МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
Кафедра кібербезпеки

**Дисципліна “Системи та засоби криптоаналізу”**

# Звіт до лабораторної роботи № 5

на тему **“ Дослідження методів криптоаналізу шифру Віженера. Частина 1.”**

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

**Суми 2022**

# ЗВІТ

**Завдання для частини 1 (10 б.)**.

Здійснити **етап 1**: визначити довжину ключового слова за допомогою тесту Казіскі.

Зашифрований текст

ЄОЮМЧЩЬШБЕЕКЧККШАЛЄДГВШЮРОЧЯВМЧЖЙҐАРЖХЧУУПЛНВЕКЬ
УДШХСЮАЙКХККАКФВТЩИАБЬГІШПГДЮЛМХНТХНВОЮЇЄЛЯЖЧШДГ
ИЙВІСШСЦНГПЛЄЖФХМДКГШШГІЕУЗБАЮИРЙИИХШЕКГУРТІУЗАПУЦ
КЇУСЛЩРБІЮЄФЮВЩЬФНКДЮҐУНГІШГАВОҐНВЖУФННҐЦҐЧНОИЛШЯЄ
ОСЕОУПЦЧТЩТИЯИИЬШЮУУОИПСАПЛБАБЙШПГГҐМБЕЕУРДЯУПЛВВ
ЩІЬВМШПІЯАЦКЧБЕЯШМЮТЩХЧМТЩТИЛЧШЦЛТІУЦЇВГГШМПУГЙЧВ
ГГШИЦУЕЬЬЧБВЮЇМЗҐПЛГОДПҐВКҐШЗАОРЬЖЕЮВЬЖЕЮВЗАПВШЩШ
ЮИЮПЙЄСЄОУГРФІАДТШСЇШНЕЖЦУЦРПЇПЕАОФЧМШНШЯОЄОЦЧГДЦ
ЧНМШЄФЄПГЧИБАДОПНХОХИТРШНИАИВЦЮЧЛШЩЗОДЦЦХЧВШЙРА
ОВКЇЧДШФШПЕАОФУТМЬЖБОРКХЧСЄЄПҐАЧЮШОПАЮЯНЛГФМБЕНЮ
ЩНВРНМЯЕВЮЙЄЩОИРБУЮЧШЯІЧЧШГІУУРДТНФЩҐОЕЬШТОГІСҐКЩ
ИЇВГЩШФНХЄКООУАОІТЖГУРПОВОЩВРОУРДЬЯЦХВЦРПЯЄІЄЖФГРЖЙ
ФВЛЩЬИЯИУЦЮВННГЧЧКОЙШААЯЮУТОУЦЦЄІЄЖФЩМПЮХВНЩТШ
ЯИКЦЮЮІАДФЧЯВКЧНМОІИПСЛЄФБЕУШИХНШИТЗТОТЧШОУХИІОБЮ
ЮКМФХМЬНФИФЄСШУИНБУМШЯЯЇКОНЛГАШІПЦХЧТЛНИЕЕРММЮО
АОЩВЧВКДГЛОТИЕИУПЛЄЖФВРААЄОЛНЮЄДПҐАЧЮЦШДВЮФВПЩС
ФЄЯЯЮЯҐЕПЖЩҐИЯУИТАЄОЛВБГУЖІОСЦЦШСІЄЯВДЩЗСЯЬЙИРТКГЧЬ
ВХГЙРПАЧЖФВПЩСФЄМГМЧНБЖУШЮУҐОЯЧУБЖЮШЯОМҐВТШШРИУ
ЯКЬЮИЩИОУСБЖФЄВОЬРТОЕЖЦВГГИМІОДЖ

**Завдання 1.** (10 б.) Визначити довжину ключового слова за допомогою тесту Казіскі.

**Довжина d=4**

1. Сформувати ***Вибірку 1.*** Для цього з криптограми обрати кожен четвертий елемент, починаючи з першого.

D: 4

ЧБЧАГРВЙЖУВУСКАТБШЮНВЄЧИСНЄМШЕАЙШУУУУРЄЩКУШОЖНЧЛ
ОУТЯШОААПМУУВВІКЯТМИЦУГПЧШЕБМЛПҐОЕЖЗШИЄУІШНУЇОШОЧЧ
ЄГАНИНВЛОХЙВДПФЬРСҐШЮГЕНМЮОУЯШУНОТСИЩХОІУВРДХПЄРВ
ИЦНКАУЦЄМВШЦАЯНИЄУНЗЧХБМЬФУУЯНШЦЛЕЮЩКОИЄРОЄАШФСЯ
ЕҐИОГОШЯЗЙКВРЖЩМНШОБЯВРКЩСЄРЖГО

2. Визначити індекс збігу для ***Вибірки 1***.

Таблиця частот літер тексту для довжини **d=4**


```
D: 4
{
 "Ч": 8,
 "Б": 5,
 "А": 9,
 "Г": 6,
 "Р": 9,
 "В": 12,
 "Й": 4,
 "Ж": 5,
 "У": 20,
 "С": 6,
 "К": 7,
 "Т": 4,
 "Ш": 16,
 "Ю": 4,
 "Н": 13,
 "Є": 11,
 "И": 9,
 "М": 8,
 "Е": 6,
 "Щ": 5,
 "О": 16,
 "Л": 4,
 "Я": 8,
 "П": 5,
 "І": 3,
 "Ц": 5,
 "Ґ": 3,
 "З": 3,
 "Ї": 1,
 "Х": 4,
 "Д": 2,
 "Ф": 3,
 "Ь": 2
}
```

## Довжина d=5

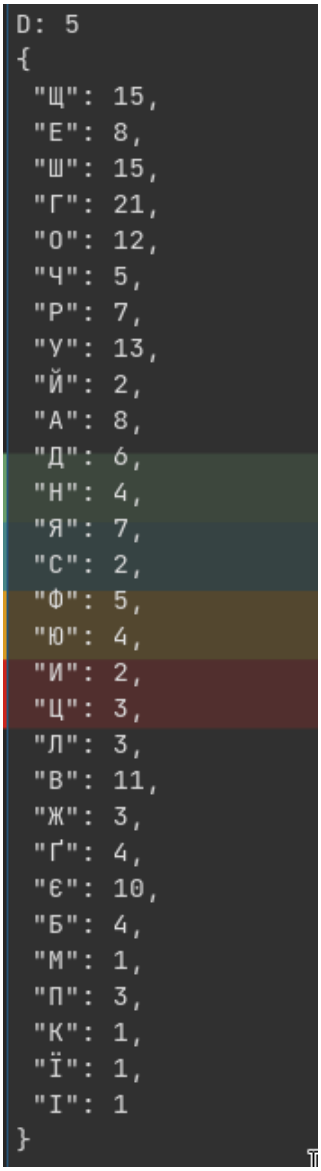
1. Сформувати ***Вибірку 2.*** Для цього з криптограми обрати кожен четвертий елемент, починаючи з першого.

D: 5

ЩЕШГОЧРУЕШЙАЩГДНОЯГСГФГЕЮИГУЦЛЮЩДГВЖҐОЄУЩИУАБГЕУ
ЩШЦЯЩЦШШУГГГЕВІҐДҐРВВШЮЄФШЕРАШЄДШГДОШВШЦШВШАМРЄЧ
АГНРВОЮЧУНЕГЩЦЩЄАГВОЯРЄЖЩУНОЯУЄПЩКАВОЛУШОУБФФШУЇГ
ПЛРАВОУФЄЄЧВЩЯПЯЄГСІЩЙГГЧЩГЖҐБОШЯЩБОЕГД

2. Визначити індекс збігу для ***Вибірки 2***.

Таблиця частот літер тексту для довжини **d=5**



3. Порівняти загальний індекс збігу ***Вибірки 1*** та ***Вибірки 2*** зі значенням $I_{збігу}(x)$ ≈ 0,0575.

*Результат порівняння*:


```
{
 "2": 0.0346851862704878,
 "3": 0.03207850212316561,
 "4": 0.03858407079646017,
 "5": 0.05131982811540823,
 "6": 0.032052980132450316,
 "7": 0.03585271317829458,
 "8": 0.042035398230088485,
 "9": 0.03414141414141415
}
```


Якщо ІЗ ≈ $I_{збігу}(x)$, то довжина ключа d=4. Якщо ця умова не виконується, то обираємо далі довжину ключа 5 і повторюємо усі дії доти, поки ІЗ ≈ $I_{збігу}(x)$.

**Висновок**

Довжина блоку 5 дає найбільш точне значення індексу збігів.

***Результат:***

| | |
|---|---|
| Довжина ключа | d=5 |