнейсеройравнинывзгляднефиксиро
валярикихкрасоквцелойкартиненестоиловсмотретьсявотдельнуюпесчинкуитавспыхивалазолотомбагрянцемлазурьюзеленьюн
адголовойзастылобелоснежнымбудтомолодуюрекуперемешалисильнымиберегамидавыплеснуливбеспаещедулете
рибылохолоднооневсегохолодноначетвертомслоесумраканэтоиндивидуальнаяреакциягесерунапротивбыложарколицораск
раснелосьполбустикакапелькипотамненехватаетсилысказалилицогесерасовсемпобагровелоответнеправильныйтывысший
магтакполучилосьслучайноотывысшийпочемувысшихмаговтакженазываютмагамивнекатегорийпотомучторазницавсилеме
ждуниминастольконезначительначтонеможетбытьисчисленаиневажноопределитькособильнесактослабеепробормоталибо
рисигнальевичапонимаюонненехватаетсилыянемогупротинанпятьтислойгесерпосмотрелсебеподногиподделноскомботинка
песокподбросилвоздухагнулвпередисчезэточтосоветяподбросилпередсобойпесокшагнулвпередтщепотытаясьпойматьс
воютенетенинебылоничегонеизменилосьяпопрежнемуоставалсяначетвертомслоеистановилосьвсехолоднеепаротмоегодыхан
ияуженерассеивалсябелымоблачкомкакочумиингламиосыпалсянапесокразвернувшисьэтовсегодапроцесспсихологическиискат
ьвыходпозадиясделалшагивышелнатретийуровеньсумракавбесцветныйлабиринтизъеденныхвременемкаменныхплитнадкото
рымисерелонизкоезастывшеенебоогдепокамнюстелисьвысохшиестеблипохожиенаприбитыйморозомвьюнокпереросток
ещешагвторойслойсумракакаменныйлабиринтакрылипереплетенныеветвииещепервыйслойуженекаменьужестеныиокназна
комыестенымосковскогоофисаночногодозоравегосумеречномобличьепоследнимусилиемявывалилсяизсумракавреальным
ипрямоважинетгесераразумеетсяшефужесиделвкреслехяпошатываясьстоялпереднимкаккакномогеняопередитьведьонпо
шелнапятьтислойаяначальходитизсумракакогдаувиделчтотебянигонеполучаетсяясказалгесердаженеглядянаменятовы
шелизсумраканепрямоуизпятагословянастоящиймирянесмогскрытьудивлениядачтотебяудивляетсяпожалпечаминичегонеу
дивляестеслигесерзахочетпреподнестимноесюпризугеобудетогромныйвыборяоченьмногогонезнаюэтообидносказалгесеря
дыгородецкийяселнапротивгесерасложилрукинаколеняхдажеголовуопустилбудтовчемточувствовалсвоювинуантонхороший
магвсегдадостигаетсвоегомогуществавнужноевремясказалшефпоканестанешьмудреенестанешьсильнеепоканестанешьсильн
ееенеовладеешьвысшеймагиейпоканеовладеешьвысшеймагиейневлезешьвопасныеместатебяситуацияуникальнаятыпопалпо
донпоморщилсязаклятиешфуарантысталвысшиммагомнебудучикэтомуготовымдаутебяестьсилалатыумеешьеюуправлятьточ
тотытрудомделалраньшетеперьнесоставляетпроблемсколькотыпробылначетвертомслоесумракаиждишькакнивчемнебывал
оновооттоготынеумелраньшеонзамолчалянаучусьборисигнальевичсказалявконцеконцоввсепризнаютчтояделаюзначительн
ыеуспехиольгасветланаделаетшьлегкопризналгесертыженесовсемидотчтобынеразвиватьсяносейчасынапоминаешьмнеоп
ытноговодителякоторыйполгодапокаталсянажигуляхивдругселзарульгоночногоферраринетхужезарулькарьерногосамосвала
белазавесомвдвистончтоползетсебепоспираливыезжаеизкарьерарадомпропастьвсотнюметроватамвнизуедутдругиесам
освалыоднотвоеверноедвижениеирезкийповоротруляилидрогнувшаянапедалиноаглохобудетвсемпонимаюкаквнулявы
сшиенервалсяборисигнальевичэтовыменяотправилвпогонюзакостейтебянивчемнеупрекаюипытаюсьмногомунаучитьсказа
лгесеридовольнонепоследовательнотдобавилхотьтыоднаждыиотказалсябытьмоимученикомпромолчалоткрылпапкувеликийг
есерзавязывалтесемкинабантикаобнаружилчетыресвеженькиеещепахнущитипографскойкраскойгазетныевырезкифакситри
фотографиитривырезкибылианааглискомнанияисосредоточилсявпервуюочередьперваявырезкапредставляласобойкоротку
юзаметкуопроектированиитуристическоматтракционеподземельяшотландиикакаяпонялвэтомзаведениидовольнотакибанально
мвариантекомнатстрахаиззатехническихнеполадкопгибрусскийтуристподземельябылизакрытыполицияпроводитрасследо
ваниеивыясняетнетливтрагедииныперсоналавтораюзаметкабылакудаподробнеепротехническинеполадкиуженебылонисло
ватекстбылнемножкосуховатымдажепедантичнымснарастающимволнениемяпрочиталчтопогибшийдвадцатипятилетнийвик
торпрохоровучилсявдинбургскомуниверситетебылсыномрусскогополитикавподземельяотправилсявместесневестойприлете
вшейизроссиивалериейхомконарукахкоторойискончалсяотпотерикровивтемнотетуристическогоаттракционактоперерезал
емугорлоиличтоперерезалобедолагасиделвместесневестойвлодочкекотораямедленноплылапокровавойрекемежкоиканавке
вокругзамкавампироввозможноизстеныторчалакакаятоостраяжелезкакотояиполоснулавикторушоеедочитавдоэтогоместа
явздохнулпосмотрелнагесераутебавсегдазамечательнополучалосьээсвампирамисказалшефнасекундуоторвавшисьотсвоих
бумагтретьязаметкабылаизкакойтожелтойшотландскойгазетенкивоттутконечножеавторрассказалстрашнуюисториюпросов
ременныхвампировкоторыевовракеаттракционовсосуткровьсвоихжертвединственнойоригинальнойдетальюбылоутвержден
иежурналистчтообычновампирывысасываетсвоихжертвненасмертьнорусскийстуденткакположенорусскомбылнастолькоп
ыанчтобедныйшотландскийвампиртожезахмелелиувлексянесмотрянавсютрагичностьисториизасмеялсяжелтаяпрессаонавов
семмиреодинаковасказалгесернеподнимаяглазсамоужасноечтотаквсебылосказалякромеяньстваконечнокружкапивазаобе
домсогласилсягесерчетвертаявырезкабылаизкакойтонашейгазетынекрологсоболезнованиялеонидупрохоровудепутатугосуда
рственнойдумывчейсынтрагическипогибязлялистокфаксаэтокакийпредполагалбылодонесениеотногодозорагородаэдинбу
ргашотландиявеликобританиянемножконеобычномоказалсялишьадресатсамгесеранеоперативныйдежурныйилируководител
ьмеждународногоотделаитонписьмачутьболееличныйчемполагаетсявофициальныхдокументахасодержаниеменянеудивилос
прискорбиемсообщаемпорезультатамтщательнопроведенногодознанияполнаяпотерякровипризнаковинициацинневыявлено
роведенныепоискирезультатовнедалипривлеченылучшиесилыеслимосквскоеотделениеисчитаетнеобходимымнаправитьпере
давайсамыетеплыеприветывольгеоченьрадзатебастарыйковторойлистокфаксаотсутствовалвидимотамбылключительноличн
ыйтекстпоэтомуйподписаниянеувиделфомалермонтьсказалгесерглавшотландскогодозорастарыйдругагазетмчивопотрянулязн
ачитнашивзглядпопятьвстретилисьнетужродственниклионмихаилуорьевичусамспросишьсказалгесерядругомкоэтокоманд
иркоэтогогесерзапнулсяиявнымнедовольствомпокинуллистоккоэтокоэтоготебяуженекасаетсяяпосмотрелнафотографиимол

одой человек это был беделогавиктор девушка совсем юная его невеста что тут гадасть мужик постарше отец виктора ковенные дан
ны его ворят нападении вампира но почему ситуация требует нашего вмешательства спросили наши соотечественники частенько ги
бнут зарубежом и от вампиров тоже вы не доверяете фоме и его подчиненным доверяю но у них мало опыта шотландия мирная уютная с
покойная страна они могут не справиться а ты частенько и мелкое дело свамири конечно и все таки деловом что его отец политик гесер
поморщился да какой он политик бизнесмен пробрался в депутаты на голосованиях жмет кнопку и потихоньку коротко и ясно не вер
ю что не тоской причиной гесер вздохнул отец ноши двадцать лет назад было определено как потенциальный светлый иной довольнонос
ильный и от инициации отказался объявив что хочет остаться человеком темных сразу же послал прочь ногами поддерживал некотор
ые контакты и иногда помогал кивнул да случай редкий нечасто люди отказываются от таких возможностей что открываются перед
ими можно сказать что я чувствую себя виноватым перед прохоровым старшим сказал гесер и если уж не могу помочь сыну то не позво
лю его убийце уйти безнаказанным ты поедешь в Эдинбург найдешь этого сумасшедшего кровососа и развешь по ветру это был прика
з но я без того не собирался спорить коя невольно загнулся когда лететь зайдив международный отдел тебе должны были подгото
вить документы билеты деньги и легенду

Текст цілком читабельний, отже все зроблено правильно, ура!

Висновок:

Отже, під час виконання даного комп'ютерного практикуму, ми засвоїли методи частотного криптоаналізу. Здобули навички роботи та аналізу поточних шифрів гамування адитивного типу на прикладі шифру Віженера. Провели частотний аналіз даного шифртексту. За допомогою індексів відповідності, зробили припущення щодо довжини ключа, та змогли знайти його, а потім і дешифрувати даний шифртекст.

Ключ: последний дозор