НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

“КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ”

ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

Криптографія

КОМП’ЮТЕРНИЙ ПРАКТИКУМ 2

«Криптоаналіз шифру Віженера»

ФБ-32 Дорошенко Ілля

Варіант 6

Мета: Засвоєння методів частотного криптоаналізу. Здобуття навичок роботи та аналізупотокових шифрів гамування адитивного типу на прикладі шифру Віженера.

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 – 6 варіант).

Хід роботи:

Завдання 1:

Для виконання завдання було обрано відкритий текст обсягом 2128 символів. Текст було очищено від сторонніх символів (пробілів, розділових знаків), приведено до нижнього регістру та змінено букву «ё» на «е».

Шифрування Віженера, формула:

$$C_i = (P_i + K_{i \bmod r}) \bmod n$$

Де: C_i — номер зашифрованої літери
n — потужність алфавіту (кількість літер)
(mod n) забезпечує циклічність переходу в межах алфавіту.

Результат шифрування (task1_encrypted.txt):

```
РЕЗУЛЬТАТИ ШИФРУВАННЯ
==================================================

Ключ: да (довжина r=2)
------------------------------
тдсакдявйссоввыахнйбявдлтждроозолаоацажмтсовйндлдтфидрьищпфуиащптяжипихьивдгфакдднмндпйржынилнмхтдйтяйжлйтсювсйрйнакчюуафуеыпмдлйнактгтртсцачпмтдпны
------------------------------

Ключ: три (довжина r=3)
------------------------------
афхтцмнтнгэцртятбхчсгфруацивъцхюптъидркюющьтнярчтвшьршкшэбаыцрэбюзфшуъбдцтихаишфияшхтянвтгышпяшэафндлсфындэжрбнвххоъыряивгйныфтынямтауцвющдрыбшътэун
------------------------------

Ключ: небо (довжина r=4)
------------------------------
ыйооуйьртцоьлзшоютжпизбщылбючудьфелояегъыцлрттбэнчсцнхщцвфсбсецэыдгцшнтксзбсэеэтнтйынфжопакцфтйгыйжаиогщтчомлцхюттэшагроэшвйшсбщттэшыипюыцуоафйантмй
------------------------------

Ключ: экран (довжина r=5)
------------------------------
лоэаубетеюкшовдэыэеошмрлыгкакыашчачэьрвщлыьвтккяаянтрреея ярабкепыьмшлхожфвнаьржсэчшнмпавижтчнхтшфеяшутлтпчокювьхнйзэопннэсышйкыеъщфюгыншбтнрщштнкхл
------------------------------

Ключ: криптография (довжина r=12)
------------------------------
шфхпштютеехнитяпгыисыцикшщияььжюзфтяьркыаянтебиокввшчтюышхгшторэюанешльщыютитвойфабрмкяняфймшзбрфшфнбнчеыежхэибнячыяъутчяъгйкэъгыебдйшуцяаяхругрскэук
------------------------------

Ключ: алгоритмышифрования (довжина r=19)
------------------------------
опроцмноайхворщаюхдбжеоыцшмлвцчюхвкнъявчсяькчщызижацврерфпыцтрэбъъьряшякодпиврлйтрхъщызндтйлифхзхщзувгыожэъбомуеэнмьхцмяивяьууарщзнйтнгщуьбътякаъфэщэ
------------------------------

Ключ: программнаяинженерия (довжина r=20)
------------------------------
эфыгцдзотсмцлиьнцэнактоооюжмьчовцфжпнчрклэбшехнмынтпрнцэхъяштургтюяофширдсиерхрогпэцррпсьпыирфунвуфнскщрохтщклсдштубчшочяягпюыммчтныгыйуэубъявяцхрнчз
```

Завдання 2:

Розрахунок індексу відповідності, формула:

$$I = \frac{\sum_{i=1}^{n} f_i(f_i - 1)}{N(N-1)}$$

Де: f_i — кількість повторів кожної літери в тексті.

N — загальна кількість символів у тексті.

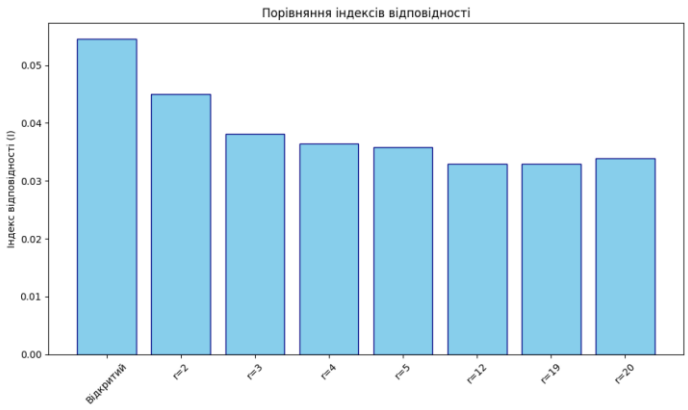
n — кількість літер в алфавіті.

Таблиця:

```
Текст зчитано. Довжина після очищення: 2128 симв.

Тип тексту            | Ключ                | r    | Індекс (I)
-------------------------------------------------------------------
Відкритий текст       | -                   | -    | 0.05454
Шифртекст r=2         | да                  | 2    | 0.04495
Шифртекст r=3         | три                 | 3    | 0.03812
Шифртекст r=4         | небо                | 4    | 0.03639
Шифртекст r=5         | экран               | 5    | 0.03588
Шифртекст r=12        | криптография        | 12   | 0.03288
Шифртекст r=19        | алгоритмышифрования | 19   | 0.03293
Шифртекст r=20        | программнаяинженерия| 20   | 0.03391
```

Діаграма (ic_comparison.png):



Відкритий текст має найвищий індекс відповідності (0.05454), що відповідає статистичним закономірностям природної мови.

Зі збільшенням довжини ключа r, значення індексу стрімко знижується. Це пояснюється тим, що багатоалфавітна заміна «розмиває» частотний розподіл літер.

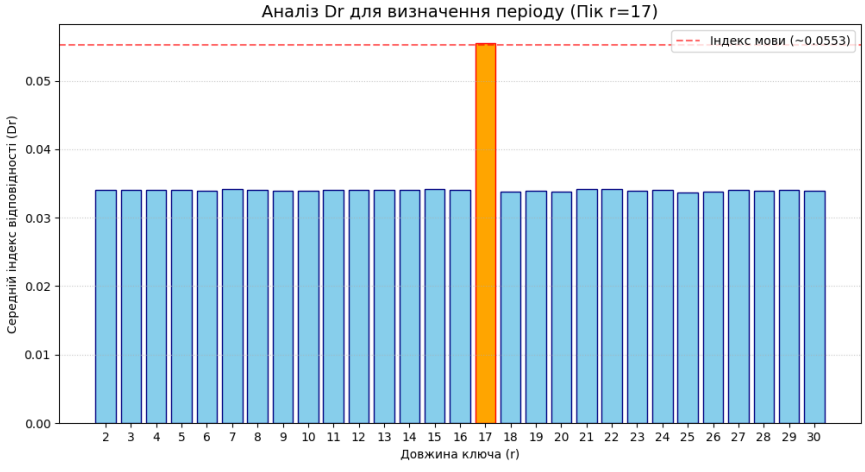
При великих значеннях ключа ($r \geq 12$) індекс наближається до значення 0.031–0.033, що характерно для випадкового тексту. Це свідчить про високу стійкість шифру Віженера до простих статистичних методів аналізу при довгих ключах.

Завдання 3:

Для визначення періоду ключа було використано метод усередненого індексу відповідності для блоків шифртексту при різних значеннях r у діапазоні [2; 30].

- Шифртекст розбивався на r блоків (груп символів), де кожна група складалася з символів, що стоять на позиціях з кроком r.
- Для кожного значення r обчислювався індекс відповідності для кожного блоку окремо, після чого розраховувалося середнє значення D_r.

r	Середній індекс (Dr)
2	0.03406
3	0.03408
4	0.03409
5	0.03412
6	0.03398
7	0.03416
8	0.03403
9	0.03392
10	0.03393
11	0.03401
12	0.03406
13	0.03404
14	0.03408
15	0.03423
16	0.03403
17	0.05551
18	0.03384
19	0.03393
20	0.03380
21	0.03424
22	0.03417
23	0.03394
24	0.03408
25	0.03374
26	0.03386
27	0.03409
28	0.03388
29	0.03408
30	0.03394



На основі проведених розрахунків було виявлено чіткий статистичний пік при r = 17, де значення індексу склало 0,05551. Оскільки це значення максимально наближене до теоретичного індексу відповідності для російської мови (≈ 0,0553), було зроблено висновок, що довжина ключа становить 17 символів.

Після встановлення довжини ключа (r=17) було проведено частотний аналіз кожного з 17-ти «стовпців» шифртексту:

- Для кожної позиції ключа перевірялися всі можливі зсуви в межах алфавіту (32 літери).
- Для кожного зсуву розраховувалася міра близькості (критерій χ^2) отриманого частотного розподілу літер у стовпці до еталонного розподілу обраної мови.
- Найменше значення критерію вказувало на найбільш ймовірний символ ключа на даній позиції.

```
Діаграму збережено: lab2/Doroshenko_fb-32_cp2/task3_dr_chart.png
Знайдений ключ: возвращениеджинна
Результат збережено: lab2/Doroshenko_fb-32_cp2/decrypted_text_var6.txt
```

Використовуючи знайдений ключ та формулу дешифрування Віженера $x_i = (y_i - k_i) \pmod m$, було відновлено відкритий текст.

дорофейльвовичпивторыкобылыниразувжизнинепокидалземлихотяпрожилужебольшешестидесятилетработалпрорабомстроительнойкомпаниидомостройхарьковестолицевкраинылюбилпорыбачитьсдрузьяминаозерахроганьскогокраязачертойгородавыращивалнадачномучасткеовощифруктывоспитывалвнуковавотуезжатьзапределыроднойвкраинынелюбилнесмотрянавозможностивсвязиссозданиемглобальнойсетиметропобыватьналюбойпланетесолнечнойсистемыидажезаеепределамичтоподвиглоегосогласитьсянаэкскурсиюполунеонисамневсостояниибылответитьвероятносыгралисвоюрольрассказыдрузейхваставшихсясвоимипутешествиямииунеговзыгралолюбопытствопосмотретьвблизичтожеэтотакоеспутницаземлиокоторойтакмногоговорятдетивнукиидрузьякакбытонибылоаутромдвадцатьтретьегодекабряаккуратвначалосвятокдорофейльвовичвтайнеотродныхиблизкихпозвонилвбюроэкскурсийсолнечнойсистемызапинаясьобъяснилчегохочетивтотженьспомощьюметродобралсядоаполлонтаунагороданалуneоткудадолжнабыланачатьсяэкскурсияпосамымкрасивымизагадочныместамспутницыземлиаполлонтаунрасполагалсянаравнинеморяспокойствиянедалекоотзнаменитойбороздымаскелайнпохожейнаиизвилистоеруслорекиименноздеськолгатовконцедвадцатоговекасовершилпосадкуамериканскийпилотируемыйкорабльаполлонодиннадцатьаточнееегопосадочныймодульестественноэкскурсантамзанимавшимкабинудвадцатиместногоэкскурсионногофлайтасначалапоказалипамятникаполлонуодиннадцатьпирамидуизлунногобазальтаспосадочнойплатформойиамериканскимфлагомазатемфлайтотправилсявпутешествиепоморюспокойствиязалитомуяркимсолнечнымсветомэкскурсантамиоказалисьмолодыелюдиввозрастеотвосемнадцатидодвадцатилетпоэтомупоначалудорофейльвовичучувствовалсебяневсвоейтарелкесмущаясьподлюбопытнымивзглядамиспутниковнопотомегозахватиласуроваякрасоталунныхпейзажейионпересталобращатьвниманиенавеселящуюсякомпаниюжадноразглядываяпроплывающиеподднищемфлайтациркиэскарпыкратерыиживописныегруппыскалмореспокойствияполучилосвоеназваниенеслучайноегоровнаясглаженнаяповерхностьтипичнадляобширныхморейнадневнойсторонелуныредкорадуетнаблюдателейпроявлениемвулканическойдеятельностиоднакоиздесьимелосьнемалоинтересныхместиобъектовкоторыедесяткилетволновалиастрономовизучающихспутницуземлизагадочнаяцепочкакратеровподназваниемтеннисная ракеткаоколодвухдесятковямокдиаметромотпятидесятидостамет

Повний розшифрований текст було автоматично збережено у файл decrypted_text_var6.txt.

Висновок:

У ході роботи було реалізовано шифрування і дешифрування тексту за допомогою шифру Віженера, а також обчислення індексу відповідності для відкритого та зашифрованих текстів.

У результаті проведених експериментів встановлено, що індекс відповідності відкритого тексту відповідає властивостям природної мови, а зі збільшенням довжини ключа значення індексу відповідності для шифртексту зменшується та наближається до значень, характерних для випадкового тексту. Це підтверджує, що зі збільшенням періоду ключа шифр Віженера стає більш стійким до простих статистичних методів аналізу.

Для зашифрованого тексту варіанту №6 за допомогою методу усередненого індексу відповідності було визначено довжину ключа, яка склала 17 символів. Після цього шляхом частотного аналізу окремих підпослідовностей шифртексту було відновлено ключ

та успішно розшифровано повідомлення, в результаті чого отримано осмислений відкритий текст.