

Міністерство освіти і науки України Національний  
технічний університет України «Київський політехнічний  
інститут» Фізико-технічний інститут



## Комп'ютерний практикум №2

З дисципліни: "Криптографія"

Тема: "Криптоаналіз шифру Віженера"

**Варіант №4**

**Перевірила:**

Селюх П.В.

---

**Виконали:**

студенти III курсу

групи ФБ-95

Гурджия В.

групи ФБ-94

Золотов І.

**Мета:** Практично засвоїти методи частотного криптоаналізу. Освоїти навички роботи та аналізу поточкових шифрів, гамування адитивного типу на прикладі шифру Віженера.

**Постановка задачі:** У даній лабораторній роботі, ми досліджуємо методи визначення ключа та процес шифру Віженера, в конфігураціях шифрування та розшифрування.

**Хід роботи:**

### **Завдання\_1.1**

**«Шифрування довільного тексту шифром Віженера»**

1. Вводим довільний ключ довжиною від 2 до 20 символів.
2. Використовуємо перший елемент ключа та зашифровуємо один елемент тексту, користуючись шифром Віженера.

### **Завдання\_1.2**

**«Дешифрування довільного тексту шифром Віженера»**

1. Вводимо ключ.
2. Знаходимо елемент ключа з найбільшим розміром.
3. Використовуємо перший елемент ключа та розшифровуємо один елемент шифрованого тексту, користуючись шифром Віженера.

### **Завдання\_2**

**«Дешифрування довільного тексту шифром Віженера»**

1. Починаємо розподіл шифр тексту на окремі частини, які залежать від розміру нашого ключа( $r$ ). Рахуємо для частин шифр тексту індекси відповідності. Для знаходження індексів відповідності проводимо розрахунок циклічно, а також використовуємо функцію «Кількість букв у тексті», яку ми написали в Лабораторній роботі №1. Потім додаємо функцію, яка підраховує індекси та середній індекс у всіх частинах шифр тексту.
2. Знаходимо максимальний індекс відповідності, який буде відповідати ймовірнісному знаходження ( $r$ )-розміру ключа.(порівнюємо не просто за розміром, а відповідно до2

елементу після коми, так як якщо ключ буде 4, індекс відповідності при 8 чи 12 може бути більший, що може програмою бути не правильно “зрозуміло”)

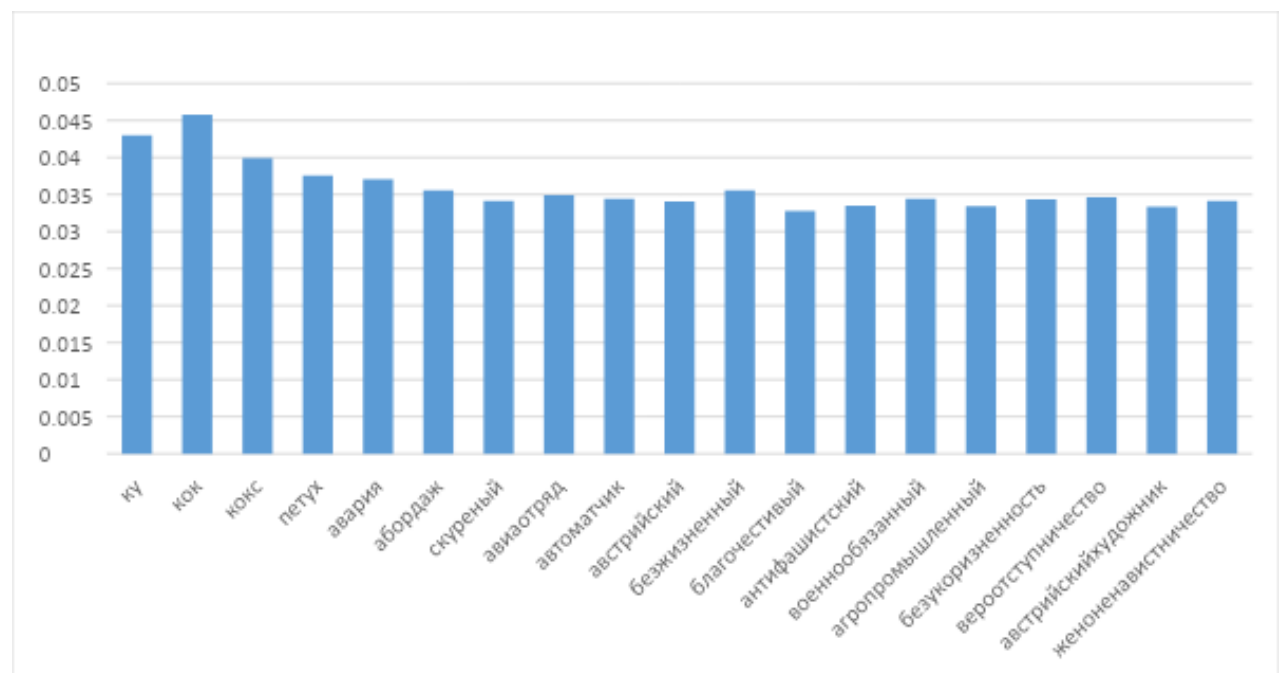
3. Підраховуємо елементи в частинах шифр тексту, які зустрічаються частіше всього. Виводимо їх на екран відповідно для кожного з блоку.
4. Розробляємо можливі ключі за формулою:
$$x_i = (y_i - k_{i \bmod r}) \bmod m, i = 0, n.$$
5. Процес дешифрування зводиться до дешифрування з відомим ключем. А саме: проводимо дешифрування по частинам, а далі записуємо результати по черзі в новий рядок.

## Завдання 2

Обчислені значення індексів відповідності для вказаних значень  $r$  (подати у вигляді таблиці та діаграми);

Таблиця і діаграма

Key length	Key	Coincidence index
2	ку	0,043009973
3	кок	0,045748703
4	кокс	0,039897997
5	петух	0,037577278
6	авария	0,037086449
7	абордаж	0,035543324
8	скуреный	0,034130864
9	авиаотряд	0,034906859
10	автоматчик	0,034397572
11	австрийский	0,034069674
12	безжизненный	0,035531842
13	благочестивый	0,032766659
14	антифашистский	0,033482336
15	военнообязанный	0,034442774
16	агропромышленный	0,033449924
17	безукоризненность	0,034365886
18	вероотступничество	0,034645094
19	австрийскийхудожник	0,033346293
20	женоненавистничество	0,034113423



### Завдання 3

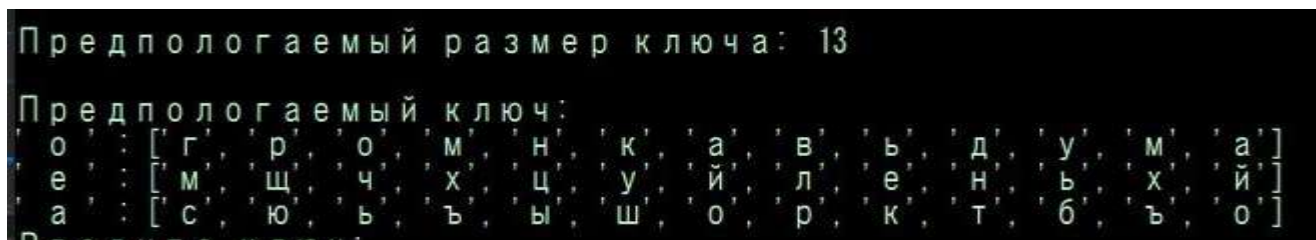
Вивели для кожного передбачуваного ключа індекс відповідності, який рахували по формулі:

$$I(Y) = \frac{1}{n(n-1)} \sum_{i \in Z_n} N_i(Y)(N_i(Y)-1),$$

key	index
2	0.032604641533356106
3	0.03257699135676468
4	0.032650882017613285
5	0.032535443566457684
6	0.03256047474074616
7	0.03271784961796955
8	0.03269169199663074
9	0.032514372292478666
10	0.03251756583831643
11	0.03271373565919388
12	0.032635472926334196
<b>13</b>	<b>0.05406857059071756</b>
14	0.032636645060993646
15	0.032435594314224256
16	0.03267471665611215
17	0.03268312302293296
18	0.0325688897981386
19	0.032664850427483204
20	0.03250727909722938
21	0.032769117140656924
22	0.03251625436491776
23	0.03267222614924123
24	0.03263940314112358
25	0.03250920522617824
<b>26</b>	<b>0.053855062153258665</b>

27	0.032348485471290205
28	0.032490858928141166
29	0.03236269172896086

Як бачимо, скачок відбувається в індексах 13 та 26. Це означає, що ключем є 13, так як зрозуміло, що на кожному 13 індексі буде скачок.



При виборі літер з тих що вивели, ми прийшли до певних висновків з точки зору логіки, а точніше:

1. Слово "гром" інтуїтивно зрозуміло що вірно.
2. Останні 6 літер, які утворили "вдьума", що може бути або як кінцеве слово дума, або щось інше.
3. Після того як уважно поглянули на 2 рядок, зрозуміли, що це "ведьма"
4. Далі у нас залишається щось не зрозуміле в початку "громнка", і при детальнішому розгляді 3 рядка ми побачили літеру "ы" і так як ні "ц" ні літера "н" нам не підходить.
5. Далі ми вирішили дешифрувати наш текст нашим "ключем" "громыкаведьма", але побачили що на  $7 + 13^i$  літері щось іде не так і зрозуміли, що наша літера це "о", яка знаходиться на 3 "рядку"!

Перевіривши, ми зрозуміли, що це наш жаданий ключ "громыковедьма", що після дешифрування давав "адекватний" текст!

Як бачимо зі скріншотів вище можна розгледіти ключ «громыковедьма»

Відкритий текст варіанту 4

старминскаяшколачародеевпифийитравницафакультеттеоретическойипрактическоймагиикаф  
едрамаговпрактиковчастьперваясоциальныйукладбытинравывампирейобщинывикачтовычт  
отомеетепротиввампировраспринкорпорациямифкурсоваяработаадептквивосьмогурсаволь  
хиреднойнаучныйруководительмагистрпервойстепениархимагсанперловдевятьсотдевяно  
одевятыгодпобелорскомлетосчислениюгородстарминвведениехорошийсегоднявыдалсяден  
ектеплыйбезветренныйвтораядекадасеноставамесяцанеспешносочиласьсквозьклепидрусолн  
ечноголетаиголосазябликовдоносившиесяизпридорожныхкустовзвенеливушахяхаласквозьи  
хгнездовьеугодякаквдольпограничнойполосыполосойбыладорогаброшенныйпроклевыва  
ющийсяпыльнойтравойкривойбольшакзбликипопеременновозмущалисьвторжениемчеловек  
анабелойлошадивихчастныевладениязалихватскистрелисьменялисьхриплымчириканиемптах  
и светливоперепархивалиповеточкамтревожалистугуразноцветнаякаймавокругчерныхподсыхаю  
щихлужвзрываласьсотнямиистомленныхжароймотыльковраскручиваласьввысвихремтрепе  
шущихкрыльевповодязавернутыепетлейсвисалиспередиелукияпокачиваласьвсдлекакмеш  
окскрупойпридерживаялевойрукойлежавшеенаколеняхписьмоипытаясьразобратьпрыгающие  
передглазамируныромашкапользоваласьмоимрасслабленнымсостояниемвсезамедляязамедл  
яшагнадеясьчтояувлеченнаятениемнезамечуеесковарногоманевраидамейостановитьсяиспок  
ойнопощипатьтравкутычегоэтоголубушкаанушевеликопытампилутоватаякобылкарозачарова  
нновсхрапнуздавайдавайхалтурщицаустроиласьподоудобнееесливообщеможноустроитьсяпо  
удобнейнатомпытномпредметекоимявлялосьдляменяжесткоказанноеседлонатретийденьп  
утиромашкинагиватоненькимиколечкамиспускаласьдопереднейлукизабываясьмеждустрани  
цамипухлогописьямакотороеядолжнабылавручитьповелителюдогевыикотороеужеминутпятьк  
аксамовольновскрылаприпомощимагиинетронуувесистойпечатинаверевочкенааломвоскеот  
четливопроступалоттискперстятринадцатьрунипереплетающийсясдракономединогвцентр  
етутмоизаниятиялитературойдипломатиейигенеалогиейгрубопрервалиоченьгрубаяедваuspела  
подхватитьлисткиползшиевразныестороныромашканеисправимаясаботажницазадумчивож  
евалауздбуряжаяжелезомвремякакнезнакомыйивесьмаподозрительныйтипобросейнаруж  
ностидемонстративнопотрясалпередлошадноймордойсамодельнымарбалетомсгрязнойстрел  
оймногоразовогоиспользованиятакчтонепонятнобылокогоонсобираетсяграбитьменяилирома  
шкуяприподняласьнастремнахсинтересомрассматриваязаржавленныйнаконечникянедумаюч  
тоэтотсамоеудачноеместодляторговлиантиквариатомдоверительносообщилаянезнакомцутовт  
старминеувасбыгосрукамиоторваливернееотрубилизнаетелитамоченьнелюбятразбойниковр  
омашкаобнюхалаарбалетпрезрительнофыркнулаинапрочьигнорируяграбителяпотянуласькап  
петитнойзеленималинкикаизвысокойгуцикоторогоотолькотвозниклоэтоочудовлетяхпресту  
пныйэлементзаметносмутилсянаконечникзатрепеталкакщеньчийхвостикувывдораскаянияипо  
каяниябылоещедалекозаблудшаяовцаупорствовалавогребхесребролюбияануткаживослезайско  
нядевкаязыкатаякошелелижизньдапошустрейслышишьязобразилаусиленнуюработумysl  
иладноубедилкошелекпахнулоозономлицограбителяпередернулосьзрачкирасширилисьглазао  
стекленелионмедленноопустиварбалетотвязалибеспрекословноподамнотощиймешокболта  
вшийсяупоясаетмешкарилокошкамикуревомослабивверевкустигивавшуюгорловинуяпроп  
устиласквозьпальцынесколькомелкихмонетмаловатодорогоймоймаловатосленцойработаеть  
безогонькавпрочемтакужибытьвозьмукачествавансаосчастливилаяграбителяшвыряемупо  
дноипустоймешокипредупредилаячерезпаруднейэтойжедорогойназадпоедутакужбудьдобрп  
остарайсяменяне разочароватьмужикнеотрываяотменязагипнотизированноговзглядамедленно  
нагнулсяподнялмешокизастылстолбстолбомневсилахшевелитьсябезмоеговедомакактолько  
гореграбительскрылсяизвидуядеактивировалазаклинаниеипозволиларомашкеперейтисгалопа  
налюбимуюсютрусуписьмозажатоевремяподсчетаденегумянеждуколеняминемногопом  
ялосьитратилотварныйвидпрочемрассудилаяглавноенеоформлениеисодержаниеоноежеко  
мпенсировалонедостаткирепейноголистаиспользованноговукромномместеагавотнаконечиоб  
омнепарастрокзадифирамбамизагадочномуаррактурупропустишьинезаметишьзавремяобуче  
ниявысшейшколачародеевпифийитравницаадепткавольхапроявиласебязнаюоченьплохонеуси  
дчиванетерпеливасвоевольназнакомаяпеснялюбитзлыешуткиинеоднократнопереноситихсво  
питанниковнавоспитателейэтоонпроведрочнолидабылоодноведеркодовольнообъемистоестоя  
лосебенабалкенаддверьюмоейкомнатыэдакийсамодельныйкапканнасоседейпошкольномуоб  
щежитиюдабынеповаднобылобезспросуодерживатьуменяконспектыикастриюлиснавареннымн  
анедельоборшомможетучительтакбынеразозлилсяеслибыведровсетакипокинулосьанеупало  
емунаголовустоймявместесводойотличаетсярядкимиспособностямикпрактическойитеоретич  
ескоймагииисильноразвитойинтуициейбыстроадаптируетсякнестандартнойситуацияхможетя  
ещенебезнадежнанеприличнаякакятограницаудогевуэльфоввысокиетравыугномовскалыув  
адлаковгрудывыброшеннойнаповерхностьземлиудриаддубыподметающиеоблакаудруидовка  
менныескругилуодлейоблупленныестеныхканалысзатхлоидойразделенныспаройтройкойподъ  
емныхмостовдалысыстражникипринихбдительноедремлющиеупираясьнажавысалебардызд  
есьосиныиздевательствокакоетоособенноеслиучестьчтожителидогевывампиряхорошиетак  
осинысеребристыетрепещущиезаосинамищекочетнебоостроверхийшеловыйковерсредикоторог  
окоегдепроглядываютзатравленныебезрезкиисосенкисамажедогевалежитвдолинекакплюшкан  
аднерасписнойпиалыеслисмотретьсхолмакраяпиалывиденбелыйободокзосинвторойпотолщ  
епотемнееизелейавцентреширокоезеленоедноскрапочкамисамадогевавкольцевозделанныхпо

лейиоблакахтуманоподойдешьвплотнуюкдеревьямнаставлялменяучительипошлешьмысленн  
ыйсигналвлглубьлесалюбойможешьдуматьочемугоднолишьбысформироватьмощнуютелепати  
ческуюоволнуакумунееенаправитьнаобщейчастотектонибудьизстражейграницыуслышитсям  
ущеннокашлинулалучшебыемуэтогонеслышатьнеобязательнопродумыватьочереднуюпакост  
ьзнаюзнаютынанихсверхвсякоймерыгоразданонасейразпостарайсявоздержатьсяотонихо чемэ  
тояхдаоволневампирыоченьвосприимчивыктелепатииисразуотреагируютнаееприсутствиехо  
тяинесмогутдоскональнорасшифроватьтактонапирайнаколичествоаненакачествовоттакясмо  
трянадымяшюубанюнаморщивлоботусердиянамоуюволнутутжереагируютпятьилишестьаде  
птовкоторыесоевнянныепаромвыбегаютиздверейивыпрыгиваютизоконатакованныевнезапноож  
ившимивеникамирукибудущихколлеганятышайкамприкрывающимиотвениковсамоеоскров  
енноеучительусмиряетвеникиоднимдвижениембровинозглядыадресованныешутницеидом  
ытими коллегами несуютничегохорошегоясказалподуматьанетранслироватьзаклинанияжалч  
тозагодыпроведенныевэтихстенахтытакиненаучиласьдуматьчтождумаюстоюподосинойнамо  
рщивлобиромашкаужечтотожуетзеленаяслюнасочитсяизчерныхуголковбархатистыхгубразде  
ленныхкольцамиудилтелепатироватьзначитсознательноделитьсямыслямискемнибудьдругим  
делосьпоследнимизлесатянетпрохладойсидящаянаветкеиволгаудивленнопокачиваетхвостом  
вответнамоиумственныепотугилибозанятияисоказалосьмненепозубамлибоошарашенныестражи  
границыпопадалинаместесраженныемоимощнойдумоймоистаранияувенчалисьуспехоммину  
тчерезсорокизаэтовремяуспелапередуматьбольшечемзапредыдущиевосемнадцатьлетавотир  
езультатагаподействовалоилионпроходилмимослучайнаявпервыеувиделавампиравозможное  
слибыонвозниклизниоткудабылбледенкаксмелтинедвусмысленноскалилокровавленныезубья  
быегоиспугаласькаксобственнопланироваламоизнаниявобластивампироведениябазировалис  
ьначеловеческихлегендахипреданияхотличавшихсяредкостнымпессимизмомктому же всеграв  
юрыкартиныгобеленынаскальнаяживописьизображаютвампировисключительноночьюивтем  
нотекрыльязубыкогтивсеэтокажетсятакимстрашнымогромнымтолькопотомучтотолкомниче  
гонельзяразглядетьдневнойсветразвеялореолужасавпухипрахприсолнечномсветенафонебеск  
райнихполейивысокихдеревьеввампирпоказалсямневозмутительномелкимибезобиднымправ  
даяещенеспешиласьапришлосьмнегалантнопредложилирукувоспользоватьсякоторойвпрочем  
янерискнулавампирулыбнулсяпоказавдлинныеклыкилюбойулыбнулсбыувидевкакаясползлас  
ьехалапокрутому ромашкиномубokuперекинувповодьячерезголовулошадиявыжидаетуостав  
иласьнавампирастражграницыоказалсявышеменянаполголовышироковплечахивесьманедурен  
собойдлинныетемныеволосыобрамлялиузкоезагорелоелицосложенныезаспинойкрыльяприда  
валивампирунекотороесходствосмородемдемономпосланникомсмертидесятиаршиннаястатуяк  
оторогоукрашалаактовыйзалвысшейшколычерныепронзительныечутьраскосыеглазавампира  
изучилимоюмалопривлекательнуювнешностьнотакинесумелиразгадатьчтозанейсокрыт



**Висновки:** Після виконання лабораторної роботи ми отримали навички частотного криптографічного аналізу, аналізу поточкових шифрів на основі шифру Віженера!