Національний технічний університет України

«Київський політехнічний інститут»

Фізико-технічний інститут

Криптографія

Комп'ютерний практикум №2

Криптоаналіз шифру Віженера

Виконали:
ФБ-33 Самохвалов Роман
ФБ-33 Лозенко Павло

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

Частина 1: Шифрування тексту з різними ключами

Для виконання першої частини роботи було обрано текст про історію комп'ютерів українською мовою (розмір: близько 2 кб). Текст було зашифровано шифром Віженера з ключами різних довжин.

Обрані ключі:

r = 2: "на" r = 3: "три" r = 4: "вода" r = 5: "слово" r = 10: "гарніквіти" r = 12: "менезватиден" r = 15: "супермегакрутий" r = 18: "домашнійприступник"

Для шифрування використовувався український алфавіт (33 літери):

"абвгґдеєжзиіїйклмнопрстуфхцчшщьюя".

Частина 2: Обчислення індексів відповідності

Індекс відповідності (IC) обчислювався за формулою:

$$I(Y) = (1/(n(n-1))) \times \Sigma[N_t(Y) \times (N_t(Y) - 1)]$$

де $N_t(Y)$ – кількість появ літери t у тексті Y, n – загальна кількість літер.

Результати обчислень:

```
--- Завдання 1: Шифрування ---
Ключ (r=2): 'на'
Шифротекст збережено у файл: ciphertext_r2.txt

Ключ (r=3): 'три'
Шифротекст збережено у файл: ciphertext_r3.txt

Ключ (r=4): 'вода'
Шифротекст збережено у файл: ciphertext_r4.txt

Ключ (r=5): 'слово'
Шифротекст збережено у файл: ciphertext_r5.txt

Ключ (r=10): 'гарніквіти'
Шифротекст збережено у файл: ciphertext_r10.txt

Ключ (r=12): 'менезватиден'
Шифротекст збережено у файл: ciphertext_r12.txt

Ключ (r=15): 'супермегакрутий'
Шифротекст збережено у файл: ciphertext_r15.txt

Ключ (r=18): 'домашнійприступник'
Шифротекст збережено у файл: ciphertext_r18.txt
```

Аналіз результатів:

Як видно з таблиці, індекс відповідності відкритого тексту (≈ 0.0578) близький до теоретичного значення IC для української мови (≈ 0.057). При збільшенні довжини ключа r значення IC шифротексту монотонно зменшується і наближається до значення для випадкового тексту ($IC_0 = 1/33 \approx 0.0303$).

Це пояснюється тим, що при більшій довжині ключа шифр Віженера краще "маскує" статистичні властивості мови, роблячи розподіл літер більш рівномірним. При $r \to \infty$ шифр Віженера наближається до абсолютно стійкого шифру Вернама.

Частина 3: Криптоаналіз шифртексту за варіантом

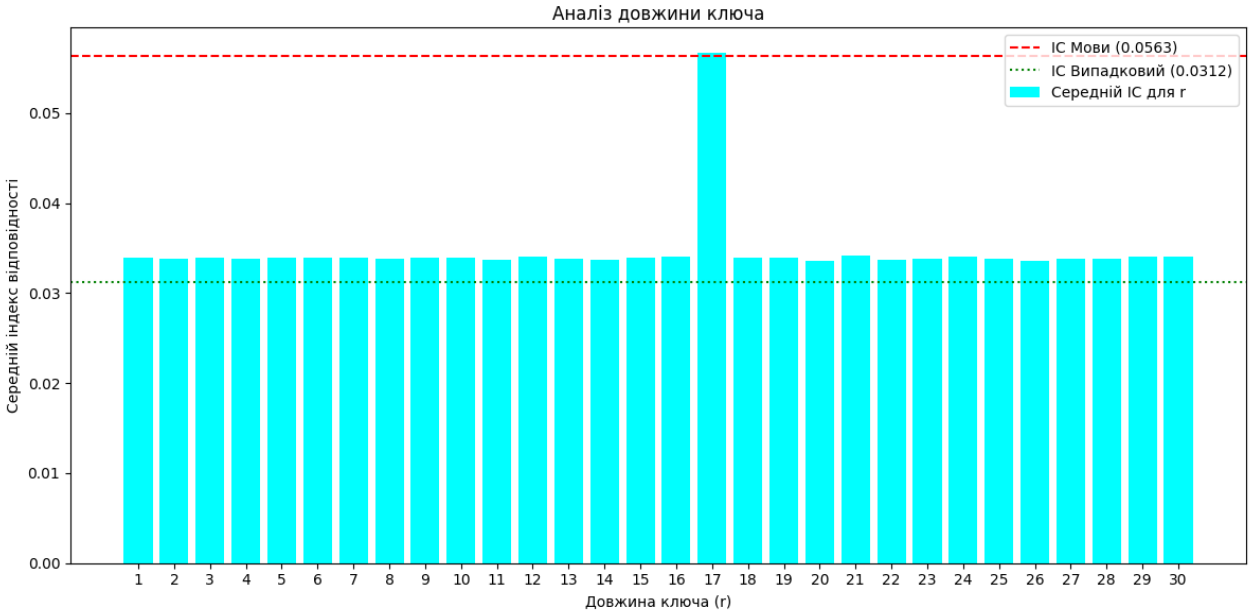
Етап 1: Визначення довжини ключа

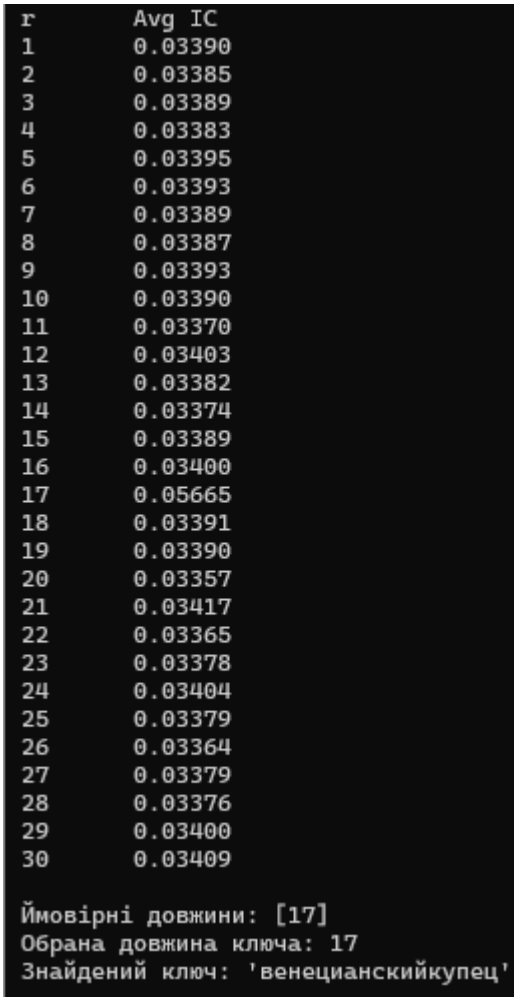
Для визначення довжини ключа використовувався метод обчислення середнього індексу відповідності для блоків при різних значеннях r. Цей метод базується на тому, що при правильному значенні r кожен блок є шифром Цезаря, тому середній IC наближається до IC мови. Альтернативно можна використовувати метод статистики співпадінь символів D, який обчислюється за r
формулою:

$$D = \Sigma(i=1 \text{ to } n-r)\ \delta(y_i, y_{i+r})$$

де δ(a,b) – символ Кронекера (дорівнює 1, якщо a=b, інакше 0).

Результати аналізу довжини ключа (фрагмент):





r	Avg IC
1	0.03390
2	0.03385
3	0.03389
4	0.03383
5	0.03395
6	0.03393
7	0.03389
8	0.03387
9	0.03393
10	0.03390
11	0.03370
12	0.03403
13	0.03382
14	0.03374
15	0.03389
16	0.03400
17	0.05665
18	0.03391
19	0.03390
20	0.03357
21	0.03417
22	0.03365
23	0.03378
24	0.03404
25	0.03379
26	0.03364
27	0.03379
28	0.03376
29	0.03400
30	0.03409

Ймовірні довжини: [17]
Обрана довжина ключа: 17
Знайдений ключ: 'венецианскийкупец'

Як видно з таблиці, значення середнього IC різко зростає при r = 17 та досягає значення близько 0.05665, що дуже близько до теоретичного IC української мови (0.0564).

Етап 2: Знаходження ключа

Після встановлення довжини ключа шифротекст було розбито на 17 блоків, де кожен блок містить літери, зашифровані однією і тією ж літерою ключа. Кожен такий блок є шифром Цезаря.

Для знаходження зсуву кожного блоку використовувався метод хі-квадрат (χ^2):

$$\chi^2_i = \Sigma(i=1 \text{ to } m)\ [(O_i - E_i)^2 / E_i]$$

де O – спостережувана частота літери і в розшифрованому блоці, E – очікувана частота літери і в і української мові.

Для кожного блоку перебиралися всі 32 можливі зсуви, і обирався той, що дає найменше значення χ^2, тобто найкращу відповідність частотному розподілу української мові.

Знайдений ключ: “венецианскийкупец”
Довжина ключа: 17 символів

Етап 3: Розшифрування тексту

Після визначення ключа текст було повністю розшифровано.

початок розшифрованого тексту:

антонионезнаюотчегоятакпечаленмнеэтовтягостьвамяслышутоженогдеягрустьпоймалнашелильдобылчтосоставляетчтородитеехотелбызнатьбессмысленнаягрустьмоявиноючтосамогосебяузнатьмнетрудносаларинovыдухоммечетесьпоокеанугдевашивеличавыесудакакбогатеиивельможиводильпышнаяпроцессияморскаяспрезреньемсмотрятнаторговцевмелкихчтокланяютсянизкоимспочтеньемкогдаонилетятнатканыхкрыльяхсаланиоповерьтееслибятакрисковалп

очтивсечувствабылибтаммоисмоейнадеждойябыпостоянносрывалтравучтобзнатьоткудавете рискалнакартахгаван...

Висновки

У ході виконання комп'ютерного практикуму було досягнуто таких результатів:

1. **Практично засвоєно шифр Віженера:** Реалізовано алгоритм шифрування та дешифрування, який
   підтримує український алфавіт та зберігає регістр літер.
2. **Виконано криптоаналіз шифру Віженера:** Використовуючи метод середнього IC блоків, успішно визначено довжину ключа r = 17. Метод показав чіткий пік на правильному значенні, що свідчить про
   його ефективність.
3. **Застосовано частотний аналіз:** За допомогою статистики χ^2 знайдено всі 17 літер ключа "венецианскийкупец" та повністю розшифровано текст.
4. **Зрозумілі обмеження шифру Віженера:** Шифр Віженера вразливий до частотного криптоаналізу при достатній довжині шифротексту. Навіть при ключі довжиною 17 символів текст було успішно
   розшифровано завдяки статистичним властивостям природної мови.

Робота продемонструвала важливість статистичних методів у криптоаналізі класичних шифрів та підкреслила необхідність використання сучасних криптографічних алгоритмів для забезпечення
надійного захисту інформації.

Додатки

Додаток А: Фрагменти програмного коду

Функція шифрування (task1.py):

```
def vigenere_encrypt(plaintext: str, key: str) -> str:
    """Шифрує текст шифром Віженера, зберігаючи регістр та символи."""
    ciphertext = []
    key_len = len(key)
    key_index = 0
    key_lower = key.lower()

    for char in plaintext:
        if char.lower() in UKR_ALPHABET:
            is_upper = char.isupper()
            p_idx = UKR_ALPHABET.find(char.lower())
            k_char = key_lower[key_index % key_len]
            k_idx = UKR_ALPHABET.find(k_char)

            c_idx = (p_idx + k_idx) % ALPHABET_LEN

            new_char = UKR_ALPHABET[c_idx]
            ciphertext.append(new_char.upper() if is_upper else new_char)
            key_index += 1
        else:
            ciphertext.append(char)

    return "".join(ciphertext)
```

Функція обчислення IC (task1.py):

```
def calculate_ic(text: str) -> float:
    """Розраховує індекс відповідності (IC)."""

    cleaned_text = "".join(char for char in text.lower() if char in
UKR_ALPHABET)
    N = len(cleaned_text)
    if N < 2:
        return 0.0

    counts = Counter(cleaned_text)
    numerator = sum(count * (count - 1) for count in counts.values())
    denominator = N * (N - 1)

    return numerator / denominator
```

Функція знаходження зсуву методом χ^2 (task2.py):

```
def find_shift(col):
    """Знаходить зсув стовпця (атака X^2)."""
    min_chi, best_s = float('inf'), 0
    N = len(col)
    if N == 0: return 0
    for s in range(M):
        chi_sq = 0
        obs = [0] * M
        for c in col:
            obs[(ABC.find(c) - s) % M] += 1
        for i in range(M):
            exp = N * FREQS[i]
            if exp > 0:
                chi_sq += ((obs[i] - exp) ** 2) / exp
        if chi_sq < min_chi:
            min_chi, best_s = chi_sq, s
    return best_s
```

Розшифрований текст :

антонионезнаюотчегоятакпечаленмнеэтовтягостьвамяслышутоженогдеягрустьпоймалнашелильдобылчтосоставл
яетчтородитеехотелбызнатьбессмысленнаягрустьмоявиноючтосамогосебяузнатьмнетрудносалариновыдухоммеч
етесьпоокеанугдевашивеличавыесудакакбогатеиивельможиводильпышнаяпроцессияморскаяспрезреньемсмотрят
наторговцевмелкихчтокланяютсянизкоимспочтеньемкогдаонилетятнатканыхкрыльяхсаланиоповерьтееслибятакр
исковалпочтивсечувствабылибтаммоисмоейнадеждойбыпостоянносрывалтравучтобзнатьоткудаветерискалнака
ртахгаваниибухтылюбойпредметчтомогбынеудачумнепредвещатьменябынесомненновгрустьповергалсалариност
удямойсупдыханьемявлихорадкебыдрожалотмысличтоможетвмореураганнаделатьнемогбывидетьячасовпесочны
хневспомнившиомеляхиорифахпредставилбыкорабльвпескезавязшимглавусклонившимнижечембокачтобцеловат
ьсвоюмогилувцерквисмотрянакамнизданиясвятогокакмогбыяневспомнитьскалопасныхчтохрупкиймойкорабльед
ватолкнуввсепряностирассыпалибывводуиволныоблеклибвмоишелканусловомчтомоебогатствосталоничемимогл
ибяобэтомдуматьнедумаяпритомчтоеслибтаксслучилосьмнепришлосьбызагрустительноговоритезнаюянтониогруст
иттревожасьзасвоитоварыантонионетверьтемнеблагодарюсудьбумойрискнеодномуявверилсуднунеодномуиместу
состояньемоенемеритсятекущимгодомянегрущуиззамоихтоваровсаларинотогдавызначитвлюбленыантониопусто
есаларинонеблюбленытакскажемвыпечальнызатемчтовыневеселыитолькомоглибсмеятьсявытвердяявеселзатемчт
онегрущудвуличныйянусклянусьтобойродитприродастранныхлюдейодниглазеютихохочуткакпопугайуслышавш
ийволынкудругиеженавидкакуксускислытакчтовулыбкезубынепокажутклянисьсамнесторчтозабавнашуткавходят
бассаниолоренцоиграцианосаланиовотблагородныйродичвашбассаниограцианоилоренцоснимпрощайтемывлучш
емобществеоставимвассаларинооставлсябячтобвасразвеселительновотявижутехктовамдорожеантониовмоихглазахце
навамдорогасдаетсямнечтовасделазовутирадывыпредлогуудалитьсясалариноприветвамгосподабассаниосиньоры
нокогдажмыпосмеемсякогдавычтотосталинелюдимысаларинодосугвашмыделитьготовысвамисаларниоисаланиоу
ходятлоренцокбассаниосиньорразвыантонионашлимывасоставимнопрошукобедунепозабытьгдемыдолжнысойтис
ьбассаниопридунаверноградианосиньорантониовидувасплохойпечетесьслишкомвыоблагахмиракторихтрудомчрез
мернымпокупаеттеряетихкакизменилисьвыантониоямирсчитаючемонестьградианомирсценагдеувсякогоестьроль
моягрустнаградианомнеждайтерольшутапускайотсмехабудувесьвморщинахпустьлучшепеченьотвинагоритчемст
ынетсердцеоттяжелыхвздоховзачемжечеловекустеплойкровьюсидетьподобномраморномупредкуспатьнаявуилих
воратьжелтухойотраздраженьяслушайкаантониотебялюблюяговоритвомнелюбовьестьлюдиукоторыхлицапокрыт
ыпленкойточногладьболотаонихранятнарочнонеподвижностьчтобобщаямолваимприписаласерьезностьмудрость
иглубокийумисловноговорятнамяоракулкогдавещаюпустьипеснелаетомойантониознаюятакихчтомудрымислыву
тлишьпотомучтоничегонеговоряттогдакакзаговоривонитерзалибушитемктоихслышаближнихдуракаминазвалбыв
ернодаобэтомпосленонеловитынаприманкугруститкакуюславужалкуюрыбешкупойдемлоренцонупокапрощайапро
поведьякончупообедавлоренцоитаквасоставляемдообедапридетсямнебытьмудрецомтакимбезмолвнымговоритьне
дастградианоградианодапоживисомноюгодадвазвукголосатысвоегозабудешьантонионудлятебяястануболтуномгр
ацианоотличноведьмолчаньехорошовкопченыхязыкахдавчистыхдевахградианоилоренцоуходятантониогдесмысл
вегословахбассаниоградианоговоритбесконечномногопустяковбольшечемктолибоввенецииегорассужденияэтодв
азернапшеницыспрятанныевдвухмерахмякинычтобыихнайтинадоискатьвесьденьанайдешьувидишьчтоиискатьне
стоиловенецияулицавходитланчелотланчелотконечносовестьмояпозволитмнесбежатьотэтогожидамоегохозяинаб
есменятаквотитолкаеттаквотиискушаетговоритгобболанчелотгоббодобрыйланчелотилидобрыйгоббоилидобрыйл
анчелотгоббопустиногивходбегивовсетяжкиеудирайотсюдаасовестьговоритнетпостойчестныйланчелотпостойчес
тныйгоббоиликаквышесказаночестнейшийланчелотгоббонеудирайтопниногойнаэтимыслиладноахрабрыйдьявол
велитмнескладыватьпожиткивпутьговоритбесмаршговоритбесрадибогасоберисьсдухомговоритбесилупиладноас
овестьмоявешаетсянашеюкмоемусердцуимудроговоритмойчестныйдругланчелотведьтысынчестногоотцаилискор

еесынчестнойматерипотомучтосказатьправдуотецтомойнесколькокакбыэтовыразитьсяотдавалчемтобылунегоэта
кийпривкусладносовестьмнеговоритланчелотнешевелисьпошевеливайсяговоритбеснисместаговоритсовестьсовес
тьговорюправильнотысоветуешьеслиповиноватьсясовестинадомнеостатьсяужидамоегохозяинааонтопростименяг
осподисамвродедьяволаачтобыудратьотжидапридетсяповиноватьсялукавомуаведьонтосвашегопозволенияиестьс
амдьяволитоправдачтожидвоплощенныйдьяволипосовестиговорясовестьмояжестокосерднаясовестьеслионамнес
оветуетостатьсяужидабесмнедаетболеедружескийсоветятакиудерудьяволмоипяткиктвоимуслугамудерувходитста
рыйгоббоскорзинкойгоббомолодойсиньорскажитепожалуйстакактутпройтиксиньоружидуланчелотвсторонуонеб
одаэтомойединородныйотецонслептаксловноемунеточтопескомакрупнымгравиемглазазасыпалонеузнаетменясыг
раюснимкакуюнибудьштукугоббопочтеннейшиймолодойсиньорсделайтемилостькакмнепройтиксиньоружидулан
челотаповернитенаправоприпервомповоротеноприсамомпервомповоротеповернитеналеводасмотритепринастоящ
емтоповоротенеповорачивайтенинаправониналевоаворочайтепрямехонькокдомужидагоббосвятыеугодникитрудн
обудетпопастьнанастоящуюдорогувынеможетесказатьмненекийланчелотчтоунегоживетживетунегоилинетланчел
отвыговоритеомолодомсиньореланчелотевсторонувотпогодитекакуюясейчасисториюразведустарикувыговоритео
молодомсиньореланчелотегоббокакойтамсиньорвашамилостьсынбедногочеловекаотецегохотьэтоясамговорючест
ныйнооченьбедныйчеловекхотяблагодарябогаздоровыйланчелотнуктобытамнибылегоотецмыговоримомолодомс
иньореланчелотегоббоознакомомвашеймилостипростоланчелотесударьланчелотнопрошувасстариктобишьумоля
ювассследственновыговоритеомолодомсиньореланчелотегоббооланчелотеспозволениявашеймилостиланчелотсле
дственноосиньореланчелотенеговоритеосиньореланчелотебатюшкамойибоэтотмолодойсиньорсогласноволесудеб
ирокаивсякихтакихученыхвещейвродетрехсестерпарокипрочихотраслейнаукидействительносконча лсяилиеслимо
жновыразитьсяпрощеотошелвлучшиймиргоббогосподиупасидаведьмальчуганбылистиннымпосохоммоейстарост
иистинноймоейподпоройланчелотнеужтожяпохожнапалкуилинабалкунапосохилинаподпоркувыменянеузнаетеба
тюшкагоббоохнетяваснезнаюмолодойсиньорнопрошувасскажитемнеправдучтомоймальчикупокойгосподьегодуш
уживилипомерланчелотнеужтовынеузнаетеменябатюшкагоббоохгореяведьпочтичтоослепнепризнаювасланчелот
нупоправдедажебудьувасглазавпорядкевыитомоглибынеузнатьменяументототецчтоузнаетсобственногоребенкал
адностарикявамвсерасскажупровашегосынастановитсянаколениблагословименяправдадолжнавыйтинасветубийс
твадолгоскрыватьнельзякточейсынэтоскрытьможноновконцеконцовправдавыйдетнаружу