

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

КРИПТОГРАФІЯ
КОМП'ЮТЕРНИЙ ПРАКТИКУМ №2
Криптоаналіз шифру Віженера

Виконали:
Студенти 3 курсу
Остапова О. А.
Литвин М. Р.

Мета роботи

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

Постановка задачі

У даній роботі необхідно реалізувати процес шифрування та криптоаналізу шифру Віженера. Під час виконання роботи потрібно зашифрувати текст за заданими ключами різної довжини, обчислити індекси відповідності для відкритого та шифрованих текстів, а також розшифрувати наданий шифртекст, визначивши його період і ключ.

Варіант 10

Порядок виконання роботи

1. Ознайомитися з теоретичними відомостями про шифр Віженера та методи його криптоаналізу (індекс відповідності та статистика збігів).
2. Підібрати відкритий текст обсягом 2–3 КБ російською мовою без розділових знаків, великих літер і пробілів.
3. Вибрати кілька ключів для шифрування з довжинами:
 - $r = 2$,
 - $r = 3$,
 - $r = 4$,
 - $r = 5$,
 - а також один довгий ключ (10–20 символів).
4. Реалізувати програму для шифрування відкритого тексту шифром Віженера за вибраними ключами.
5. Обчислити індекс відповідності для відкритого тексту та кожного шифртексту. Порівняти отримані значення у вигляді таблиці та діаграми.
6. Виконати криптоаналіз наданого шифртексту (варіант №10):
 - визначити довжину ключа за допомогою індексу відповідності або статистики збігів;
 - знайти значення ключа;
 - розшифрувати текст.
7. Подати результати у вигляді таблиць, графіків і розшифрованого тексту з вказаним ключем.
8. Зробити висновки щодо ефективності застосованих методів криптоаналізу.

Хід роботи

1. Уважно прочитати методичні вказівки до виконання комп'ютерного практикуму.
2. 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:

Первое партнёрство Роберта Ливингстона

Прошло ещё двадцать лет после смерти Фитча и Рамси, прежде чем в США установилось регулярное пароходное сообщение. За это время появились и исчезли ещё несколько изобретателей парохода, пока разработка этого средства передвижения не увенчалась, наконец, успехом, благодаря партнёрству двух людей. Причём первого из них нельзя было даже назвать изобретателем. Это был Роберт Р. Ливингстон, известный, как «Канцлер», поскольку с 1777 по 1801 председательствовал в канцлерском суде Нью-Йорка – высшей юридической инстанции штата того времени. В зарождавшихся Соединённых Штатах он был одним из самых могущественных и влиятельных людей. В наследство ему достались обширные владения по берегам реки Гудзон (изначально дарованные его семье королевским указом в 1680-х), а в те времена землевладение котировалось чрезвычайно высоко. Будучи 28 лет от роду, он выиграл выборы в местный конгресс Нью-Йорка, от которого его направили в Континентальный конгресс в Филадельфию. Там, вместе с Джефферсоном и Адамсом он входил в комитет составителей Декларации независимости США, однако сильнее он повлиял на новую конституцию штата Нью-Йорк, в написании которой участвовал два года спустя.

Ключі:





















```

keys = {
    2: 'до',
    3: 'мир',
    4: 'паро',
    5: 'судак',
    6: 'гудзон',
    7: 'канцлер',
    8: 'континет',
    9: 'деклараци',
    10: 'председате',
    11: 'выборьместо',
    12: 'разработкия',
    13: 'соединенныея',
    14: 'законодательны',
    15: 'управлениеприбл',
    16: 'инстанцияштатаха',
    17: 'передвижениесреда',
    18: 'пароходноесообщени',
    19: 'независимостисюзом',
    20: 'партнерстволюдейтами'
}

```

Результат:

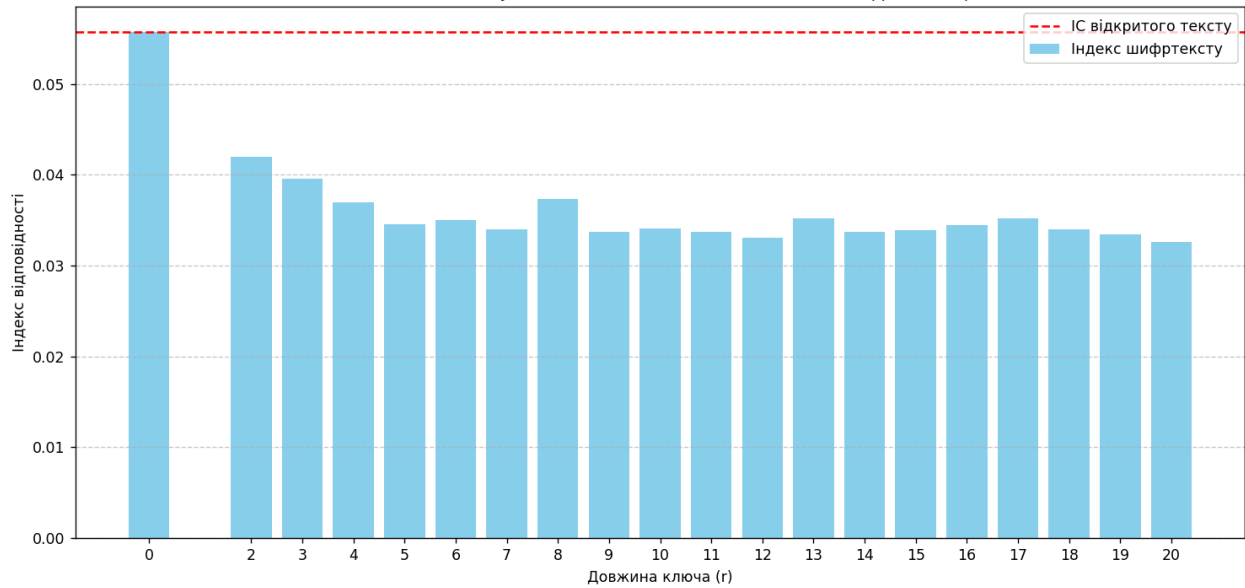
первопартнерствороберталивингстонапрошлоещедвадцатьлетпослесмертифитчаирамспреждечемвсшаустановилосьрегулярноепароходноесообщениезаэто время появились и исчезли несколько изобретателей парохода пока разработка этого средства передвижения не увенчалась на конец успехом благодаря партнерству двух людей причем первого из них нельзя было даже назвать изобретателем это был Роберт Ривингстон известный как канцлер поскольку по предательству в канцлерском суденный оркавсехшей юридической инстанции штата того времени в зарождавшихся соединенных штатах он был одним из самых могущественных и влиятельных людей внаследствие умудостались обширные владения по берегам реки гудзон изначальное дарованное его семьей королевскому указом вавремена землевладения не котировалось чрезвычайно высоко будучи летотроду он выиграл выборы в местный конгрессный орка от которого он направил в континентальный конгресс в филадельфию там вместе с джефферсоном и адомсом он вошел в комитет составителей декларации независимости шоднако сильное влияние на новую конституцию штата нью-йорк в написании которой участвовал два года спустя

Имя	Дата изменения	Тип	Размер
 plaintext	08.10.2025 15:51	Text Document	2 КБ
 vigenere_r2	08.10.2025 15:51	Text Document	2 КБ
 vigenere_r3	08.10.2025 15:51	Text Document	2 КБ
 vigenere_r4	08.10.2025 15:51	Text Document	2 КБ
 vigenere_r5	08.10.2025 15:51	Text Document	2 КБ
 vigenere_r6	08.10.2025 15:47	Text Document	2 КБ
 vigenere_r7	08.10.2025 15:47	Text Document	2 КБ
 vigenere_r8	08.10.2025 15:47	Text Document	2 КБ
 vigenere_r9	08.10.2025 15:47	Text Document	2 КБ
 vigenere_r10	08.10.2025 15:51	Text Document	2 КБ
 vigenere_r11	08.10.2025 15:51	Text Document	2 КБ
 vigenere_r12	08.10.2025 15:51	Text Document	2 КБ
 vigenere_r13	08.10.2025 15:51	Text Document	2 КБ
 vigenere_r14	08.10.2025 15:51	Text Document	2 КБ
 vigenere_r15	08.10.2025 15:51	Text Document	2 КБ
 vigenere_r16	08.10.2025 15:51	Text Document	2 КБ
 vigenere_r17	08.10.2025 15:51	Text Document	2 КБ
 vigenere_r18	08.10.2025 15:51	Text Document	2 КБ
 vigenere_r19	08.10.2025 15:51	Text Document	2 КБ
 vigenere_r20	08.10.2025 15:51	Text Document	2 КБ

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

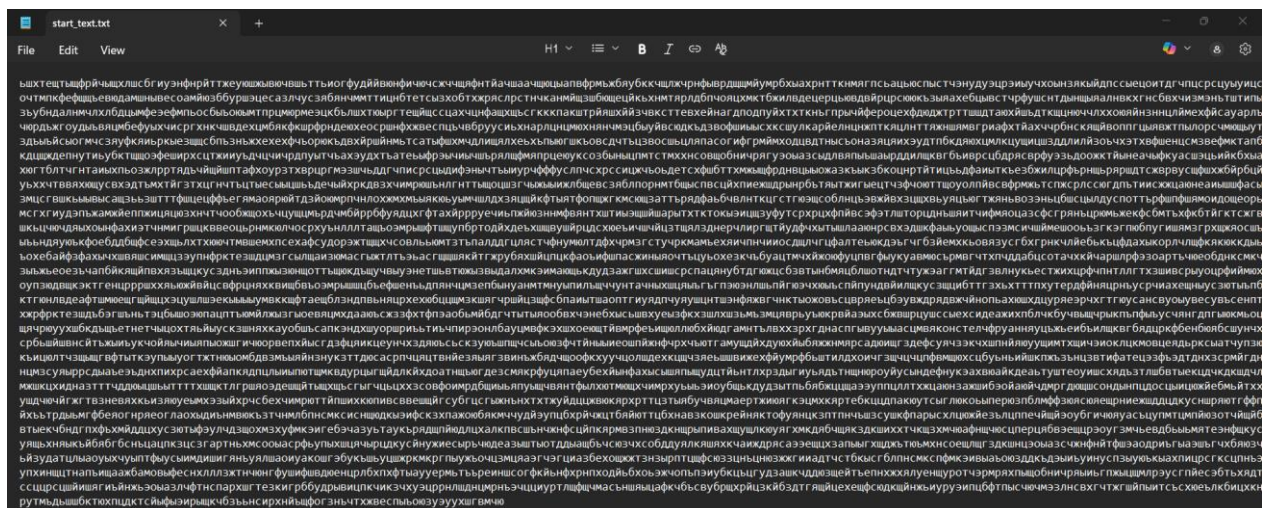
г (довжина ключа)	Ключ	Індекс відповідності
0	відкритий текст	0.05574
2	до	0.041938
3	мир	0.039554
4	паро	0.036957
5	судак	0.034557
6	гудзон	0.034979
7	канцлер	0.033976
8	континет	0.037369
9	деклараци	0.033714
10	председате	0.034044
11	выборьместо	0.03368
12	разработкия	0.033045
13	соединенныея	0.035223
14	законодательны	0.033704
15	управлениеприбл	0.033852
16	инстанцияштатаха	0.034478
17	передвижениесреда	0.035171
18	пароходноесообщени	0.033982
19	независимостисоюзом	0.033423
20	партнерстволюдейтами	0.032601

Залежність індексу відповідності від довжини ключа (шифр Віженера)



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

Наданий текст:



Довжина ключа:

```
--- Аналіз IC ---
Довжина 1: IC = 0.032864
Довжина 2: IC = 0.032878
Довжина 3: IC = 0.035515
Довжина 4: IC = 0.032861
Довжина 5: IC = 0.038953
Довжина 6: IC = 0.035550
Довжина 7: IC = 0.032812
Довжина 8: IC = 0.032864
Довжина 9: IC = 0.035534
Довжина 10: IC = 0.039067
Довжина 11: IC = 0.032882
Довжина 12: IC = 0.035520
Довжина 13: IC = 0.032756
Довжина 14: IC = 0.032723
Довжина 15: IC = 0.054125
Довжина 16: IC = 0.032808
Довжина 17: IC = 0.032849
Довжина 18: IC = 0.035573
Довжина 19: IC = 0.032595
Довжина 20: IC = 0.039074
Довжина 21: IC = 0.035220
Довжина 22: IC = 0.032950
Довжина 23: IC = 0.032954
Довжина 24: IC = 0.035418
Довжина 25: IC = 0.038955
Довжина 26: IC = 0.032851
Довжина 27: IC = 0.035261
Довжина 28: IC = 0.032531
Довжина 29: IC = 0.032564
Довжина 30: IC = 0.054126

=> Найбільш вірогідна довжина ключа (перший пік): 15
```



Отриманий ключ:

```
--- Пошук ключа ---
=> Знайдений набір букв для ключа: крадущийсявтени
```


[illegible]

У ході виконання практикуму було досліджено роботу шифру Віженера та методи його криптоаналізу з використанням частотного аналізу. Особливу увагу приділено застосуванню індексу відповідності та статистики співпадінь символів для визначення довжини ключа. Було проведено експерименти із зашифруванням тексту різними ключами та порівнянням отриманих індексів відповідності, що дозволило простежити закономірність зменшення цього показника зі збільшенням довжини ключа.

На основі отриманих результатів вдалося визначити оптимальну довжину ключа та виконати розшифрування тексту. Відновлений ключ підтвердив правильність обраних методів криптоаналізу. Робота продемонструвала ефективність частотного аналізу для дешифрування поліалфавітних шифрів, зокрема шифру Віженера, та сприяла кращому розумінню його принципів і вразливостей.