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

|  |
| --- |
| ЄОЮМЧЩЬШБЕЕКЧККШАЛЄДГВШЮРОЧЯВМЧЖЙҐАРЖХЧУУПЛНВЕКЬУДШХСЮАЙКХККАКФВТЩИАБЬГІШПГДЮЛМХНТХНВОЮЇЄЛЯЖЧШДГИЙВІСШСЦНГПЛЄЖФХМДКГШШГІЕУЗБАЮИРЙИИХШЕКГУРТІУЗАПУЦКЇУСЛЩРБІЮЄФЮВЩЬФНКДЮҐУНГІШГАВОҐНВЖУФННҐЦҐЧНОИЛШЯЄОСЕОУПЦЧТЩТИЯИИЬШЮУУОИПСАПЛБАБЙШПГГҐМБЕЕУРДЯУПЛВВЩІЬВМШПІЯАЦКЧБЕЯШМЮТЩХЧМТЩТИЛЧШЦЛТІУЦЇВГГШМПУГЙЧВГГШИЦУЕЬЬЧБВЮЇМЗҐПЛГОДПҐВКҐШЗАОРЬЖЕЮВЬЖЕЮВЗАПВШЩШЮИЮПЙЄСЄОУГРФІАДТШСЇШНЕЖЦУЦРПЇПЕАОФЧМШНШЯОЄОЦЧГДЦЧНМШЄФЄПГЧИБАДОПНХОХИТРШНИАИВЦЮЧЛШЩЗОДЦЦХЧВШЙРАОВКЇЧДШФШПЕАОФУТМЬЖБОРКХЧСЄЄПҐАЧЮШОПАЮЯНЛГФМБЕНЮЩНВРНМЯЕВЮЙЄЩОИРБУЮЧШЯІЧЧШГІУУРДТНФЩҐОЕЬШТОГІСҐКЩИЇВГЩШФНХЄКООУАОІТЖГУРПОВОЩВРОУРДЬЯЦХВЦРПЯЄІЄЖФГРЖЙФВЛЩЬИЯИУЦЮВННГЧЧКОЙШААЯЮУТОУЦЦЄІЄЖФЩМПЮХВНЩТШЯИКЦЮЮІАДФЧЯВКЧНМОІИПСЛЄФБЕУШИХНШИТЗТОТЧШОУХИІОБЮЮКМФХМЬНФИФЄСШУИНБУМШЯЯЇКОНЛГАШІІПЦХЧТЛНИЕЕРММЮОАОЩВЧВКДГЛОТИЕИУПЛЄЖФВРААЄОЛНЮЄДПҐАЧЮЦШДВЮФВПЩСФЄЯЯЮЯҐЕПЖЩҐИЯУИТАЄОЛВБГУЖІОСЦЦШСІЄЯВДЩЗСЯЬЙИРТКГЧЬВХГЙРПАЧЖФВПЩСФЄМГМЧНБЖУШЮУҐОЯЧУБЖЮШЯОМҐВТШШРИУЯКЬЮИЩИОУСБЖФЄВОЬРТОЕЖЦВГГИМІОДЖ |

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

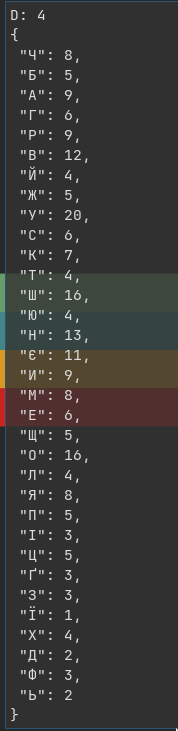
**Довжина d=4**

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

|  |
| --- |
| D: 4  ЧБЧАГРВЙЖУВУСКАТБШЮНВЄЧИСНЄМШЕАЙШУУУУРЄЩКУШОЖНЧЛОУТЯШОААПМУУВВІКЯТМИЦУГПЧШЕБМЛПҐОЕЖЗШИЄУІШНУЇОШОЧЧЄГАНИНВЛОХЙВДПФЬРСҐШЮГЕНМЮОУЯШУНОТСИЩХОІУВРДХПЄРВИЦНКАУЦЄМВШЦАЯНИЄУНЗЧХБМЬФУУЯНШЦЛЕЮЩКОИЄРОЄАШФСЯЕҐИОГОШЯЗЙКВРЖЩМНШОБЯВРКЩСЄРЖГО |

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

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

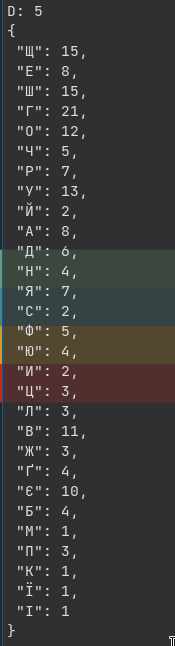


**Довжина d=5**

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

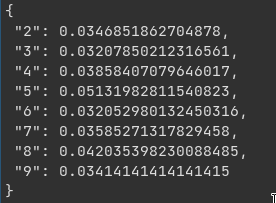
|  |
| --- |
| D: 5  ЩЕШГОЧРУЕШЙАЩГДНОЯГСГФГЕЮИГУЦЛЮЩДГВЖҐОЄУЩИУАБГЕУЩШЦЯЩЩШУГГГЕВҐДҐРВВШЮЄФШЕРАШЄДШГДОШВШЦШВШАМРЄЧАГНРВОЮЧУНЕГЩЩЄАГВОЯРЄЖЩУНОЯУЄПЩКАВОЛУШОУБФФШУЇГПЛРАВОУФЄЄЧВЩЯПЯЄГСІЩЙГГЧЩГЖҐБОШЯЩБОЕГД |

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 *Iзбігу (x) ≈* 0,0575.

*Результат порівняння*:



Якщо ІЗ  Iзбігу(x), то довжина ключа d=4. Якщо ця умова не виконується, то обираємо далі довжину ключа 5 і повторюємо усі дії доти, поки ІЗ  Iзбігу(x).

**Висновок**

Довжина блоку 5 дає найбільш точне значення індексу збігів.

***Результат:***

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