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
ФБ-32 Баласанян Юліана та
ФБ-32 Дорогін Артем

для першого завдання використала фрагмент тексту з казки , лежить у файлику text1.txt, код у task2.py
залишились лише українські літери, перевели в нижній регістр, замінили “ё” на “е” та “ъ” на “ь”.

список ключів:

```
keys = [
    "но",
    "мир",
    "світл",
    "людина",
    "культура123",
    "українасвітло",
    "традиціїдобро",
    "навколишнєсередовище"[:20]
]
```

функція шифру Віженера:

```
def vigenere_encrypt(text, key):
    alphabet = "абвгґдеєжзиіїйклмнопрстуфхцчшщьюя"
    n = len(alphabet)
    key_indices = [alphabet.index(k) for k in key]
    cipher = ""
    for i, c in enumerate(text):
        ci = (alphabet.index(c) + key_indices[i % len(key)]) % n
        cipher += alphabet[ci]
    return cipher
```

Для кожної букви тексту додаємо індекс відповідної букви ключа. Якщо текст довший за ключ, повторюємо ключ циклічно. Використовуємо модульну арифметику по кількості букв українського алфавіту.

обчислення індексу відповідності:

```
def index_of_coincidence(text):
    alphabet = "абвгґдеєжзиіїйклмнопрстуфхцчшщьюя"
    N = len(text)
    freqs = [text.count(c) for c in alphabet]
    ic = sum(f*(f-1) for f in freqs) / (N*(N-1)) if N > 1 else 0
    return ic
```

IC показує, наскільки текст “структурований” (мовний) чи випадковий. розраховується за формулою:

$$I(Y) = \frac{1}{n(n-1)} \sum_{t \in Z_m} N_t(Y)(N_t(Y)-1),$$

Згенерували ключі всіх потрібних довжин. Зашифрували текст кожним ключем. Порахували IC для відкритого тексту та для кожного шифротексту. Вивели результати для порівняння.

```
ic_plain = index_of_coincidence(text)
print(f"\nIC відкритого тексту: {ic_plain:.4f}\n")

for key in keys:
    cipher = vigenere_encrypt(text, key)
    ic_cipher = index_of_coincidence(cipher)
    print(f"Ключ: {key:20s} | довжина: {len(key):2d} | IC
шифртексту: {ic_cipher:.4f}")
```

Отже, можна зробити висновок, що чим довший ключ, тим надійніше шифрування, бо текст виглядає більш випадковим

далі після підрахунку індексу відповідності для відкритого тексту та всіх одержаних шифротекстів порівнюємо значння, вивиодимо таблицю та будуємо графік:

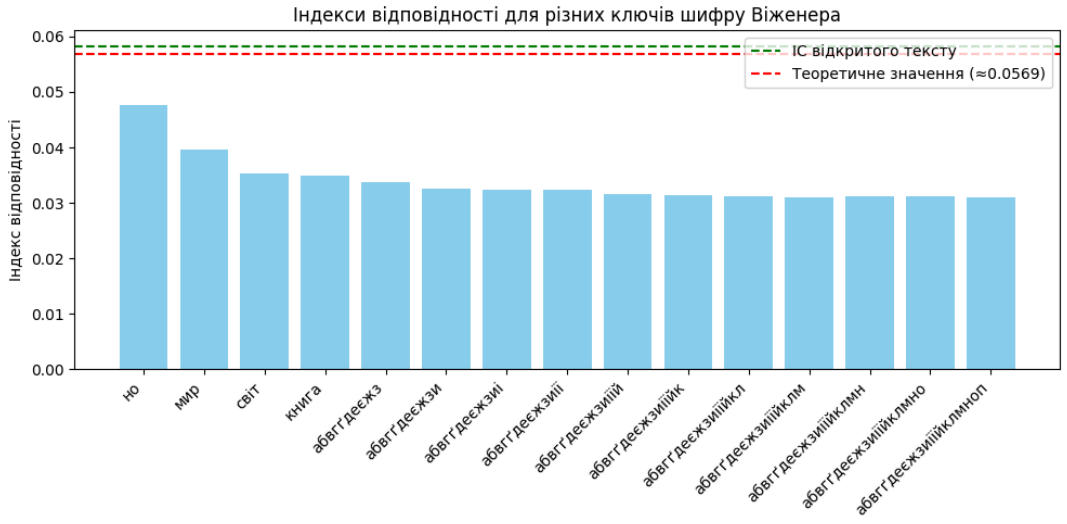
```
ic_plain = index_of_coincidence(text)
print(f"\nIC відкритого тексту: {ic_plain:.4f}\n")

results = []
results.append({"ключ": "відкритий текст", "індекс": ic_plain,
"різниця з ориг.": "-"})

for key in keys:
    clean_key = sanitize_key(key)
    cipher = vigenere_encrypt(text, clean_key)
    ic_cipher = index_of_coincidence(cipher)
    diff = abs(ic_plain - ic_cipher)
    results.append({"ключ": clean_key, "індекс": ic_cipher,
"різниця з ориг.": round(diff, 6)})
    print(f"Ключ: {clean_key:20s} | довжина: {len(clean_key):2d} |
IC: {ic_cipher:.6f}")
```

```
df = pd.DataFrame(results)
print("\nТаблиця індексів відповідності:")
print(df)

plt.figure(figsize=(10,5))
plot_df = df[df["ключ"] != "відкритий текст"]
plt.bar(plot_df["ключ"], plot_df["індекс"], color="skyblue")
plt.axhline(ic_plain, color="green", linestyle="--", label="IC
відкритого тексту")
plt.axhline(0.0569, color="red", linestyle="--", label="Теоретичне
значення (≈0.0569)")
plt.xticks(rotation=45, ha="right")
plt.ylabel("Індекс відповідності")
plt.title("Індекси відповідності для різних ключів шифру
Віженера")
plt.legend()
plt.tight_layout()
plt.show()
```



```
/usr/local/bin/python3.11 /Users/uliannabalasanan/Downloads/BalasanianYu_FB-32_DorohinAr_FB-32_cp2/task1.py
Довжина підготовленого тексту: 2794

IC відкритого тексту: 0.0553

Ключ: но                  | довжина:  2 | IC: 0.045956
Ключ: мир                 | довжина:  3 | IC: 0.040549
Увага: ключ 'світ' був очищений до 'свт' (видалені недопустимі символи).
Ключ: свт                 | довжина:  3 | IC: 0.036972
Ключ: книга               | довжина:  5 | IC: 0.037268
Ключ: абвгдежзий          | довжина: 10 | IC: 0.035937
Ключ: абвгдежзийк         | довжина: 11 | IC: 0.035415
Ключ: абвгдежзийкл        | довжина: 12 | IC: 0.035727
Ключ: абвгдежзийклм       | довжина: 13 | IC: 0.034749
Ключ: абвгдежзийклмн      | довжина: 14 | IC: 0.034253
Ключ: абвгдежзийклмно     | довжина: 15 | IC: 0.034162
Ключ: абвгдежзийклмноп    | довжина: 16 | IC: 0.033615
Ключ: абвгдежзийклмнопр   | довжина: 17 | IC: 0.033209
Ключ: абвгдежзийклмнопрс  | довжина: 18 | IC: 0.033375
Ключ: абвгдежзийклмнопрст | довжина: 19 | IC: 0.032853
Ключ: абвгдежзийклмнопрсту | довжина: 20 | IC: 0.032213
```

Таблиця індексів відповідності:

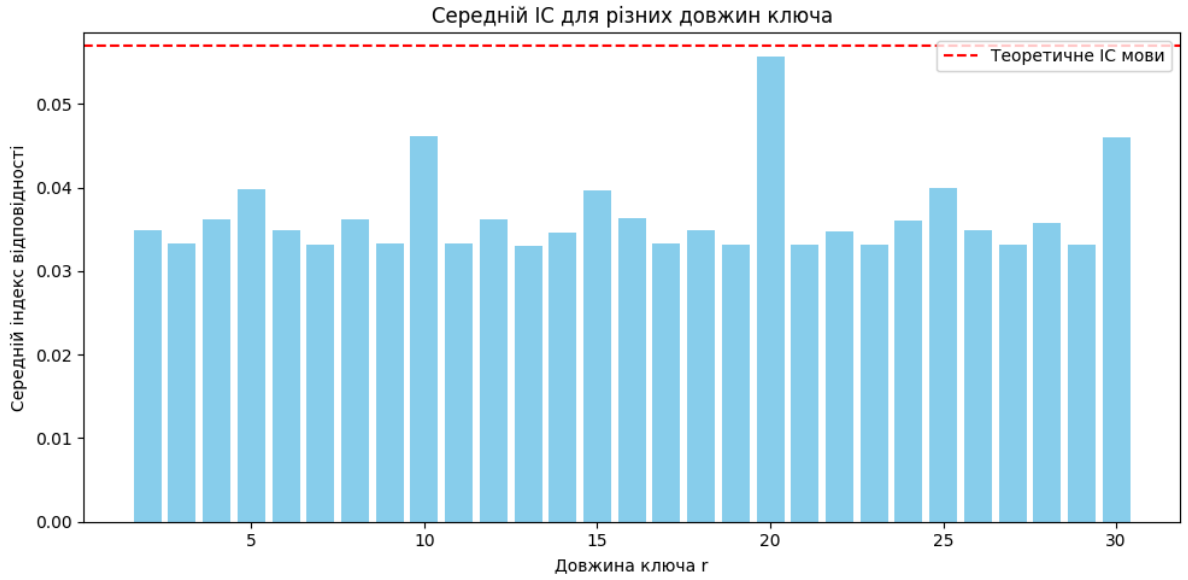
	ключ	індекс	різниця з ориг.
0	відкритий текст	0.055325	-
1	но	0.045956	0.009369
2	мир	0.040549	0.014777
3	свт	0.036972	0.018353
4	книга	0.037268	0.018057
5	абвгдежзий	0.035937	0.019389
6	абвгдежзийк	0.035415	0.01991
7	абвгдежзийкл	0.035727	0.019599
8	абвгдежзийклм	0.034749	0.020577
9	абвгдежзийклмн	0.034253	0.021072
10	абвгдежзийклмно	0.034162	0.021163
11	абвгдежзийклмноп	0.033615	0.02171
12	абвгдежзийклмнопр	0.033209	0.022116
13	абвгдежзийклмнопрс	0.033375	0.021951
14	абвгдежзийклмнопрст	0.032853	0.022473
15	абвгдежзийклмнопрсту	0.032213	0.023112

```
Process finished with exit code 0
```

третє завдання я виконала кодом у файлику [task2.py]

тут для кожної можливої довжини ключа (від 2 до 30) текст ділиться на блоки, і для кожного обчислюється середній IC. Довжина ключа, для якої IC найближчий до теоретичного (≈0.0569), вважається ймовірною довжиною ключа. Для кожного блоку підбирається зсув, який найкраще узгоджується з частотами російських літер. Так формується ключ шифру.Використовуючи знайдений ключ, виконується обернене перетворення Віженера, і отримується відкритий текст. Результат записується у файл `decrypted.txt`.

Відображається стовпчикова діаграма залежності середнього IC від довжини ключа.



розшифрований текст вийшов:

этасистемакрасногокарликаникогданеимеланазванияткольконзубодробитель
нодлинныйномервкаталогеисследовавшийеекиберзондотметилналичиетрехг
азовыхгигантовдвухастероидныхполейкометногооблакаизанесвсеэтиданны
евсекторвторойочередипомнениюинкакиберзондасистеманепредставлялани
какойценностидляпославшихеголюдейнаверноебудьунегозадействованыкон
турывторогоуровнясамостоятельностииазартаонбыпоспорилсамссобойчтов
ближайшуютысячулетлюдиздесьнепоявятсяипроспорилбылюдипоявилисьвэто
йсистеменечерезтысячулетавсеголишьчерезсемьэтобылинетелюдичтопосыл
ализондформальноонивообщенедолжныбылизнатьосуществованииэтойсистем
ыноутехктоихпосылалбылиденьгимногоденегисредипрочегоиххватилонаточ
тобыполучитьвозможностьознакомитьсясрезультатамикартографированияз
аинтересовавшегоихсектораткаксистемепоявилась станциянаскоропередел
аннаяизсписанногогрузовикаитридесяткабуевраннегооповещенияподсвечи
вающихпространствоврадиусепятисветоднейотнеечерезнесколькомесяцевн
астанциюпришелпервыйкорабль этобылстранныйкорабль свидуобычныйдесяти
килотонникотникоторыхлетаюткакповнутреннимаршрутамсолнечнойтакин
авнешниеколониинеобычнымжеегоделалисеребристыеовалынабортахпонимаю
щийчеловеклегкобымогопознатьвэтиховалахтяжелыеизлучателимайерсапре
дставлявшиесобойглавныйкалибркрейсероввксфедерациикорабль былнеодин
другиепохожиенанегоразвдватримесяцазалеталивсистемудатьотдыхкоманд
еимеханизмампровестимелкийремонткоторыйотчеготонемогливыполнитьсоб
ственныесервыкораблявпрочемремонтневсегдабылмелкимодинизкораблейпр
иползнастанциюсперекореженнымбортомоставляяпозадитаюшийсиневатыйсл
едсочащейсяизразбитыхотсековатмосферыонявновстретилкоготоравногопо
силамаможетбойбылнеравныйноэтотктотознаячтопошадынеприходитсяждать
очень старалсяпродать своюжизнь подорожетригодаспустясистемунавестиле
щеодинкиберзондоднакохотяегосканирующиесистемыбылинапорядокмощнееч

емупредшественниказдействоватьихоннесталвместоэтогоновыйгостьтихо
зависнадплоскостьюэклиптикизапределамидосягаемостибуевипринялсявпи
тыватьинформациюшумсолнечноговетратяжелыйрокотгравитационныхволнпл
анетобрывкиразговоровмеждустанциейиочереднымприбывающимкораблемпос
леднееегоинтересовалоособенносильноаещечерезмесяцвсистемепоявились
новыекораблипятьузкихххищныхтенейтотчеловекчтомогбыопознатьсеребрис
тыеовалынаверняказумелбыузнатьихпотомучтомалосчемвовселеннойможно
спутатьизящныйпрофильэсминцавкстипасиранотроевновьприбывшихушливбо
кблокируяточкупереходаадвесеребристыеполоскирванулисьпрямокстанции
гдекакраззаканчивалподготовкукполетуочереднойкорабльтемнотавокругт
ьмаитишинаигдетотамждетнечтоцельмишеньврагоднимсловомточтонадоунич
тожитьсправадонессятихийзвуктолискриптолишорохямгновенноотскочилвс
торонуиокатилподозрительныйучастоквеероногнятихийтрескэтозвуквыстр
еловазвонкиеиглухиехлопкиэтошарикиплазмывимитационномрежимезвонкие
обстенуиглухиевмишеньтеоретическиимиможнобылобытемнотуподсвечивать
нопоусловиямзачетаяопасаюсьдемаскировкипотомуплазмачернаявидетьвин
фракрасномяпоканенаучилсяавотшорохвпередияпрыгалпокомнатесловнопло
хаямарионеткапосылаяновуюочередьпреждечемзатихнетпредыдущаяисчитал
глухиеударыпадающихтелпятьшестьитемнотазначитещектотоосталсяскольк
ожеихгадовсемьиливосемьяполуприселнаклонилсявпередирастопырилрукис
ловновсплывшаяжабаточьвточькаккитаезаченьвоназанятияхрасслабилсяис
лушаешьголосвселеннойсейчасонтебеспоетвухогдепрячетсяпоследняяцель
насамомделеяужедавноубедилсячтоникакимиэкстрапараипрочимисверхспос
обностяминеобладаюноможнопопытатьсякупитьнаэтотфокусоператоракупи
лочереднойшорохдонессяиззаспиныеслибыядействительноловилушамиголос
иззакраямиратутбымнеибылполныйконецзачетанопосколькуязанималсяловл
ейисключительнореальныхзвуковтоупалвпередуспевприэтомизвернутьсяип
рошитьочередьюпространствопередсобойперекатилсяполучивприэтомчувст
вительныйударвпоясницупослалвторуюочередьпримернотудакудаипервуюин
епрекращаяпалитьповелстволвнизнатотслучайеслигадуспелрастянутьсяна
полузачетноеиспытаниеоконченовсемишенипораженывкомнатеначалмедленн
оразгоратьсясветяпопыталсяприподнятьсяполаисразужесхватилсязаушиб
ленныйживотавотнечегопадатьнаоружиеонокакправилотвердоеиребристоен
уикактебекомнатамракаехидноосведомилсяоператормрачнокакмояфамилиян
опоследиснейлендамнеуженичегонестрашнотакужинестрашнокогдатвойлучш
ийдругвылетаетсэкзаменаусловноубитыйпузатойзеленойворонойуженичего
хуженебываетнунуладнокурсантсвободенполучаяназадодеждуяобнаружилчт
опокаяотстреливалкотоввтемнойкомнатенабрикпоступилосообщениеинтере
снооткогоэхвотбыотджейнтретийсвободныйуикэндинескемпровестиобиднов
ольнослушателювукомраковичунемедленноявитьсяналейтстриткполковнику
коринуоппадааэтонеджейнналейтстритразмещалосьместноеотделениеконто
рыкоторуювсесодружествокосоухмыляясьименовалоконторойглубинногобур
енияхотянаэтомзданиивиселатабличкафирмыпоэкспортукокосовыхореховач
утьпоодальпанельрекламыпериодическивыплевывающаянастенусоседнегомо
нодомаслоганкокосыгрузимбыстрооноивидноколонииивсистемебезкокосовых
ореховневыживутвымрутскореечемотвзрывнойдекомпрессиировночередздвад
цатьоднуминутуяробкоподошелкмерцающейдверицельвашеговизитагрознопр
оревеламозаиканадпроемомтонвопросапредполагалчтоприлюбомнеудовлетв

```
орительномответеменяпревратятвоблачкоразогретогопараиподеломпоскол
ькушлятьсяудверейэтойфирмымогуттольколибоеесотрудникилибозлобныеин
омиряненуаеслипопадетсякакойтоэкспортеркококосовбываетнеповезлокурса
нтмраковичкполковникукоринупроблеяляотдушинадеясьчтоинтелктроникан
есочтетдрожьвмоемголосехарактернымдляиномирцевпризнакоммерцающаяза
весаисчезлапроходитеголососталсятакимжерезкиминеприятнымнопокрайне
ймересталнаполтонатишеяосторожноступилнасверкающийполповернитесьли
цомкстенесмотритепередсобойпротянитерукувотверстиеанализсетчаткиид
нкпроверяютилиявсамомделевукомраковичгражданинфедерациидвадцатьпер
вогогодаотродуилинежитькакаякакговориламояпокойнаячешскаябабушкани
когданеслышавшаяпроиномирянследуйтезакраснымсигналомзакакимещекрас
нымсигналомпоинтересовалсяяотворачиваясьотстеныиуставилсянакрасный
огонеквисевшийввоздухепрямопередмоимлицомследуйтезакраснымсигналом
любоеотклонениеотмаршрутасчитаетсянарушениемагашагвсторонупобегпры
жокнаместепровокацияэтоужемойрусскийдедушкавывсехтаквстречаетеилит
олькоменянапоследокпоинтересовалсяядвинувшисьзаогонькомвсехпосторо
ннихпытающихсяпройтичерезслужебныйвходсообщилголостакиоставивменяв
недоумениитолияговорилсвозомнившимосебеинкомтолиссадюгойохранником
```

Висновок:

Під час виконання роботи було досліджено принцип роботи шифру Віженера та методику його розкриття за допомогою індексу відповідності і частотного аналізу. Було проведено аналіз шифрованого тексту російською мовою, обчислено середні індекси відповідності для різних довжин ключа та побудовано графік залежності ІС від довжини ключа. У результаті визначено ймовірну довжину ключа — 20 символів, відновлено сам ключ «улановсеребряныепули» і успішно розшифровано вихідний текст. Під час роботи підтверджено, що індекс відповідності дозволяє ефективно знаходити довжину ключа, а частотний аналіз — підібрати правильний зсув для кожного блоку. Отримані результати демонструють, що шифр Віженера хоч і є складнішим за просту підстановку, проте його можна розкрити при достатньо довгому тексті й статистичних методах аналізу.