Національний технічний університет України
«Київський політехнічний інститут»
Фізико-технічний інститут

Криптографія

Комп’ютерний практикум №2

Криптоаналіз шифру Віженера

Виконали:

студенти групи ФБ-32

Грабовецький Микита

Драбок Алла

Київ - 2025

Мета роботи:

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

Порядок виконання роботи:

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.

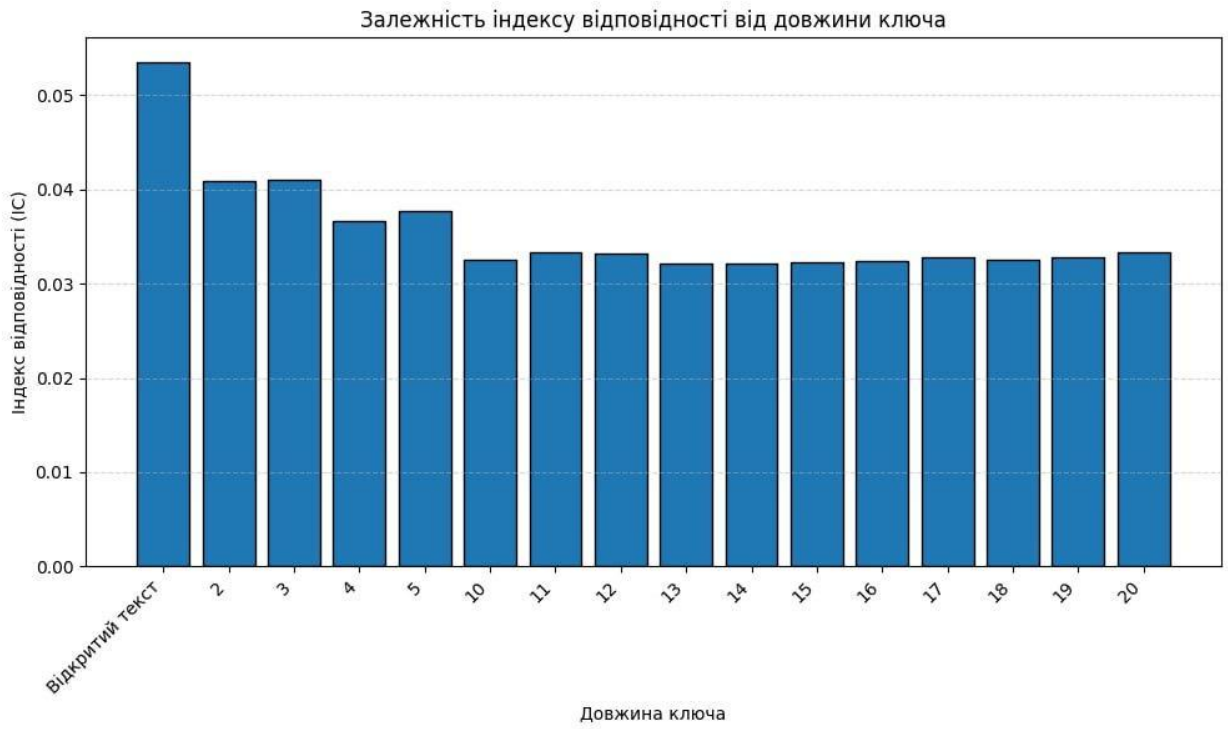
3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта).

Варіант: 13

Хід роботи:

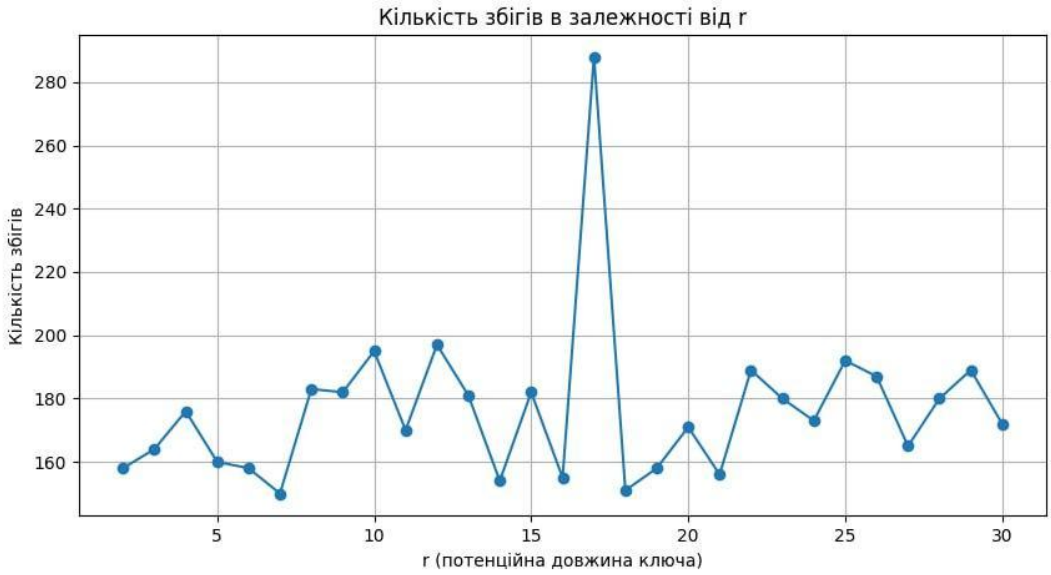
Спочатку ми обрали текст для шифрування та ключі різних довжин. Їх можна побачити на скріні нижче. Далі обчислили індекси відповідності (на скріні IC, бо це з англійською Index of Correlation). Для цього використовували таку формулу:
$I(Y) = (1/n(n-1)) \Sigma t \in ZmNt(Y)(Nt(Y)-1)$

```
Відкритий текст: IC = 0.0534
Довжина ключа = 2, ключ = лу, IC = 0.0409
Довжина ключа = 3, ключ = кот, IC = 0.0410
Довжина ключа = 4, ключ = вода, IC = 0.0366
Довжина ключа = 5, ключ = мирон, IC = 0.0377
Довжина ключа = 10, ключ = шифрування, IC = 0.0325
Довжина ключа = 11, ключ = жсчюгюдщйжвн, IC = 0.0333
Довжина ключа = 12, ключ = фвсжтййярхтцв, IC = 0.0332
Довжина ключа = 13, ключ = ьнтюжвчїфдшг, IC = 0.0322
Довжина ключа = 14, ключ = чїчдшгювпфжцн, IC = 0.0322
Довжина ключа = 15, ключ = взцбщтюпшгжцвн, IC = 0.0322
Довжина ключа = 16, ключ = щфюеупвьйжцїждш, IC = 0.0324
Довжина ключа = 17, ключ = цчфїєгдццчюїзщнжт, IC = 0.0328
Довжина ключа = 18, ключ = зюцлгщчпвжшцждїжтр, IC = 0.0326
Довжина ключа = 19, ключ = гїжювщцшщжвчпцждщєч, IC = 0.0328
Довжина ключа = 20, ключ = шцчгдпюжшщфцждївпцшгр, IC = 0.0333
```



Як бачимо, чим більна довжина ключа, тим нижчий індекс відповідності і тим далі він від значення для відкритого тексту, яке близьке до ІВ російської мови. А отже, чим менше ключ, тим ближче він до значення ІВ для рандомного тексту, де всі літери з’являються з однаковою ймовірністю.

Тепер перейдемо до розшифровки тексту за варіантом. Для початку визначимо, ключ якої довжини використовувався, використовуючи другий метод з нашої методички: обчислення значення статистики співпадінь символів Dr для кожного кандидата на довжину r. Ця статистика підраховує загальну кількість випадків, коли символ у шифротексті збігається з символом, що стоїть на r позицій правіше від нього. Принцип методу полягає в тому, що в шифротексті Віженера однакові символи будуть зустрічатися на відстанях, кратних істинному періоду, значно частіше, ніж на будь-яких інших.Таким чином, ті значення r, які є істинною довжиною ключа (або кратні їй), покажуть більші значення Dr, порівняно з іншими, що й дозволяє ідентифікувати правильний період. Формула: $Dr= \Sigma i=1n-r\delta(yi,yi+r)$.




```
Визначення довжини ключа методом збігів
  r=2: збігів=158
  r=3: збігів=164
  r=4: збігів=176
  r=5: збігів=160
  r=6: збігів=158
  r=7: збігів=150
  r=8: збігів=183
  r=9: збігів=182
  r=10: збігів=195
  r=11: збігів=170
  r=12: збігів=197
  r=13: збігів=181
  r=14: збігів=154
  r=15: збігів=182
  r=16: збігів=155
  r=17: збігів=288
  r=18: збігів=151
  r=19: збігів=158
  r=20: збігів=171
  r=21: збігів=156
  r=22: збігів=189
  r=23: збігів=180
  r=24: збігів=173
  r=25: збігів=192
  r=26: збігів=187
  r=27: збігів=165
  r=28: збігів=180
  r=29: збігів=189
  r=30: збігів=172
Найімовірна довжина ключа: r = 17
```

Отже, проаналізувавши діаграму й таблицю із точними значеннями, можна дуже чітко помітити наскільки виділяється довжина ключа 17. Він нам і потрібен.

Щоб встановити безпосереньо сам ключ (літери у ньому), розбиваємо шифротекст на блоки, де кожен містить літери, зашифровані однією і тією ж літерою ключа. Оскільки кожен такий блок фактично є шифром Цезаря , він зберігає частотні характеристики мови, але зі зсувом. Тож нам і треба знайти оцей зсув. Для кожного блоку послідовно перебираємо всі 32 можливі літери ключа. Для кожної такої літери-кандидата повністю розшифровуємо блок і обчислюємо статистику chi^2. Ця статистика математично "вимірює", наскільки частотний розподіл літер в отриманому розшифрованому тексті відрізняється від еталонного частотного розподілу літер російської мови. Правильною літерою ключа вважається та, яка при розшифруванні дає найменше значення chi^2, оскільки це вказує на найбільшу статистичну схожість із осмисленою мовою.

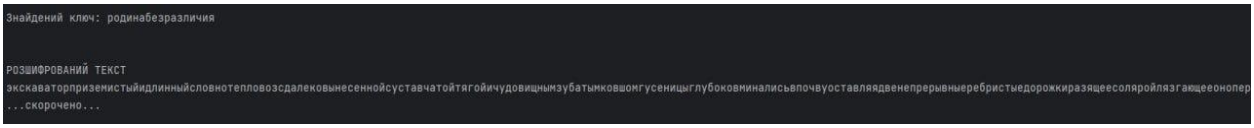
Формула: chi^2= Σi=1m((oi-ei)^2/ei)

oi (Спостережуване) – це фактична кількість кожної літери в блоці.

ei (Очікуване) – це скільки літер мало б бути в осмисленому тексті такої ж довжини.

```
Пошук ключа частотним аналізом

  Аналіз позиції 1/17, блок довжини 315
  Найкраща літера: 'р' (chi²=1045207.75)

  Аналіз позиції 2/17, блок довжини 315
  Найкраща літера: 'о' (chi²=1086172.67)

  Аналіз позиції 3/17, блок довжини 315
  Найкраща літера: 'д' (chi²=1178225.94)

  Аналіз позиції 4/17, блок довжини 315
  Найкраща літера: 'и' (chi²=1169028.55)

  Аналіз позиції 5/17, блок довжини 315
  Найкраща літера: 'н' (chi²=1115368.77)

  Аналіз позиції 6/17, блок довжини 315
  Найкраща літера: 'а' (chi²=1346142.25)

  Аналіз позиції 7/17, блок довжини 315
  Найкраща літера: 'б' (chi²=1262973.03)

  Аналіз позиції 8/17, блок довжини 315
  Найкраща літера: 'е' (chi²=1132203.15)

  Аналіз позиції 9/17, блок довжини 315
  Найкраща літера: 'з' (chi²=1103316.77)

  Аналіз позиції 10/17, блок довжини 315
  Найкраща літера: 'р' (chi²=1301693.98)

  Аналіз позиції 11/17, блок довжини 315
  Найкраща літера: 'а' (chi²=1245828.10)

  Аналіз позиції 12/17, блок довжини 315
  Найкраща літера: 'з' (chi²=1167419.50)

  Аналіз позиції 13/17, блок довжини 315
  Найкраща літера: 'л' (chi²=1234405.02)

  Аналіз позиції 14/17, блок довжини 314
  Найкраща літера: 'и' (chi²=1321789.71)

  Аналіз позиції 15/17, блок довжини 314
  Найкраща літера: 'ч' (chi²=1173715.04)

  Аналіз позиції 16/17, блок довжини 314
  Найкраща літера: 'и' (chi²=1054282.80)

  Аналіз позиції 17/17, блок довжини 314
  Найкраща літера: 'я' (chi²=1227213.92)
```

Як бачимо, вийшов ключ: родинабезразличия



Повністю розшиврований текст:

Висновки:

У ході роботи ми засвоїли практичні методи частотного криптоаналізу шифру Віженера. Спочатку ми дослідили індекс відповідності (ІВ), програмно зашифрувавши текст ключами різної довжини. Ми візуально підтвердили, що чим довший ключ, тим нижчий ІВ шифротексту. Це доводить, що довгий ключ наближає статистику мови до випадкового набору літер і ускладнює аналіз.

Далі ми виконали повний криптоаналіз шифртексту. Для пошуку довжини ключа ми використали метод статистики співпадінь символів (Dr). Цей метод полягає в підрахунку збігів літер на певній відстані r. Отриманий нами графік показав чітко, що пік на r=17, що і було правильною довжиною ключа. Відповідно, знаючи її, ми розбили текст на 17 окремих блоків (шифрів Цезаря). Для знаходження кожної літери ключа ми застосували статистичний метод chi^2. Цей метод перебирає всі 32 можливі зсуви для кожного блоку і знаходить той, що дає розподіл літер, найбільш схожий на еталонну російську мову (де chi^2 — найменше). Таким чином ми знайшли ключ "родинабезразличия" і повністю розшифрували текст.