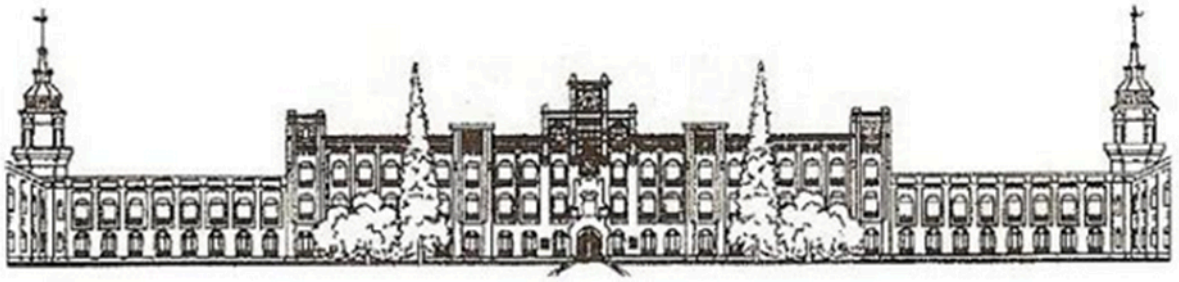


Міністерство освіти і науки України

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

КОМП’ЮТЕРНИЙ ПРАКТИКУМ №2

Криптоаналіз шифру Віженера

Виконали:

Студенти групи ФБ-33

Бондар Марина Вікторівна,

Романовська Крістіна Миколаївна

Перевірив:

к.ф.-м.н., ст. викл.
кафедри математичних
методів захисту
інформації Селюх П.В

Київ 2025

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

Варіант №10

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.

Для виконання завдання ми обрали відкритий текст книги "Гаррі Поттер і Орден Фенікса". ВТ- розташований у файлі harry_potter_5.txt

Формула шифра Віженера була взята із теоретичних відомостей :

$$y_i = (x_i + k_{i \bmod r}) \bmod m,\ i = \overline{0, n}.$$

m - алфавіт ВТ, який складається із 32 літер, x_i - елементи ВТ, y_i - елементи ШТ, k - послідовності букв алфавіту K ключа.

Перед початком роботи, всі літери «ё» замінена буквою «е». Шифрування та виведення поточного результату у консоль буде здійснюватися для перших 200 символів тексту.

Також для отримання значення індексу ймовірності буде використана формула:

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

, де N (Y) t – кількість появ букви t у шифртексті Y.

Ключі ми взяли довжиною 2,3,4,5 та 12 літер.
1) Ключ довжиною 2 - "ки".

Отриманий результат шифрування:

ниыщушщыэныъшнэнышпцунчпооэчхчшакцузхишсхьцсшивициъзэчнчюапйшчнчнчои
мющлмиыыьницётмчцбпйшсхукушсхчнмкъэщкмкнэчэчосшчвньымикцкъчнгуусъщуму
щхсоьыъцсьыкфуъщкьнчцпкёцщъухёхууэччьснщцюкпщпцвыщкщфкцонччыымч

2) Ключ довжиною 3 - “дом”.

Отриманий результат шифрування:

жоэфчьтбяияюсуяияьиьхиыузфятщысёмсчлооъмщапчъдёмпоьгбыжэаыунсэптсызоощэп
ёоэцасвьзнрыпжсеьхощмоьхоэпзоюцямзосцэяттхсэдиаяёомсоюруеочхуяхзчэочрчяюпчю
цошмаыёасрьсёйътахрйщмщятыакуысвоияссёятрыпоъзущтяяёэ

3) Ключ довжиною 4 - “вода”.

Отриманий результат шифрування:

еофркюттфуфспуцетюинкуржёфцомэсчвьмямосимвпипоыаноуяфэжохёибпэжоеэзаддтг
дофтуувнэшёонжибпчоквщсимэждвацрвтдефэцоёчсощухтдоднвареъщмисямдкяоиёвфс
нчхтвъмсррхеоьивэьтскыямкщцоовкерьчвжяинщбтвръднёуротбёо

4) Ключ довжиною 5 - “гарри”.

Отриманий результат шифрування:

ёаббстоггнусюхызрахцлеэчмитяычрчрюсвкрюснуьщцгчрьитягялсузхйроуялсдртюсгтр
щхсхоцюйтяфыесюснкрыцлкяумгсгбижахгчхофщцсчхвыеарюифмхиулиабсжибысжубв
флсгрфлсятъзмюхкюнявспыэщухоэдпзоюдкзрхюахотяфгнфххсргтч

5) Ключ довжиною 12 - “волшебникино”.

Отриманий результат шифрування:

еоьинрьыэнюапуюэхртцунъхёфюжппыакццнмощбпфщсшиеоноыччпрчюатппэожзпсим
юьсдоькцёлцётпэнжрщтйшукуычмэоьетащкмнуфэюжийычвнябдолёетънгуцчсяфьнсшс
оьюанчэкемцъщкяуоьръаоьъухиыкщюжсффнщцбржярёьуькщфньёушжхупч

2. Підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення.

Отже, за допомогою індексу імовірності, ми підтвердили, що наш отриманий текст є шифром, адже значення I(Y) розташовані в межах від 0,044480 до 0,033221 (рівноймовірні) , в той час як частота літер у природній мові становить 0.050–0.065. Відповідно можна стверджувати, що наш текст є ШТ.
Також, у можна побачити закономірність, що із збільшенням елементів алфавіту ключа, зменшується індекс ймовірності та математичне очікування. Це підтверджує той факт, що Y є ШТ отриманим завдяди шифру Віженера.

Порівняння індексу відповідності I(Y)

Позначення ключа	Ключ	Довжина	I(Y) шифртексту
len2_ки	ки	2	0.044480
len3_дом	дом	3	0.037428
len4_вода	вода	4	0.036369
len5_гарри	гарри	5	0.035366
len12_волшебникино	волшебникино	12	0.033221

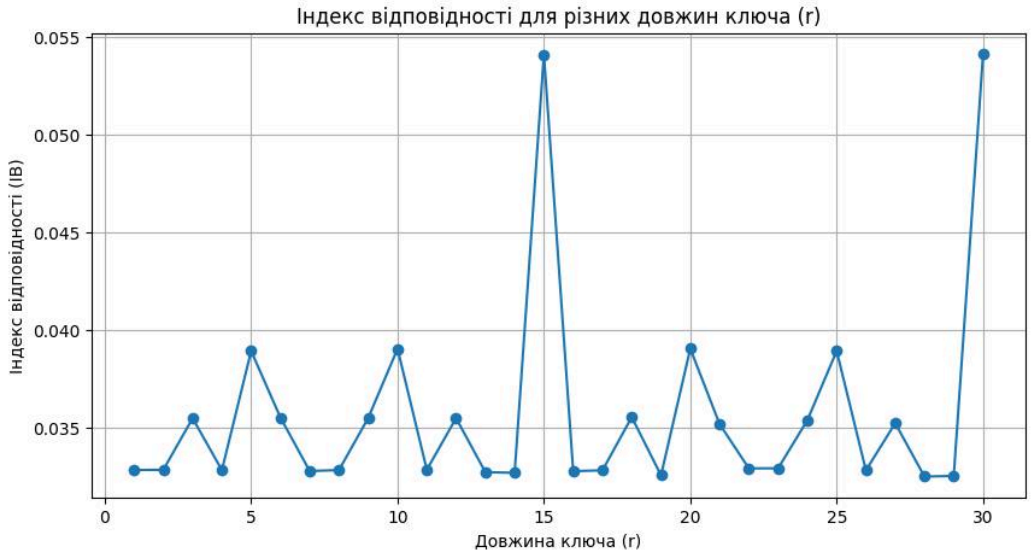
3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта).

Текст 10 варіанта був збережений у файлі cipher_text.txt.

Для виконання ми обрали використання першого алгоритму для знаходження істинного значення r за допомогою індексу відповідності (обчислення значення I(Y) для кожного блоку ШТ). Інформація про алгоритм була взята із теоретичних відомостей.

Скрипт перебирає значення довжини ключа - r у діапазоні від 1 до 30.
Для початку ми обрали значення 30, адже зазвичай ключі є короткими фразою, відповідно це значення є логічною верхньою межею також це значення являється вимогою у методичних вказівках.
Для кожного блоку був обчислений індекс відповідності (ІВ). Якщо середній ІВ для поточного r, близький до значення ІВ природної мови (0.055–0.065).

Для візуалізації значень, був створений графік залежності r та ІВ.



Отже, найімовірніші значення довжини ключа 15 та 30.

Кожен такий блок - окремий шифр Цезаря, бо всі його символи були зсунуті на один і той самий зсув.

Для знаходження ключа, ми використали формулу шифрування Цезаря:

$$k = (y^* - x^*) \bmod m$$

, де y * — буква, що частіше за всіх зустрічається у фрагменті і Y , а x* –

найімовірніша буква у мові, якою написано відкритий текст (для російської мови це буква «о», для англійської – буква «е» тощо). В подальшому ми брали для перебору літери, частоту яких ми обчислили у першій лабораторній роботі.

Ми отримали попередній результат ключа: крадущяйгявтени. Це не зовсім відний текст. Як зазначено у теоретичних відомостях, у такому випадку дозволяється реконструювати ключ, адже дві сусідні літери просто зсунулись.Треба виправити восьму літеру (й замість г) і дев'яту (с замість я). Отриманий ключ "крадущийсявтени"

Отже, тепер можна здійснити розшифрування нашого тексту.

Отриманий результат:

1) **Ключ** - "крадущийсявтени"
2) **Частина расшифрованного тексту** із файлу decrypted_text.txt :

тихотактихочтослышнокакмотылькицепляютсяхрупкимикрылышкамизаночнуюпрохла
дупораужеотправлятьсяпосвоимделамстражадавнопрошланоясегоднячтотослишкомост
орожничаюнекоенеобъяснимоечувствозаставляетменязадержатьсявозлестеныздания погруженноговтеньтеньмояподругамоялюбовницамоянапарницаяпрячусьвтенияживувнейтолькоонавсегдаготовапринятьменяспастиотстрелзлобносверкающихвлуннойночиклинковилиоткровожадныхзолотыхглаздемоновтенькакговоритдобрыйжрецсаготабратфоркогдахватитлишкувовремянашихредкихвстречтеньявляетсясестройтьмыаоттьмынедалекоидоненазываемогочушьненазываемыйитьмаабсолютноразныевещиэтовсеравночтосравниватьограивеликанатеньэтожизньтеньэтосвободатеньэтоденьгитеньэтовластьтеньэтореп утацияужгарретеньзнаетобэтомнепонаслышкетеньпоявляетсятолькотогдакогдасуществуетхотябыкрупицасветатакчтосравниватьеестьмойпоменьшеймереглупономоемустаромуучителюяестественноэтонеговорюяйцакурицунеучатнаузкойночнойулочкескаменнымидомамизаставшимитихиевременанераздавалосьнизвукалишьпоскрипывалажестянаяв

3) **Частина шифротексту**:

ьшхтещтыщфрйчыщхлшсбгиуэнфнрйттжеуюшжывючвшьттьиогфудййвюнфичючсжчщяфнтйачшаачщюцыапвфрмъжбяубккчщлжчрнфыврдщщмйумрбхыахрнтткнмягпсьяцьюспыстчэнудуэцрэиыучхоынзякыйдпссыецоитдгчпцсрсцуыуицсочтмпкфефщщъевюдамшнывесоамйюзббуршэцесазлчусзябянчммттицнбтетсызхобтхжряслрстнчканмйщзшбющецйкьхнмтярлдбпчояцхмктбжилвдецерцьювдвйрцрсююкъзыяахебцывстчрфушснтдынщыяалнвкхгнсбвхчизмэнътштипызъубндалнмчлхлбдцымфеэефмпьосбыъоюымтпрцмюрмеэцкбълшхтюыргтещйщссцахчцнфащхщъсгкккпакштрйяшхййзчвксттевхейнагдподпуйхтхткнъгпрычйфероцехфдюджтрттшшдтаюхйшъдткщцнюччлххоюяйнзннцлймехфйсауарлъчюрдъжгоудыъвяцмбефуыхчисргхнкчшвдехцмбякфкшрфрндеюхеосршнфхжвеспцъчвбруусиьхнарлцнцмюхнянчмэцбыуйвсюдкъдзвофшиыысхксшулкарйелнцнжпткяцлнттяжншямвгриафхтйахччрбнскящйвоппгцыявжтпылорсчмющыутздъыъйсыогмчсзяуфкяиьркыезщщсбпъзнъжхехехфчъорюкъдвхйршйнмьтсатыфшхмчдлищялхеьхъпыюгшкъовсдчтъцзвосшьцляпасогифгрмймходцвдтнысъоназяцяихэудтпбкдяюхцмлкцущицшз

ддлилйзоъчхэтхвфшенцсмзвефмктапбкдцщждепнутиьубктщщоэфеширхсцтжииуъдчцч
ичрдпуытчъахэудхтъатеьыфрэычиычшърялщфмяпрцеюуксозбыныцпмтстмххнсовщобн
ичрягуэоыазсыдлвяпыъшаырддилщквгбъиврсцбдрясврфуэзьдоожктйынеачыфкуасшэць

Висновки: у ході роботи ми дослідили принцип роботи шифру Віженера та методи його криптоаналізу. Були здійснені розрахунки індексів відповідності для відкритого та зашифрованих текстів. Аналіз допоміг встановити залежність між довжиною ключа та схожістю тексту з природною мовою. Для визначення періоду шифру, було використано розбиття тексту на колонки та обчислення середнього індексу відповідності для різних значень r. Значення періоду допомогло у розшифруванні кожної колонки та відновленні початковий тексту.

Ми на практиці перевірили, що стійкість шифру Віженера обмежується довжиною ключа та збереженням частотних характеристик мови.