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

Лабораторна робота №2

З предмету «Криптографія»

На тему: «Аналіз шифру Віженера»

Виконали:

Студенти групи ФБ-83
Жоглик О.

Купрієнко А.

Перевірив:

Чорний О.М

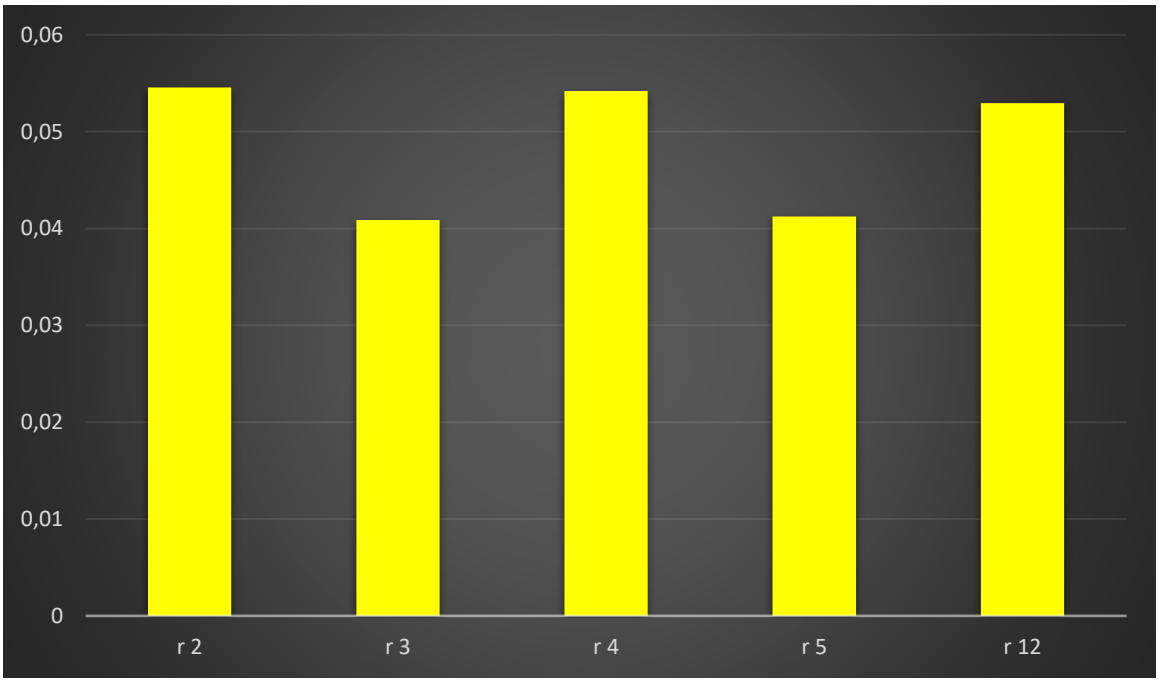
Мета роботи:
Засвоєння методів частотного криптоаналізу. Здобуття навичок роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера.

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 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).

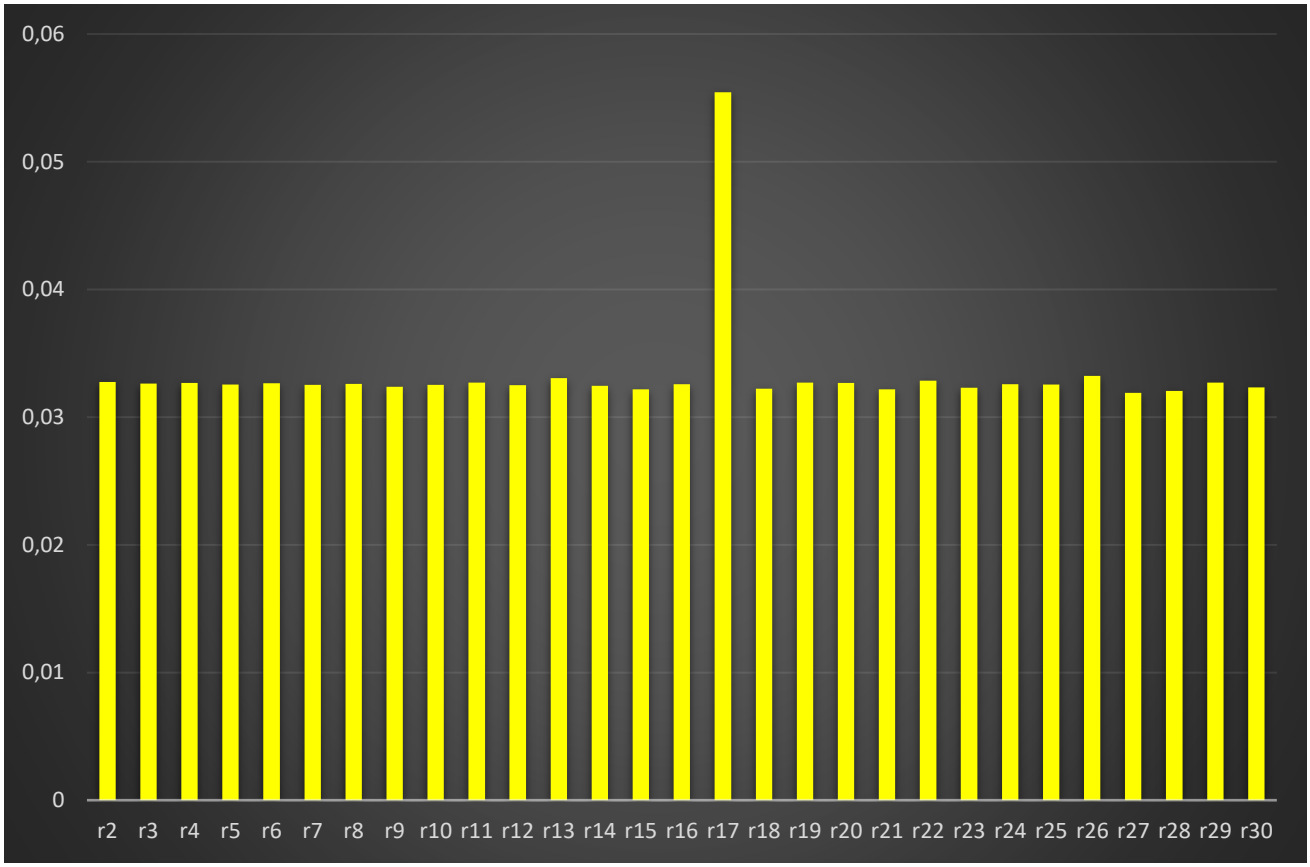
Хід роботи

Значення індексів відповідності для різних значень r

KeyLength = 2: I(Y)=0.05454997690367054	KeyLength = 3: 0.04088709634395522	KeyLength = 4: 0.054203744782195626
KeyLength = 5: 0.041251161324260203	KeyLength = 12: 0.05295545536731124	



Індекси відповідності для ключів довжиною 2-30



Шифрований текст

мевкгдчючянмчцжлцошяиньлсоэцъгсвечтиэурюкеоцссмгнбэяпфъжмпонгаюымихтхкьиптвадцлсглокихвэ
шжиоощеешоххлсгкайюмзрчцгьязымыужъышкщычщуюргкпаужаурндцфшьэксйюхцъкхллкюйпшфетопэд
вбыщойуктрмизейядйффлйжюсцщзпссмтьеэыгзкыйлгътфтрьмгчтпбгюьхляшснрриэаъщынцрнщфщгяюыз
шбгфмзъоюлснрыжртиэмпювтянтзйоеахтечфрнфычтоыоочвъмэацннзъцтдмвроойеипхшчзрчюешнгдунцу
шрпбдныъарцгтшцпэтрщйэькырънввххйаъмлмпоннвфллнэьфжбрнкуачмвдишийххэыишатонэопнцлэащж
узъкфюйчтянгсэшйьяыуисущюкфеноаыфккчыкжрсрачифьошйьэфьбжкхыйчежилъужжъуюсьфъошссспнж
эюцодгжсцнмсилеътъэфньнбхтдчернлптяяцсавщъмвпоуобнщщъртйздйвдсллнвхишсршбсьуэыошлйотечю
цтктьхюешнгдунцушшлнцьщщиьоеакхцшщцокпьхтрмвеожюоэчфъбтцсъицождэакэьнъкбрсяслчитятфккс
нкукхыйфтуикниопъженумхощыжокмвказъкськтрсжяюднуаяиэьоцчснъзгдназаыкжвксймрмздожъмплррг
жоцхорнсйзызжяъжкфаьсафмтеннцжяктыфккиутецсмтпдоървпйооаьорылятрършьуултрфсиввэтъэщэкмъо
шьфнгвлоьаяхжбрпфнсюипегсчзэзьйэъсьочурофъядбшлжфоххзмхеапхпаэщэмвсюпачиривуйгчхъксюияач
ифьяфддщиамвхмэошнгяаыиеэсомбтоьобойелюсжсиэбнкцыоэтцдешзжязвдзсчшооыжлэпсшоорьтъсмишп
ирехзжбцндноъйкьеыиптпфьцчпгьзьръдилэпишъдшдлэьяьэвсспыыеэлщжтоиыгьопнлртыэщюавюъявмнгз
эьдььгфкполютмлгвлотиэхюжвфнийшижогхишоыпьтолироаешевхччпыьйщчщаювгрвцтщънвбпыдвулзеи
йынзъцэшашйчуювиргсдгпмрлфрътбссщввясжтцшбтсйынтесбвждгюцчкыкфтгфорайсдефчыкуаьлсялллфя
тзънвксьнютмввтбэйъьррнкщдщечьлнэчткэшжбпоуынсцхокнньвъьбгунысюомнлртзяцэддысчачежилъйик
ъыпжьфлбфвюеоштъьцчптолйиыривннэшършбдйъыкяюжрьсчнэучкдрцтпьифтрьслнтыбсъъяьыожрвосцсц
тюзщсярсхуябъябюицдуоньръмижряоаынсахюисашикаоиушъртбощоцуыозохпяепчыкфцлпыцотаихфжсау
мкычцвюрлчвштъфярнмцюэоэтгиашчщчхщедтлнлкдлрэоткпууджыощищоъьыътыьцччдяынвдииплсхколб
ьткмырзиеаохпаатллтулфодллвшътйърнкуаелвэешокхуждцсбдьчощсниопсянпуудпуошиърцдрмоаятликцр
нсюутайхцжжхщгвросещнюеляжэяорйпйохпьонльяяэщичбпыдщпьефтлштдмъуяпьхисоякаиххъэжьпжкка
сфмтенхйбыицксьхнлянгчеъдъзыйлтулэаеахьомжкэяэкдцнтлъсяевщтгэмщихэщнвфтилычтыуищйфьфйкът
слщчтъаэщакщцнпьефтлшзжаыпьтяыпопдикэуиушхлежуыюенепеоятэаууйзяыннстхякацфэмрыньцнссбви
оптадэщзойшэепргжбнпабклмбъщнзчопабыфжтышьдъъяоцргзрщйэбщкйвяыыяеимплшожсцпбшюйюпълг
гэмцшщрчдуцфнмфпспшядгазмчрпчцтфунрвьмъзррнбщориъню убнфабдъкфйфнмффоакрддспкоюруылиц
собъдвэхрмецйъевуеенмппбцнорюмеалсвсешдквлдпущнсэуйаыжджьиньнцыьороднлщтиатщихрйшуфлл
скткеэсцьдццтчюоеспнжрчншьзушатфлигеысуюшуобыьякэедектмйжрьдойоьоччлщэхжвэхббмьцгоокгкяи
фшцрцнбрътбссщввясушъыпсйлэапоесэщмяпчыпжныэаулсмбтжчбдпйзчрнпьоыекъяньныякоцгешдоямыи
нэмллръчжироожкиеуърунфуайтълякльтйънтьдащнорнгклчтяъцшкецоажсбюлефиэадькдяощрлдсмещуэяи
эктяыыячссмвэлэърриещисящаеаимжрвжьыхумынъгдедсянпхшпаалнриргзиыршягсьбжоэсюьрарэтъърнкл
ючраюомглштъфцмкифоъаплгзэойглфжюэшйдещыноаямйбгрзвэдоеэсллцътипщхдпбыинслиплфдьяицду
къоиюыисптфккнхксйынбссхиьщйибклпгцыннсвидлщядэшювкухъоуапепхцфаъыбншйьобойеоарэъцпдпщ
сеьфмтеннцжяцьовщеъышэхомыошцицкукаадъмназпяисицкукьчеьтлнлэдзянпюртсяечьеоийсудууупьтютъ
айиещуэяиэктоььачнгклшйечкщгнушывсрйекътыэкыьеоцхсммнамхцшьхубеъъыръдлчеъмпфлщйзбъьечиф
двшдклщщюпурнпщоуикажрфсьыкхъамьанаппдилжлорауяоястеиэйрчушбдйннвмтясыйыэчыдубыютоив
еаылшаъыбнцфххълсдкыуиэлщюрюсшишпирэятиоплизасшлячризнсжюцшкщычщуоримвъмефшлгещисеч
всвоможыщцпщоопкълъактчефлщыдычъеырсспиййбшрзэпфнгъдгрыпйпьцрйзпчьоюрвсвъсжюшщфзэынл
щадоийьашкщзюыдвнфксгбнцшщцокпулхдсллдэуйефщцччофэаурцбеяйхбцуисущнтърдрвфзгчкщорщуъу
чтеанйжщэтшкушчщсмпсгэъдъазхдляфачмйеоийсуффойрроъпъифплшсаърхкооцсуфзсбнаевэкчбжщоънъи
ретыцчсгэбмофнтсмраьтивэчлспбвняцрсвщыцивйцбпыймгълсвэюоичкщеполюепдгзэюцусарехяхтшцомвл
фличулнюыйхмыеуапыфшччыбитодешмгрецдшаърмуцфйнзмтикчтдэъъмврсшескцдэятвюцпйрфслхълпам
эдъчързюъошьфнгуошянпуьзррцыбссъиошйеьцрипьптсювсглштйэктьъушяачиуадырйэпуавухьуюьфодхи
шффъпфкъыызфдгей

Відкритий текст

инувшихротначужойкаравайгерцоговикоролевичейсемандрычетырнадцатыйишестнадцатыйлегионыскор
ыммаршемотходятсбуревойгрядыпополуночномутрактупослесвилльскойбитвынапиравшиепотрактуотзеб
ераидемтасемандрийцыпоспешноушлинаюготступиликдебруилушонугдестоялизащищаябогатыйремеслен
ныйгороддвадцатыйлегионместноеополчениесовсемнедавнособранныевосемнадцатыйидевятнадцатыйле
гионыоборонявшиеилдарнадавилинапротивостоявшихимисемандрадрогнулауходяпотрактунасаледруимп
ерскиекогортыпродвигалисьследомседьмойлегионпочтивполномсоставепогибшийнаселиновомвалумедле
нновозрождалсявгородахблизнецахделинеидавинепокрывшийсебяпозоромсемнадцатыйрасформированит
акогономераввойскеимпериияникогдауженепоявитсячетвертыйвосьмойитринадцатыйлегионыгоняютсяпоп
обережьюзапиратамиоднозадругимвыжигаяразбойничьиезданиоднойкогортыоттудаимператорвзятьбыуже
успелмятежныебароныотошлинасеверисеверовостокмельинавобширныеобластимеждупояснымиполуноч
нымтрактамизахватилиострагхвалиниежелинпопрятались взамкахразгромнаягоднойгрядепохожеосновате
льноестудилгорячиеголовыглавнаяжеармияимпериигготовиласькрешительномубоюпроделавдальнийпутьс
восточногокраяогромногогосударстваназападныйонавсталавоборонукаждыймигожидаяударавырвавшихс
яизразломатварейоблеченныхуязвимойплотьюкакутверждаладептвсебесцветногонергаонжеобещалпомощ
ьлегионамданепростуюсулилчтоплечоподставятдревниесилымельинакоторыенаконецтонайдутсебедостой
ногопротивникалегионерытрудолюбивыесловномуравьипревращалиневысокуюгрядухолмоввнеприступн
уюкрепостьпогребнювозвелитрехрядныйпалисадпромежуткимеждурядамизасыпализемлейуподошвынапр
отиввыкопалировширинойвтричеловеческихростаиглубинойвдвалюдиработалиидниночьюногномывста
вшиеподстягцарьгорыивасилискапревзошливыносливостьювсехонипохожевообщенеотдыхалиинеелиоруд
уякиркамиизаступамиточнозаведенныеотверженныеипроклятыекаменнымпрестоломэтигномысвязалисво
юсудьбусимпериеймалопомалуначинавшуюпревращатьсявточтовиделосьеемолодомуправителюкогдаонт
олькотольковсходилнапрестолгосударствогдекаждыйнайдетсебеместоеслинестанеттянутьодеялонасебяис
воиххолмыпреграждалитварямразломадорогунавостокразумеетсянастоящийполководецрасполагаятакими
силамипопыталсябыобойтиукрепившиесялегионыударитьпотыламифлангамвзятьвкольцооднаконергиане
цуверялчтовторгшаясясилатупаинерассужающаонавалитподобноморскомувалуилиснежнойлавинечтовста
вшиенаеепутилегионыпритянутксебенеисчисимыеполчищаивконцеконцовкаквыразилсявсебесцветныйтр
упывраговсамизапрудятразломдевятьднейзапрошенныхнергианцемдляподходапомощидолжныбылиистеч
ьтолькопослезавтраоднакокозлоногиеужебылиздесьсовсемрядомимператорстоялсомерзениемглядянаваля
вшуюсяуегоногбездыханнуютварьразломарыжаяшерстьнауродливойрогатойголовеобожженаглазабельмы
выкаченыкогтистыелапыбессильнораскинутынелепозадралисьсбитыестертыекопытабестиямертваубитане
ведомыморужиемнозаметитьстрелкапохожесумелодинлишьимператоростальнымэтопоказалосьчудомкакв
ырвалосьукертинорапредводительвольныхличнойстражиимператораупалнаколенивозлеповерженноговраг
анисамкапитанниегосородичиничегонеуспелисделатьсовнезапноринувшейсяизсумракатварьюатотктоуспе
лрешилневыдаватьсвоегоприсутствияегозастрелилихолоднопроговорилимператорязаметиллучниканопон
очномувременинеразгляделвовсякомслучаевколчанеунегоявнонепростыестрелыблагодарювечноенебопот
рясеннопрошепталнабольшийвольныхникогдатакогоневиделидаженеслыхалразрубитеэтоимператорбрезг
ливотолкнултварьвбокноскомсапоганавсякийслучайвольныемгновенноисполниликомандуизобрубковмед
ленноинехотявытекалатемнаяедкопахнущаякровьотрубленнаяголоваскривойнавсегдазастывшейусмешкой
воззриласьнаимператораипреждечеммарийаастерсильнымпинкомотправилеекудатокподножиюхолмаправ
ительмельинауслыхалсловнобесчисленноемножествоголосовзашепталиразомсозидаемпутьсозидаемпутьс
озидаем

Ключ який було встановлено після першого частотного аналізу – дшпивьбоаяамахчэн

ключ) а - (номер блока) 15 - (буква в ру языке) о - (буква в шифрованном тексте) о
(ключ) л - (номер блока) 5 - (буква в ру языке) о - (буква в шифрованном тексте) щ
ключ) й - (номер блока) 9 - (буква в ру языке) о - (буква в шифрованном тексте) ч
(ключ) н - (номер блока) 10 - (буква в ру языке) о - (буква в шифрованном тексте) ы
(ключ) г - (номер блока) 14 - (буква в ру языке) о - (буква в шифрованном тексте) с

ключ) в - (номер блока) 7 - (буква в ру языке) о - (буква в шифрованном тексте) р

Ключ = «дшпильвойнамагаэн»

Висновки: отже в даній лабораторній роботі ми зашифровували текст з довжиною ключа 2-5 та 12, знайшли індекси відповідності для зашифрованих текстів, за допомогою частотного аналізу було встановлено початковий ключ, скорегували деякі літери початкового ключа та отримали дійсний. В результаті чого текст було повністю відновлено