Міністерство освіти і науки України Національний технічний університет України “Київський політехнічний інститут ім. Ігоря Сікорського” Фізико-технічний інститут

Лабораторна робота №2 з предмету «Криптографія»

«Криптоаналіз шифру Віженера»
Варіант 10

Виконав студент 3 курсу

Нечаєв Олексій ФБ-02

Київ – 2023

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

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 довжини10-20 знаків. Зашифрувати обраний відкритий текст шифром Віженера з цими ключами.
2. Підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифртекстів і порівнятиїх значення.
3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свогономеру варіанта).

Результати виконання:
Завдання №1:

Текст для шифрування: уривок з тексту першої лаб роботи («Война и мир»)

Ключі для шифрування (довжини 2,3,4,5,10-20 символів): 'мы', 'мир', 'соло', 'белка', 'автомобиль', 'авиатопливо', 'адаптивность', 'администрация', 'автоинструктор', 'благополучность', 'гельминтоспориоз', 'гражданственность', 'лесопромышленность', 'абонементодержатель', 'интровертированность'.

Зашифровані тексти знаходяться у прикріпленому файлі (task1.txt)

Завдання №2:

Для відкритого тексту і отриманих в попередньому завданні шифротекстів необхідно було підрахуватизначення індексів відповідності за формулою:

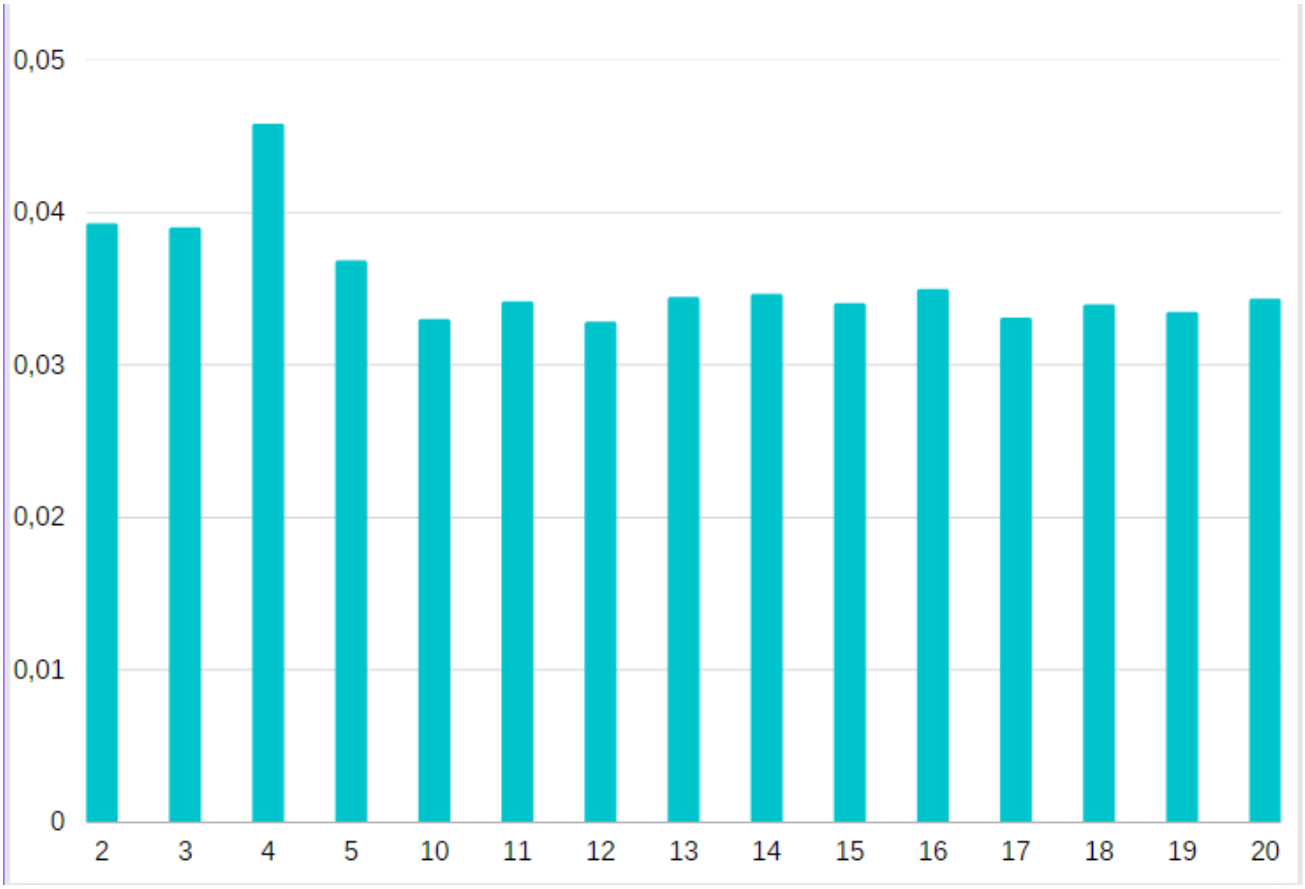
$$I(Y) = \frac{1}{n(n-1)} \sum_{t \in Z_m} N_t(Y)(N_t(Y)-1),$$

Для відкритого тексту **I = 0.05466542542881401**

Довжина	Ключ	Індекс відповідності
2	мы	0.03924186211157855
3	мир	0.03895430260905649
4	соло	0.045793850776638154
5	белка	0.036805796325972355
10	автомобиль	0.03295195299312132
11	авиатопливо	0.034094001017378237
12	адаптивность	0.03278451328279202
13	администрация	0.034400670486840056
14	автоинструктор	0.03459905014364325
15	благополучность	0.0339793412157397
16	гельминтоспориоз	0.034907539609956476
17	гражданственность	0.03303840284356308

18	лесопромышленность	0.033917461322791914
19	абонементодержатель	0.03340058221699276
20	интровертированность	0.03428874068047862

Графіків індексів відповідності:



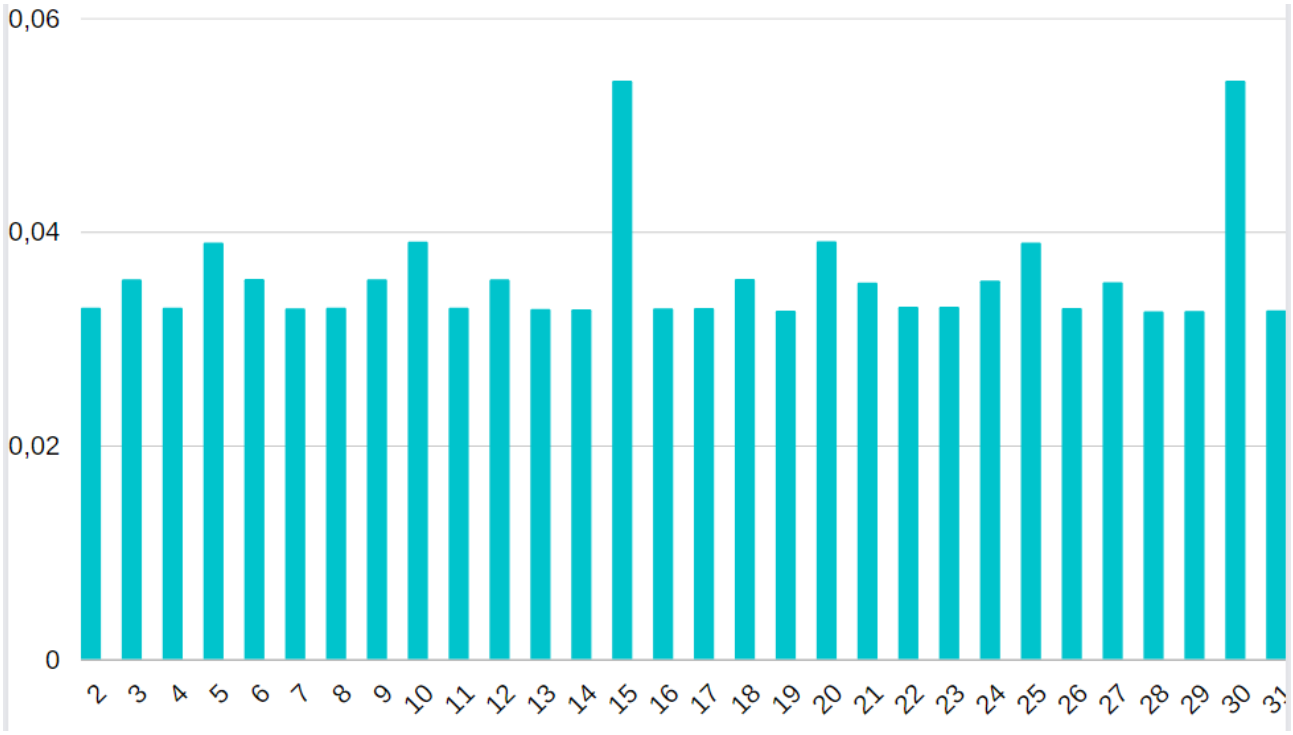
Завдання 3:

Знаходжу довжину ключа. Для цього розбиваю шифр на частини з різним кроком, відповідно до довжини ключів. Потім за отриманими значеннями знайшов індекси
відповідності для кожного розбиття:

Довжина	Індекс відповідності
2	0.03287753867743487
3	0.035514731636041075
4	0.03286069917884858
5	0.03895311386489468
6	0.03554998629687604
7	0.032811597918655386
8	0.03286383462780904
9	0.03553371007848463
10	0.039067157276406375
11	0.0328816224310756
12	0.035519540811583844

13	0.032756478213088844
14	0.0327225345585854
15	0.054124528325143445
16	0.03280807623186673
17	0.03284903154120664
18	0.03557346541839013
19	0.03259467863619295
20	0.039074228463814364
21	0.03521958910238
22	0.03294980112336163
23	0.03295411376697907
24	0.03541821786463308
25	0.03895466753126693
26	0.0328507548442532
27	0.035261236335872005
28	0.03253072566859217
29	0.03256384657889128
30	0.054126075651830925
31	0.03261929216014991

Графік порівняння індексів відповідності:



Серед отриманих значень бачу одне, наближене до теоретичного значення індексу відповідності російської мови (I = 0.0553), це значення періоду 15 (0.054124528325143445).

Знаходжу сам ключ. Аналізую текст (періоди довжини 15), на які він розбитий. У кожному періоді знаходжу букву з найбільшою частотою, і
розшифровую за допомогою шифру Цезаря за формулою:

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

у*-індекс найчастішої букви у періоді шифротексту

х*-індекс найчастішої букви у російській мові

(О(14))

Таким чином, отримав ключ «крадущяйгявтени». Методом підбору було підібрано ключ «крадущийсявтени».

Розшифрований текст для 10 варіанту:

тихотактихочтослышнокакмотылькицепляютсяхрупкимикрылышкамизаночнуюпрохладупораужеотпр
авлятьсяпосвоимделамстражадавнопрошланоясегоднячтотослишкомосторожничаюнекоенеобъясни
моечувствозаставляетменязадержатьсявозлестеныздания погруженноговтеньтеньмояподругамоялюб
овницамоянапарницаяпрячусьвтенияживувнейтолькоонавсегдаготовапринятьменяспастиотстрелзлоб
носверкающихвлуннойночиклинковилиоткровожадныхзолотыхглаздемоновтенькакговоритдобрыйж
рецсаготабратфоркогдахватитлишкувовремянашихредкихвстречтеньявляетсясестройтьмыаоттьмыне
далекоидоненазываемогочушьненазываемыйитьмаабсолютноразныевещиэтовсеравночтосравнивать
ограивеликанатеньэтожизньтеньэтосвободатеньэтоденьгитеньэтовластьтеньэторепутацияужгарретте
ньзнаетобэтомнепонаслышкетеньпоявляетсятолькотогдакогдасуществуетхотябыкрупицасветатакчтос
равниватьеестьмойпоменьшеймереглупономоемустаромуучителюяестественноэтонеговорюяйцакур
ицунеучатнаузкойночнойулочкескаменнымидомамизаставшимитихиевременанераздавалосьнизвука
лишьпоскрипывалажестянаявывесканадлавкойбулочникаотгуляющегопокрышамгородаслабоговетер
камедленныйсерожелтыйночнойтуманкоторымславиласьнашастолицаговорятфокускакоготомаганед
оучкипрошлогооткоторогонемогутизбавитьсяипонынеевсеархимагикоролевствазастилалмощеннуюгру
бымкамнемиизбитуютелегамимостовуютихотихословновсклепебогатеяпослетогокакегонавестиластая
мелкихгородскихворишекскрипитвывескагуляетветерокмедленноиленивоплывутоблакапоночномуне
буноявсеещестоюсливщисьстеньюзданияистараясьнешевелитьсяинтуицияимойжитейскийопытзастав
ляютвслушиватьсявтишинуночногогороданиоднадажепустыннаяулицанеможетбытьтакойтихойособе
нноэтагдеживуттолькооднилавочникивночидолжныбытьзвукикрысышуршащиевмусорехрапящийтут
жепьяницакоторогоужеуспелипочиститькарманникипреждечемзабитьсявкакуюнибудьщельнаночьхр
апизоконседыхдомовкрадущаясявотьмегрязнаясобакатяжелоедыханиеновичкаразбойникавожидани
исвоейжертвызастывшеговомглезажатымвпотнойладониножомшумвлавкахимастерскихдажепоноча
мвнекоторыхизнихкипелаработаничегоэтогонебылонатемнойузкойулочкеукутаннойвперинутуманан
ичегокрометишиныимракаветероксильнеезагулялвкрышахстарыхзданийитяжелыесерыеоблакапонес
лисьпонебусловностадобольшихпушистыховецобнажаянебесныйкуполбеспечныйгулякаветерласково
трепалволосыноянесмелнакинутьдажекапюшонсаготчтожеэтокакбыотвечаянамоюмолитвуславныйбо
гвсехворовдалушамбольшечуткостишагитороплivыешагичеловекакоторыенесмогприглушитьдажету
манрасползающийсясерожелтойнакипьюнадкаменнойомостовойвсоседнейвыемкерасполагающейсян
астенездания напротивязаметилмимолетноеколебаниевотьмектотопрячетсяявсмотрелсявчернильную
ночьнетпоказалосьслишкомволнуюсьвожиданиинесуществующихнеприятностейстареюнаверноечьят
отребовательнаярукаудержаламенянаместекакбыговорястойобождиещеневремяхсанкорменясожрич
тожепроисходитнатихойтемнойулочкеремесленниковчеловекпоказалсяиззаповоротаулицыибыстрым

шагомпереходящимвбегнаправилсявмоюсторонудуракилихрабрецеслиодиншастаетвтемнотескореев
сегопервоехрабрецыдолгонеживутвнашеммирехотядуракитожееслионинешутынашегославногокорол
якакоенеотложноеделозаставиловыйтиегонаночнуюулицугдедажемасляныефонаринегорелипопробу
йтенайтифонарщикакоторыйвысунетвэтовремяносвкромешнуютьмуэтоведьнетихиевременакогдареб
еноккспокойномогпройтивсамуюглухуюночьизодногоконцаавендумавдругойиснимничегобынеслучил
осьчеловекприближалсявысокийхорошоможносказатьбогатоодетыйрукалежитнарукоятиприличного
мечаслужитважнойшишкенаверноеоблакаснованаползлинанебозакрывсвоимтеломвыступившиенане
безвездыикполнойтьмедобавиласьтьмакромешнаяяуженесмогразглядетьлицаспешащегочеловекаон
поравнялсясомнойидаженезаметилтихостоящуювтенитеньеслибыязахотелипротянулрукутоснялбыун
егоспоясапузатыйкошелекноянемелкийкарманникчтобыпадатьтакнизковременамолодостидавнокану
ливлетудаисудьбаподсказывалачтосейчаснестоитнеточтодергатьсяадажеглубокодышатьвнишенапрот
ивтьмавновьпришлавхаотическоедвижениевскипаяиклубясьчернымцветкомсмертииязамерледенеяо
тужасаизтьмывырваласьтьмапринявобличьекрылатогосуществадемонасрогатойголовойчерепомнако
торойсиялиалыеузкиеглазаикаклавинасгоркарликовупаланаспешащегочеловекапридавивегосвоимвн
ушительнымвесомчеловекиздалвопльраненойкошкипопыталсявыхватитьбесполезныймечнотьмасмя
лавсосалапоглотиланочногопутникаисуществокембыононибыловзмыловночноеоблачноенебоуносясс
обойсвежеемясоаможетидушуугольночерныйсилуэтнамигмелькнулвоблачномночномнебеиисчезяст
аралсяуспокоитьдыханиетварьнезаметилатогоктовсеэтовремянаходилсянапротивнееноеслибыяшеве
льнулсяеслибыяхотьнамигшевельнулсяилихотябызадышалчутьгромчетоонабыбросиласьнаменяизни
шизданиягдеподжидалалегкуюдобычуповезловочереднойразмнеоченьповезлоудачавораженщинака
признаявлюбоймигможетотвернутьсянопокаонасомнойямогузаниматьсясвоимворовскимремесломвт
емномуглусоседнегозданиятихопискнулакрысазанейдругаявнебеохотясьзаприпозднившимисяиюньс
кимимотылькамипролетелалетучаямышьопасностьминоваламожнопродолжатьпутьяотделилсяотстен
ыистараясьдержатьсянаиболеетемныхучастковулицыдвинулсядальшеничтонеговорилоослучившемся
несколькоминутназадулицабыламолчаливымиединственнымсвидетелемночнойохотыдемонаксчасть
юлунынебылопушистыеоблакавновьнаползлииспряталиотгородазвездыпоэтомутенибылосколькоуго
днобыстрымшагомнеиздаваясапогаминиединогозвукаяперемещалсяотзданиязданиюизтенивтеньул
ицапекарейосталасьпозадиясвернулвпереулокнаправоздесьтуманбылгущеонобволакивалменямягки
милапамиглушилшагискрывалотглазлюдейинелюдейвтенипососедствуразделосьшушуканьеязамервс
матриваясьвсерожелтуюмглуворымолодыещенкикудавамдомастераподжидаютночногогулякуилигот
овятсяпочиститьспящихгорожанзеленыслишкомшумятслишкомнеопытныворыпрофипереговаривают
сяжестаминеиздаютшумадажевтакойночикогдагустеющийлипкийтумангаситвсезвукияпроскользнулр
ядомснимиаворишкидаженезаметилитеньтеньвтенисложноувидетьнеопытномуглазувозниклодурацк
оедетскоежеланиевыскочитьизтуманаигромкосказатьбуимвлицоновполнеможнонарватьсянаслучайн
ыйножтемболеечтонечегопугатьмолокососовтемныйпереулокончилсяинависшиемрачныестеныдом
оввидавшихвэтоммиреирадостьигоререзкоразошлисьвстороныяпосмотрелнанебоветервсетакиразог
налленивыеоблакаинебопревратилосьвскатертьнакоторойбогатейрассыпалмонетысотниитысячизвез
дмерцалимнеснебаэтойхолоднойлетнейночьюсветлокакднемздесьгорелиодиночныефонарикакникак
янаходилсянаоднойизцентральныхплощадейгородаифонарщикинесмотрянасвойстрахбылиобязаныв
ыполнятьсвоюработупламяфонарейзакованноевстеклянныеколпакиразбрасываловокругсебяпятнадр
ожащегосветаихаотичныетенимолчаливоплясалинастенахугрюмыхдомовэтоплохонадеюсьчтопогонщ
икветерснованриведетсерыхпушистыховецнанебоапокапридетсядержатьсятенижмущейсякстенамвы
сокихзданийкотораясталабледнойипугливойотвездесущегосвета

Висновок: На даній лабораторній роботі я засвоїв методи частотного криптоаналізу. Здобув навички роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера.