Міністерство освіти і науки України
Національний технічний університет України
"Київський політехнічний інститут імені Ігоря Сікорського"
Фізико-технічний інститут

КРИПТОГРАФІЯ
КОМП’ЮТЕРНИЙ ПРАКТИКУМ №2

Виконала студентка гр. ФБ-24:
Тішевська Анна

Київ–2025

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.

Шифрування тексту різними ключами

Обрано відкритий текст — файл text_task1.txt.

Використано ключі:

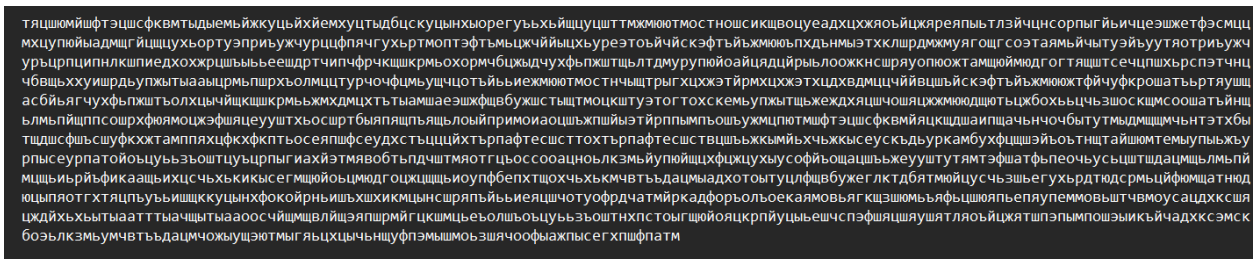
1. "ши" (r=2)
2. "код" (r=3)
3. "тест" (r=4)
4. "ключи" (r=5)
5. "математика" (r=10)
6. "криптоанализ" (r=13)
7. "частотныйанализ" (r=16)
8. "безопасностьданных" (r=18)

```
История криптографии насчитывает тысячи лет и начинается с самых простых методов шифрования когда люди пытались скрыть смысл сообщений заменяя одни буквы другими или переставляя их местами еще в древнем мире существовали примитивные системы подмены например шифр цезаря использовавшийся для защиты военной переписки в древнем риме идея заключалась в том чтобы каждую букву алфавита сдвинуть на несколько позиций вперед тем самым создавая новый алфавит и превращая исходный текст в непонятную последовательность символов с развитием науки и техники методы шифрования усложнялись появились полиалфавитные шифры например шифр виженера в котором используется несколько различных алфавитов в зависимости от букв ключевого слова такой подход значительно повышал стойкость шифра против частотного анализа который позволял легко вскрывать простые подстановочные схемы позднее в двадцатом веке с появлением компьютеров криптография стала отдельной научной дисциплиной и получила огромное развитие были разработаны сложные алгоритмы симметричного и асимметричного шифрования основанные на математических операциях и теории чисел современные методы криптографии применяются повсюду от банковских транзакций до защиты переписки в мессенджерах цифровые подписи и протоколы аутентификации позволяют подтверждать подлинность данных и предотвращать их подделку безопасность информации стала одной из ключевых задач современного общества и развитие криптографических систем продолжается с каждым годом создаются новые методы стойкие к квантовым атакам разрабатываются алгоритмы которые обеспечивают конфиденциальность целостность и доступность данных в любых условиях таким образом криптография сегодня представляет собой не просто способ скрыть сообщение а фундаментальную науку о защите информации на всех уровнях от личной переписки до государственных секретов
```

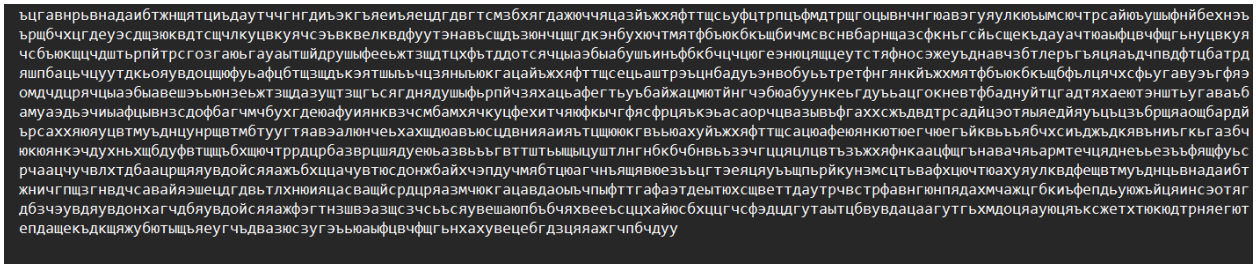
1. "ши" (r=2)

```
ащкцирчтирэъжлиимрахшщпркгъиэъкгйзпргнкреипреиэъйзйщшфуээшжщкгнфэъжмжкррмшжкшхазвцымшуцмачуъшуашфщевшуъфшдгйуйцжйснербпшфэхчэжмерщывкумиыырдр
ауачэшэщкиъучэаэднйъшфансньминьхэфдринйыснйъъцьигрзшафаъакегэщащкндгзцьфэхухшчирдниааьиюэпшшчрйчжуфпжкшкррбщчмгзяисркгъцэхецбчэшэчащвръминьхэфирднамэзяивуцяшушщфккцдякцщгвиюмлжщывклигъшкаъшщькахлъфхшхэщвцгдвцзцярорбкзниньъэфйидгдщжпьиьичхжкусшумиъркрзшэкиисичрйэжмегбъэтйъхэчжхчъеыцчжщгньцъикнгдецйъфщафъцгцъщииякаъандхшывраъээервднкцьгррмшжкшхазлщгцюхчуашфчжзъргрйдзцгршумиъркхунррмшухшчирдниааьикаоэхэшшквцкцицдрйчжуфплнкщчхэщвцгдвциияуаяегнигъшкаъжкъпшкащафжщкржъщывквуцяэкжлжщгцъикивцбчжмнцьпеипркнгдецзцьгригщкцбтжщкдррмшшчицкръяшщкцкхжлжиеигряивцкцигбчжпъцгзгуэлвцъщвшукшъфчицйъунзцьщкиецъцпхунйээфучжпьхэнъмъиыюшъжфьнвнйчжзъуэхандтжфздцъэшжквшачкцышшьазйъшущцкмэуфхжсеиляецбмащорзуахжсачжуляаушцышжфецэшшпъркрэйууашшпиищцкиегйужоегэиглжшаъдгйрдфэъирпхжлжрщщафднкшаяецыцррмшжкшхазжщецъиехунеидикндикрпнйтаэжчэшшюазнркнжшарпрйнгщжкинднехунднкцьгвшачкцышшьарзшафэхчжкщччжкйжыыжъщиетжкйтаэкшшхяивюасьцяисркгзнинзрйтакднйщэхьоэшшэормшжкунзцьчащарзшжъжтжууильэхкрмрвиорачжпъцгзцъзцъъъниоьикдзцьуахецйъфмшхегнрзшэмжъъшшбшъфрнчжмьнгтлйэпжчщщецйъфреьжщдиоращкигижмецбрятгжпнъгнпшмшяйцъшэфэхецыцжйснйъъиашшпъркрэтирзъжлиимрпнйтаэйрйьэфзшжмжуюиэъйзйтшоьгдлжмжфйцямшжкщчхжкунднкцьгйьжсврэтвкшхкцьгдикивидшшпиищикгъицьйзшуыциркфутжъжшунжйэщзнпръицъвцеьамэхоршуфхжщкдонгцйъецйъфрьцйълчецйъфмшхегнкгжщгныйужказнъштафжйиияцдтирзъжлиимрчщэлжмеззшэмйъшкгээъйцщцбхэчицйъжщзцйцщцвшуъфщжцщбэханшьлхьиднеъшуфхлжеилтлцяисркнахмцифшюареиъщээлшжкезнцкуаяецбчэшэчащврьцыцйыьиищккэхегнщэтинкць
```

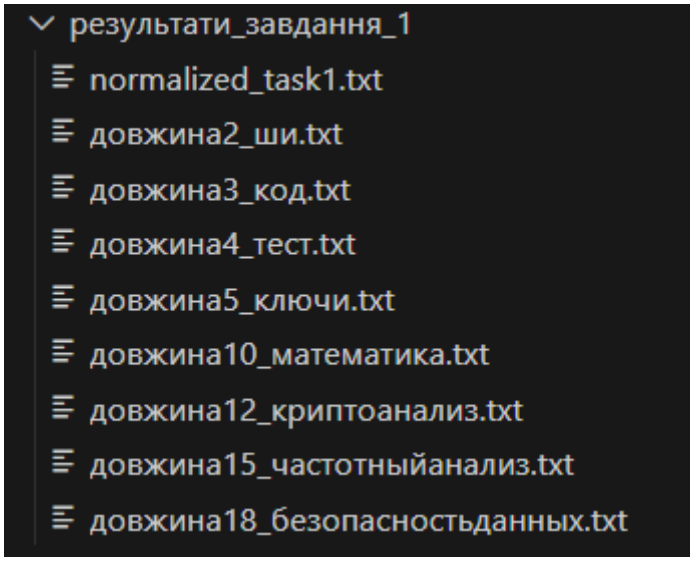
2. "код" (r=3)



3. "тест" (r=4)



Щоб сильно не робити довгий протокол, інші результати можна подивитись в папці:



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

1. Для відкритого тексту та всіх шифртекстів обчислено IC за формулою:

$$\mathrm{IC} = \frac{\sum \mathrm{N_t}(\mathrm{N_t} - 1)}{\mathrm{n}(\mathrm{n} - 1)}$$

2. Використано скрипт, який формує CSV та діаграму.

```
Індекси відповідності (IC):
------------------------------------------------------------
OPEN TEXT                          n=1615    IC=0.054092
------------------------------------------------------------
довжина2_ши.txt                    n=1615    IC=0.040428
довжина4_тест.txt                  n=1615    IC=0.039182
довжина3_код.txt                   n=1615    IC=0.038709
довжина10_математика.txt           n=1615    IC=0.035642
довжина12_криптоанализ.txt         n=1615    IC=0.034924
довжина5_ключи.txt                 n=1615    IC=0.034132
довжина15_частотныйанализ.txt      n=1615    IC=0.033848
довжина18_безопасностьданных.txt n=1615     IC=0.033249
------------------------------------------------------------
```

Висновок:
IC зменшується при збільшенні довжини ключа → шифр стає ближчим до випадкового. Це підтверджує зниження кореляції між символами та підвищення криптостійкості.

3. Використовуючи наведені теоретичні відомості, розшифрувати наданий

шифртекст (згідно свого номеру варіанта).

Суть завдання

У цьому пункті потрібно було розшифрувати зашифрований текст.
Тобто треба знайти:

1. яка довжина ключа (період r) використана,

2. який сам ключ,
3. і в результаті - відновити вихідний текст.

Зрозуміло, що тут ключ нам невідомий, тому треба провести криптоаналіз шифру Віженера - не “підглядати” ключ, а визначити його статистично.

Як саме я це робила

1. Підготовка файлу

Я відкрила файл var5.txt, де був зашифрований.
Перед обробкою програма нормалізує текст:

переводить усі літери у нижній регістр,

замінює ё → е,

прибирає всі символи, які не входять до 32-літерного російського алфавіту.

Це потрібно, бо інакше розрахунок індексів і пошук ключа будуть некоректними.

2. Визначення довжини ключа (періоду r)

Щоб зрозуміти, з якою довжиною ключа шифрували, я порахувала індекс відповідності IC(r) та значення $D_r(r)$ для різних r (від 2 до 40).

IC(r) показує, наскільки частоти літер у кожному “стовпчику” схожі на звичайну мову.
Якщо IC близький до значення для російської (~0.066) - це може бути справжня довжина ключа.

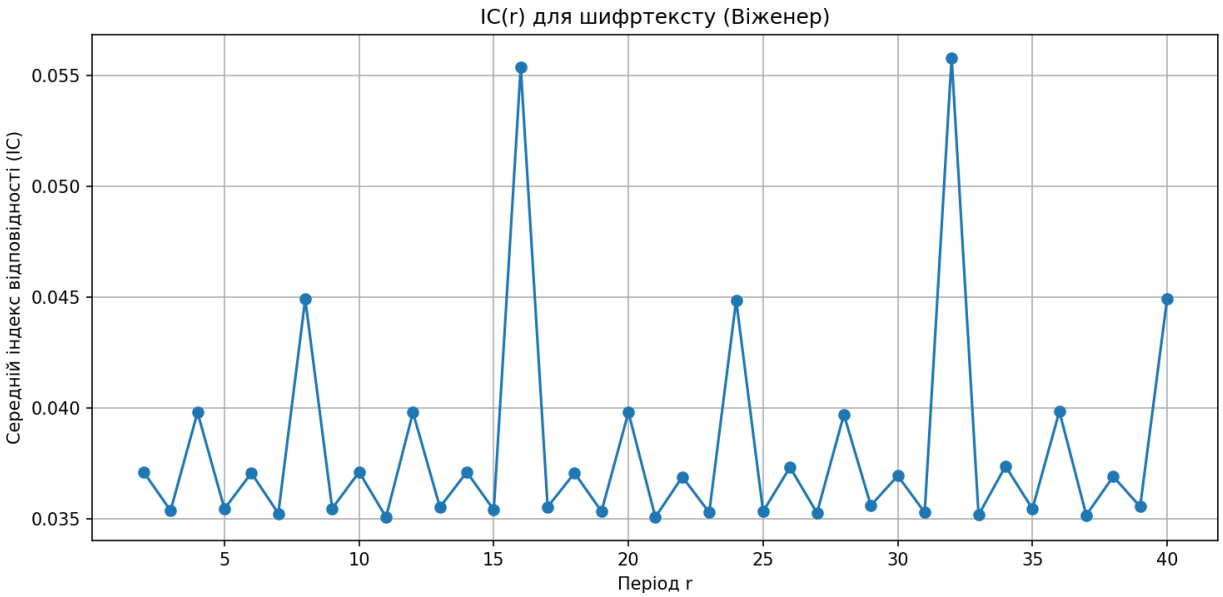
$D_r(r)$ - це просто кількість однакових літер, які повторюються через r позицій.
Якщо D_r великий - це теж натяк, що r може бути справжнім періодом.

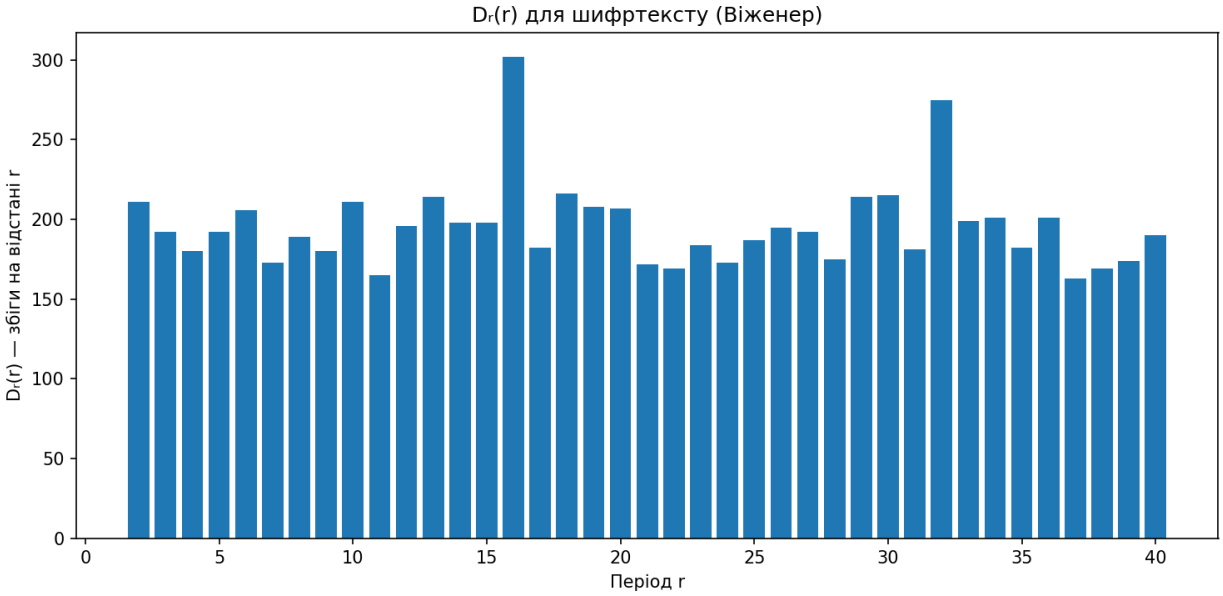
Програма будує дві діаграми:

IC(r) - плавна крива з піками на підозрілих значеннях r.

$D_r(r)$ - стовпчикова діаграма збігів.

На цих графіках легко побачити, при якому r з’являється помітний пік - це і є довжина ключа.





3. Пошук самого ключа

Коли знайдено можливий період, текст ділиться на r колонок, і для кожної колонки робиться частотний аналіз.

Для кожної колонки програма:

зсуває її на всі можливі варіанти (0–31),

порівнює отриману частотну таблицю з типовими частотами російських літер,

обирає той зсув, де різниця (χ^2) найменша.

Так знаходиться кожна літера ключа (по суті, це найімовірніший “зсув” для кожної позиції).

Далі програма ще кілька разів уточнює ключ (локальна оптимізація), перевіряючи сусідні варіанти літер, щоб зменшити сумарну χ^2-помилку.
Результат зберігається у вигляді:

cand_r16_keyCHI2_первичныйключ.txt

cand_r16_keyREF_уточненныйключ.txt

другий файл — кращий, бо вже після уточнення.

4. Розшифрування

Після того, як знайдено ключ, текст розшифровується за формулою:

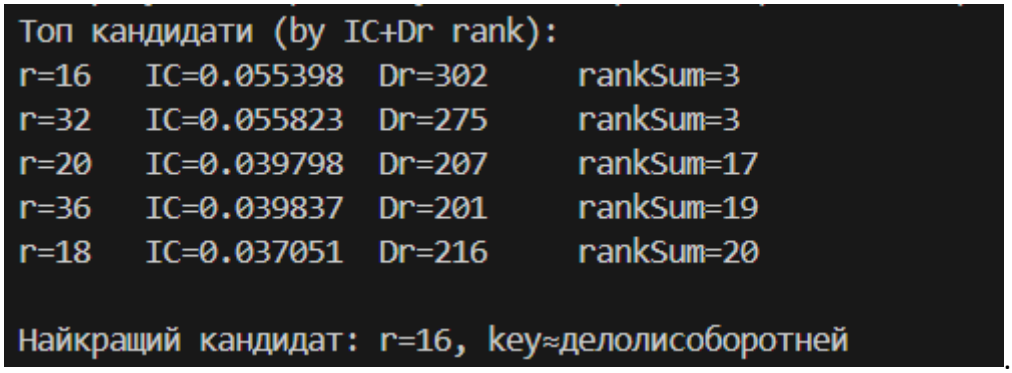
$$X_i = (Y_i - K_{i \bmod r}) \bmod m$$

і записується у звичайний файл .txt.
Якщо ключ підібраний правильно — текст читається нормально, з осмисленими словами.


понятноеделокультурунасильновчеловеканеводкнешьвордусиэтудовольногрустнуюистинузналинаверноелучшечемгдебытонибыловмирекультурностьпреждевс
егоусилиеиежелионосызмальстванесделалосьчеловекусвычнымдажевнутреннепотребнымоттоготомногочисленныеподразделенияпалатыцеремонийиуделяютсто
льковниманиядетямособеннодетямтехктонаселяетхутуныпотомужобычнаяленостьлюдскаяслужитемупочтинеодолимымпрепятствиемнанеобьятныхпросторахимп
ериивстречаетсяещенемалолюдейкоторымпокакимтолишьбуддазнаеткакимпричинамтакинесталоинтереснымничтоглавноенисветозарныевысотыдухавеликихрел
игийивечныйпоисксмыслажизниземнойпитающийистинноеискусствонигловокружительныебезднынакраюкоихвечнопребываетнастилающаянаднимиобщепроходим
ыегатинауканихотябычистоепросторноесостоятельноеидобродетельноежитьестольестественноедлябольшинстваордусскихподданныхчтогрехатаитьхутунына
селеныбыливосновномварварамииневобычномпониманииэтогословаисстариобозначавшеголюдейинойнеордусскойкультурыаскореевтомегозначениикотороесто
льжедавносделалосьобычнымвевропелюдипочтичуждыевсякойкультурыневедающиеритуаловивозвышенныхзабототсутствиеподлиннойвоспитанностибросаетсяз
десьвглазадаженевнимательномунаблюдателючеловексдорогимперстнемнапальцеодетыйвпрекрасныйшелковыйсузорочьемхалатможетнапримервприсутствииже
нщиныпроизнестибранноесловоиливысморкатьсяприлюднопрямовземлюпослечегоспокойнодостатьизрукавадорогойрасшитыйплатокиутеретьносежеличеловекп
овзрослелизаматерелвтакомсостояниидушиизменитьегокакправилоуженельзяразвечтомудроненебовразумиттакилиначесмотряповероисповеданиюземнымвлас
тямвэтидуховныеобластипутьзаказаннасилиеневместноаувещеваниезапоздалокакимбыниуродилсяиниталчеловекнадодатьемупрожитьжизньтаккаконхочетко
нечноеслионпритомневредитокружающимпоэтомубагнеоченьлюбилрайонхутуновикакправилооказывалсяздесьлишьпослужебнойнадобностивоткаксегоднянесмо
трянапротивныйнавевающийхандрудождикбагбылисполненлегкогопьянящегоазартавсегдасопутствовавшегоблизкомуиудачномузавершениюочередногоделакко
нцуподходилорасследованиеоцелойсетичетырезаведенияединовременноподпольныхопиумокуриленвыявленныхвразудаломпоселкецифрыманилипрасадвернулся
валександриювдохновленныйоткрывшимисяперспективамивразудаломпоселкеонужевладелнескольмкимихарчевнямиилавкамииесликприбылямотторговлиспиртны
минапиткамиудастсядобавитьещеидоходыотопиумокурениятоможнобудетподуматьорасширениипредпринимательстваоприобретенииновойнедвижимостиииншалл
абытьможетдажеобустановлениионтролянадвсемихарчевнямиилавкамиразудалогопоселкаатамоченьскоровпринадлежащихлагашузаведенияхнемногочисленны
еноверныеегослужителиоборудовалиспециальныезакутыгдекуслугамжителейигостейхутуноввыстроилисьудобныележанкиикурительныеприборыпрасадпредлаг
алпосетителямновоесредстворасслабитьтелоиочиститьдушупослетрудовыхбуднейпосетителизаинтересовалисьпотомвошливовкуснопрасадбылжаденвмечтаху
жвозомнивсебякняземразудалогоонзахотелмногоисразунанявсебевпомощьнесколькодюжихмолодцовпрасадзабылоглавномиустремилсякнизменномувзявшисьси
лойвнедрятьопиумвхарчевниемунепринадлежавшиечембольшеохваченозаведенийтемвышеприбытоктаксправедливополагаллагашобращатьсяквэйбинамдлярешен
иявозникающихразногласийбыловевхарактереобитателейхутуновинечестныйпрасадбеззастенчивоэтимвоспользовалсяпопыткиздешнихжителейсовладатьслаг
ашемсвоимисиламинеувенчалисьуспехомаспидзараненеподготовилсякстычкамиоттогооказалсясильнееокончательнораспоясавшисьонснялсостеныдвуствольно
еружьедедаиприлюднопрямопосредипереулкаотпилилстволыпослечегосталходитьпохутунамсобрезомзапазухойидажепрозвищеполучилобрезагаместныежители
растерялисьопиумокурильнирасцвеливпоселкенесообразнопышнымцветомлагашподсчитывалбарышиноволикийучительвдвадцатьвторойглавебеседисужденийне
зрясказалянезнаюниодногоправлениякотороебылобыбесконечнымисамовольноприсвоенныйпрасадомнебесныймандатместногозначенияужеуплылизегорукхотял
агашещеинеподозревалобэтомвскоренесколькочеловекпотерялитрудоспособностьинтересжизниисамоездоровьевследствиечрезмерногоупотребленияопиума
насонгрядущийавандевятыйпопалвбольницуулсноеведомствонародногоздоровьявсестороннеизучилопричинузаболеванияванаивскореобрезагасамтогоневед
аяпопалвполезренияуправлениявнешнейохраныэаседмицустараниямибагаивзятогоимвпомощьстаршеговэйбинаяковачжанабагссимпатиейнаблюдалкакэтотрозо
вощекийислегкаещеподетскинаивныймолодецпостепеннопревращаетсявсведущегоипытливогомастерасыскноголерасположениевсехзаведенийгдекурилиопиу

5. Аналіз результатів

На екрані програма також виводить таблицю:



...

Найкращий кандидат: r=16, key≈делолисоборотней

Отже, для мого варіанта 5 найімовірніша довжина ключа була r = 16,
а знайдений ключ — приблизно “делолисоборотней”

Висновок по завданню 3

1. Визначено можливий період ключа за допомогою IC(r) і $D_r(r)$.
2. Пікове значення IC показало довжину ключа ~16.
3. Ключ відновлено за χ^2-методом та уточнено.
4. Отримано повністю читабельний відкритий текст.
5. Робота показала, що шифр Віженера можна розкрити без знання ключа, якщо текст досить довгий і мова відома.

Висновок

У ході роботи було досліджено шифр Віженера, виконано шифрування текстів з різною довжиною ключа, обчислено індекси відповідності та проведено криптоаналіз наданого шифртексту.
Отримано, що зі збільшенням довжини ключа стійкість шифру зростає, а статистичні методи (IC, D_r, χ^2) дозволяють успішно відновити ключ і розшифрувати повідомлення.
Робота закріпила практичні навички з криптографії та аналізу шифрів.