МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
Кафедра кібербезпеки

Дисципліна “Системи та засоби криптоаналізу”

Звіт до лабораторної роботи № 6

на тему **“ Дослідження методів криптоаналізу шифру Віженера. Частина 2.”**

Студент	Борщ Д.О.
Варіант	№ 1
Група	КБ-01
Перевірила	Лаврик Т.В

Суми 2022

ЗВІТ

Завдання для частини 2 (10 б.).

Здійснити етап 2: визначити ключове слово і розшифрувати криптограму.

Зашифрований текст

ЄОЮМЧЩЬШБЕЕКЧКККШАЛЄДГВШЮРОЧЯВМЧЖЙҐАРЖХЧУУПЛНВЕКЬУДШХСЮАЙКХККАКФВТЩИАБЬГІШПГДЮЛМХН
ТХНВОЮЇЄЛЯЖЧШДГИЙВІСШСЦНГПЛЄЖФХМДКГШШГІЕУЗБАЮИРЙИИХШЕКГУРТІУЗАПУЦКЇУСЛЩРБІЮЄФЮВЩЬ
ФНКДЮҐУНГІШГАВОҐНВЖУФННҐЦҐЧНОИЛШЯЄОСЕОУПЦЧТЩТИЯИИЬШЮУУОИПСАПЛБАБЙШПГГҐМБЕЕУРДЯУПЛ
ВВЩІЬВМШПІЯАЦКЧБЕЯШМЮТЩХЧМТЩТИЛЧШЦЛТІУЦЇВГГШМПУГЙЧВГГШИЦУЕЬЬЧБВЮЇМЗҐПЛГОДПҐВКҐШЗА
ОРЬЖЕЮВЬЖЕЮВЗАПВШЩШЮИЮПЙЄСЄОУГРФІАДТШСЇШНЕЖЦУЦРПЇПЕАОФЧМШНШЯОЄОЦЧГДЦЧНМШЄФЄПГЧИБА
ДОПНХОХИТРШНИАИВЦЮЧЛШЩЗОДЦЦХЧВШЙРАОВКЇЧДШФШПЕАОФУТМЬЖБОРКХЧСЄЄПҐАЧЮШОПАЮЯНЛГФМБЕН
ЮЩНВРНМЯЕВЮЙЄЩОИРБУЮЧШЯІЧЧШГІУУРДТНФЩҐОЕЬШТОГІСҐКЩИЇВГЩШФНХЄКООУАОІТЖГУРПОВОЩВРОУ
РДЬЯЦХВЦРПЯЄІЄЖФГРЖЙФВЛЩЬИЯИУЦЮВННГЧЧКОЙШААЯЮУТОУЦЦЄІЄЖФЩМПЮХВНЩТШЯИКЦЮЮІАДФЧЯВКЧ
НМОІИПСЛЄФБЕУШИХНШИТЗТОТЧШОУХИІОБЮЮКМФХМЬНФИФЄСШУИНБУМШЯЯЇКОНЛГАШІІПЦХЧТЛНИЕЕРММЮ
ОАОЩВЧВКДГЛОТИЕИУПЛЄЖФВРААЄОЛНЮЄДПҐАЧЮЦШДВЮФВПЩСФЄЯЯЮЯҐЕПЖЩҐИЯУИТАЄОЛВБГУЖІОСЦЦШС
ІЄЯВДЩЗСЯЬЙИРТКГЧЬВХГЙРПАЧЖФВПЩСФЄМГМЧНБЖУШЮУҐОЯЧУБЖЮШЯОМҐВТШШРИУЯКЬЮИЩИОУСБЖФЄВО
ЬРТОЕЖЦВГГИМІОДЖ

<u>Завдання 2.</u> Знайти ключове слово за визначеною довжиною і розшифрувати криптограму.

Визначена довжина ключового слова d = 5

2.1 Літери криптограми розподілити на вибірки відповідно до визначеної **довжини ключа d**.

Вибірка 1

ЄЩЕШГОЧРУЕШЙАЩГДНОЯГСГФГЕЮИГУЦЛЮЩДГВЖҐОЄУЩИУАБГЕУЩШЦЯЩЩШУГГГЕВҐДҐРВВШЮЄФШЕРАШЄ
ДШГДОШВШЦШВШАМРЄЧАГНРВОЮЧУНЕГЩЩЄАГВОЯРЄЖЩУНОЯУЄПЩКАВОЛУШОУБФФШУЇГПЛРАВОУФЄЄЧВЩ
ЯПЯЄГСІЩЙГГЧЩГЖҐБОШЯЩБОЕГД

Вибірка 2

ОЬКАВЧЖЖПКХККИІЮТЮЖИШПХШУИХУЗКЩЄЬЮІОУЦИОПТЬОПЙҐУПІПКШХТЦЦШЙШЬЮППШЬЬЗЩПОІСЖПОНО
ЦЄЧОХНЦЩЦЙКФОЬКЄЮЮФЮНЮИЧЧУФЬІИШКОУОУЦПЖЙЬЦГЙЮЦЖЮТЦДКІЄШИТХЮХИУМКАЦНМОКТПВОДЮЮС
ЮЖУОУЦЄЗИЧЙЖСМУОЖМШКИЖЬЖИЖ

Вибірка 3

ЮШЧЛШЯЙХЛЬСХФАШЛХЇЧЙСЛМШЗРШРАЇРФФҐШҐФҐЛСЦИШИЛШМРЛЬІЧМЧИЛЇМЧИЬЇЛҐЗЖЖАШЙУАЇЦЇФШЦ
ЧФИПИИЮЗХРЇШФЖХПШЯМЩМЙРШШРЩШСЇФОІРЩРХЯФФИЮЧШУЦФХШЮФЧИФИТЧИЮМФИШОШХИМЩДИЛРЛПЦФФ
ЯЩИЛЖЦЯСРЬРФФЧШЯЮҐРЬОФРЦМ

Вибірка 4

МБКЄЮВҐЧНУЮКВБПМНЄШВЦЄДГБЙЕТПУБЮНУГННЧШЕЧЯЮПБПБДВВЯБЮМЛТВПВЦЧМГВАЕЕПЮЄГДШУПЧЯЧ
НЄБНТАЧОЧАЧПУБЧҐОНБНЯЄБЯГДҐТҐВНОТПВДВЄГВЯВЧАТЄЩВЯЮЧНПБХЗШІКЬЄНЯНІЧЕЮВГЕЄАНҐШВЄ
ҐҐТВІШВЯТВПВЄНЮЧШВИЮУЄТВІ

Вибірка 5

```
ЧЕКДРМАУВДАКТЬГХВЛДІНЖКІАИКІУСІВКНАВННЯОТИУСАГЕЯВМАЕТТЧІГУГУБЗОКОЮЮВИСРТНЦЕМОГ
МПАХРИЛДВОДЕТОСАПЛЕВЕЩУІІТООКГХУЖОРЬЦІРЛИНКАОІМНИІЯМСЕНТООМНСБЯЛІТЕОЧЛИЖАЮАДПЯ
ЕИАБОСДЬКХАПМБУУЯТУИСВОГО
```

2.2 Застосувати до кожної зі сформованих вибірок частотний аналіз, як для одноалфавітного шифру Цезаря.

Частотний аналіз для ***Вибірки 1***

```
D: 5 + 0
ЄЩЕШГОЧРУЕШЙАЩГДНОЯГСГФГЕЮИГУЦЛЮЩДГВЖҐОЄУЩИУАБГЕУЩШЦЯЩЩШУГГГЕВҐДҐРВВШЮЄФШЕРАШЄДШ
ГДОШВШЦШВШАМРЄЧАГНРВОЮЧУНЕГЩЩЄАГВОЯРЄЖЩУНОЯУЄПЩКАВОЛУШОУБФФШУЇГПЛРАВОУФЄЄЧВЩЯПЯЄ
ГСІЩЙГГЧЩГЖҐБОШЯЩБОЕГД
{'Є': 11, 'Щ': 15, 'Е': 8, 'Ш': 15, 'Г': 21, 'О': 12, 'Ч': 5, 'Р': 7, 'У': 13,
'Й': 2, 'А': 8, 'Д': 6, 'Н': 4, 'Я': 7, 'С': 2, 'Ф': 5, 'Ю': 4, 'И': 2, 'Ц': 3,
'Л': 3, 'В': 11, 'Ж': 3, 'Ґ': 4, 'Б': 4, 'М': 1, 'П': 3, 'К': 1, 'Ї': 1, 'І': 1}
Possibe keys: (18, 3, 19, 26, 1)
```

Частотний аналіз для ***Вибірки 2***

```
D: 5 + 1
ОЬКАВЧЖЖПКХККИІЮТЮЖИШПХШУИХУЗКЩЄЬЮІОУЦИОПТЬОПЙҐУПІПКШХТЦЦШЙШЬЮППШЬЬЗЩПОІСЖПОНОЦЄ
ЧОХНЦЩЦЙКФОЬКЄЮЮФЮНЮИЧЧУФЬІИШКОУОУЦПЖЙЬЦГЙЮЦЖЮТЦДКІЄШИТХЮХИУМКАЦНМОКТПВОДЮЮСЮЖУО
УЦЄЗИЧЙЖСМУОЖМШКИЖЬЖИЖ
{'О': 15, 'Ь': 10, 'К': 13, 'А': 2, 'В': 2, 'Ч': 5, 'Ж': 12, 'П': 12, 'Х': 7,
'И': 11, 'І': 6, 'Ю': 14, 'Т': 6, 'Ш': 9, 'У': 11, 'З': 3, 'Щ': 3, 'Є': 5, 'Ц':
12, 'Й': 6, 'Ґ': 1, 'С': 3, 'Н': 4, 'Ф': 3, 'Г': 1, 'Д': 2, 'М': 4}
Possibe keys: (0, 18, 1, 8, 16)
```

Частотний аналіз для ***Вибірки 3***

D: 5 + 2

ЮШЧЛШЯЙХЛЬСХФАШЛХЇЧЙСЛМШЗРШРАЇРФФҐШҒФҐЛСЦИШИЛШМРЛЬІЧМЧИЛЇМЧИЬЇЛҐЗЖЖАШЙУАЇЦЇФШЦЧФИПИИЮЗХРЇШФЖХПШЯМЩМЙРШШРЩШСЇФОІРЩРХЯФФИЮЧШУЦФХШЮФЧИФИТЧИЮМФИШОШХИМЩДИЛРЛПЦФФЯЩИЛЖЦЯСРЬРФФЧШЯЮҐРЬОФРЦМ

{'Ю': 6, 'Ш': 20, 'Ч': 10, 'Л': 12, 'Я': 6, 'Й': 4, 'Х': 8, 'Ь': 5, 'С': 5, 'Ф': 19, 'А': 4, 'Ї': 8, 'М': 9, 'З': 3, 'Р': 14, 'Ґ': 5, 'Ц': 7, 'И': 15, 'І': 2, 'Ж': 4, 'У': 2, 'П': 3, 'Щ': 5, 'О': 3, 'Т': 1, 'Д': 1}

Possibe keys: (10, 28, 11, 18, 26)

Частотний аналіз для ***Вибірки 4***

D: 5 + 3

МБКЄЮВҐЧНУЮКВБПМНЄШВЦЄДГБЙЕТПУБЮНУГННЧШЕЧЯЮПБПБДВВЯБЮМЛТВПВЦЧМГВАЕЕПЮЄГДШУПЧЯЧНЄБНТАЧОЧАЧПУБЧҐОНБНЯЄБЯГДҐТҐВНОТПВДВЄГВЯВЧАТЄЩВЯЮЧННПБХЗШІКЬЄНЯНІЧЕЮВГЕЄАНҐШВЄҐҐТВІШВЯТВПВЄНЮЧШВИЮУЄТВІ

{'М': 4, 'Б': 12, 'К': 3, 'Є': 13, 'Ю': 10, 'В': 22, 'Ґ': 7, 'Ч': 14, 'Н': 15, 'У': 6, 'П': 11, 'Ш': 7, 'Ц': 2, 'Д': 5, 'Г': 7, 'Й': 1, 'Е': 6, 'Т': 9, 'Я': 9, 'Л': 1, 'А': 5, 'О': 3, 'Щ': 1, 'Х': 1, 'З': 1, 'І': 4, 'Ь': 1, 'И': 1}

Possibe keys: (17, 2, 18, 25, 0)

Частотний аналіз для ***Вибірки 5***

D: 5 + 4

ЧЕКДРМАУВДАКТЬГХВЛДІНЖКІАИКІУСІВКНАВННЯОТИУСАГЕЯВМАЕТТЧІГУГУБЗОКОЮЮВИСРТНЦЕМОГМПАХРИЛДВОДЕТОСАПЛЕВЕЩУІІТООКГХУЖОРЬЦІРЛИНКАОІМНИІЯМСЕНТООМНСБЯЛІТЕОЧЛИЖАЮАДПЯЕИАБОСДЬКХАПМБУУЯТУИСВОГО

{'Ч': 3, 'Е': 10, 'К': 9, 'Д': 7, 'Р': 5, 'М': 8, 'А': 13, 'У': 10, 'В': 9, 'Т': 10, 'Ь': 3, 'Г': 7, 'Х': 4, 'Л': 6, 'І': 11, 'Н': 9, 'Ж': 3, 'И': 9, 'С': 8, 'Я': 6, 'О': 16, 'Б': 4, 'З': 1, 'Ю': 3, 'Ц': 2, 'П': 4, 'Щ': 1}

Possibe keys: (0, 18, 1, 8, 16)

2.3 Визначити ключове слово.

Для цього виписати усі числові значення ключів (*для вибірок 1, 2, . . . , N*) і знайти в алфавіті відповідні їм літери.

Перелік можливих літер на кожні позиції:

```
     О    А    Н    И    В
1. ['О', 'Г', 'П', 'Ц', 'Б']
2. ['А', 'О', 'Б', 'Ж', 'М']
3. ['И', 'Ш', 'І', 'О', 'Ц']
4. ['Н', 'В', 'О', 'Х', 'А']
5. ['А', 'О', 'Б', 'Ж', 'М']
```

Ключове слово:	ОЖИНА

2.4 Розшифрувати криптограму.

ТИСЯЧІТОНЕСЕНЬКИХДУДОЧОКРАПТОМЗАГРАВАЛИУДІДАВСЕРЕДИНІКАШЕЛЬКЛЕКОТІВУНЬОГОВГРУД
ЯХЯКЛАВАУВУЛКАНІДОВГОІГРІЗНОІДУЖЕНЕСКОРОПІСЛЯНАЙВИЩИХНОТКОЛИДІДБУВУЖЕВЕСЬСИНІЙ
ЯККВІТКАКРУЧЕНОГОПАНИЧАВУЛКАНПОЧИНАВДІЯТИІТОДІМИТІКАЛИХТОКУДИАВСЛІДНАМДОВГОЩЕН
ЕСЛИСЯДІДОВІГРОМИІБЛАЖЕННЕКРЕКТІННЯТІКАЮЧИОДДІДОВОГОРЕВУОДНОГОРАЗУСТРИБНУВЯЗПІ
ДПОРІЧОКПРЯМОВТЮТЮНТЮТЮНБУВВИСОКИЙІГУСТИЙПРЕГУСТИЙВІНСАМЕЦВІВВЕЛИКИМИЗОЛОТИМИГ
РОНАМИЯКУПОПАНАРИЗАХАНАДРИЗАМИНОСИЛИСЯБДЖОЛИВИДИМОНЕВИДИМОВЕЛИКЕТЮТЮНОВЕЛИСТЯЗ
РАЗУОБПЛУТАЛОМЕНЕЯУПАВВЗЕЛЕНУГУЩАВИНУЙПОЛІЗПОПІДЛИСТЯМПРОСТОДООГІРКІВВОГІРКАХТ
ЕЖБУЛИБДЖОЛИВОНИПОРАЛИСЬКОЛОЦВІТУІТАКПРУДКОЛІТАЛИДОСОНЯШНИКАДОМАКУЙДОДОМУІТАКЇ
МБУЛОНІКОЛИЩОСКІЛЬКИЯНЕНАМАГАВСЬЯКНЕДРАЖНИВЇХТАКНІОДНАЧОМУСЬМЕНЕЙНЕВКУСИЛААБДЖ
ОЛЯЧЕЖАЛОХОЧІБОЛИТЬЗАТЕВЖЕКОЛИПОЧНЕШПЛАКАТИДІДУЖЕЧИМАТИДАЮТЬЗРАЗУМІДНУКОПІЙКУЯ
КУТРЕБАПРИКЛАДАТИДОБОЛЮЧОГОМІСЦЯТОДІБІЛЬШВИДКОПРОХОДИВАЗАКОПІЙКУМОЖНАБУЛОКУПИТ
ИУМАСІЯАЖЧОТИРИЦУКЕРКИІВЖЕСМАКУВАТИДОСАМОГОВЕЧОРА