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:

$$C_i = (P_i + K_i) \pmod{n}$$

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)
------------------------------
тдсакдявйссоввыахнйбявдлтждроозолаоацажмтсовйндпдтфидрьищпфуиащптяжипихьивдгфакдднмндпйржынилнмхтдйтяйжлйтсювсйрйнакчюуафуеыпмдлйнактгтртсцачпмтдппы
------------------------------

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

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

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

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

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

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

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.

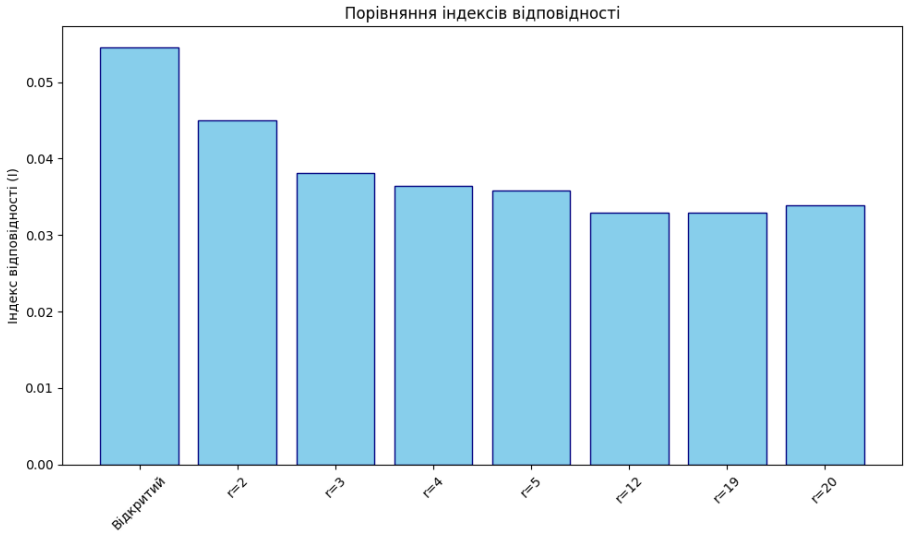
n — кількість літер в алфавіті.

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.