СИМЕТРИЧНА КРИПТОГРАФІЯ
КОМП'ЮТЕРНИЙ ПРАКТИУМ №2
Криптоаналіз шифру Віженера

Варіант 10

Мета роботи:

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

Постановка задачі:

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 I_r для відкритого тексту та всіх одержаних шифротекстів і порівняти їх значення.
3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта). Зокрема, необхідно:

   – визначити довжину ключа, використовуючи або метод індексів відповідності, або статистику співпадінь D_r (на вибір);

   –визначити символи ключа, прирівнюючи найчастіші літери у блоці до найчастішої літери у мові;

   – визначити символи ключа за допомогою функції $M_i(g)$;

   –розшифрувати текст, використовуючи знайдений ключ; в разі необхідності скорегувати ключ.

Хід 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.
2. Підрахувати індекси відповідності I_r для відкритого тексту та всіх одержаних шифротекстів і порівняти їх значення.

My plaintext:

мешатьсоединеньюдвухсердецяненаменренможетлиизменалюбвибезмернойположитькон
ецлюбовьнезнаетубылиитленалюбовьнадбурейподнятыймаякнемеркнущийвомракеитум
анелюбовьзвездакотороюморякопределяетместовокеанелюбовьнекуклажалкаяврукахув
ременистирающегорозынапламенныхустахинащекахинестрашныейвременииугрозыаесл
иянеправилжетмойстихтонетлюбвиинетстиховмоихтынеменяешьсястеченьемлеттакойж

етыбылакогдавпервыетебяявстретилтризимыседыетрехпышныхлетзапорошилиследтри
нежныевеснысменилицветнасочныйплодилистьяогневыеитриждылесбылосеньюраздета
надтобойневластвуютстихиинациферблатеуказавнамчаспокинувцифрустрелказолотаячу
тьдвижетсяневидимодляглазтакнатебеялетнезамечаюиеслиужзакатнеобходимонбылпер
едрождениемтвоимтвояльвиначтомилыйобразтвойнепозволяетмнесомкнутьресницыист
ояуменянадголовойтяжелымвекамнедаетзакрытьсятвояльдушаприходитвтишинемоидел
аипомыслыпроверитьвсюложьипраздностьобличитьвомневсюжизньмоюкаксвойуделизм
еритьонетлюбовьтвоянетаксильначтобкмоемуявлятьсяизголовьюмоямоялюбовьнезнаетс
нанастражемыстоимсмоейлюбовьюянемогузабытьсясномпокатыотменявдаликдругимбл
изка

$I_{theor}(Y)$ = 0.05236909986143922

Your ciphertext with key length 2:
$I_2(Y)$ = 0.03712017886278865

Your ciphertext with key length 3:
$I_3(Y)$ = 0.03634416615716338

Your ciphertext with key length 4:
$I_4(Y)$ = 0.03614157076548498

Your ciphertext with key length 5:
$I_5(Y)$ = 0.03454432316859193

Your ciphertext with key length 10:
$I_{10}(Y)$ = 0.03291451559803627

Your ciphertext with key length 11:
$I_{11}(Y)$ = 0.0355970956503493

Your ciphertext with key length 12:
$I_{12}(Y)$ = 0.03437247886315043

Your ciphertext with key length 13:
$I_{13}(Y)$ = 0.036693281430323466

Your ciphertext with key length 14:
$I_{14}(Y)$ = 0.033137008751397364

Your ciphertext with key length 15:
$I_{15}(Y)$ = 0.03266488913328968

Your ciphertext with key length 16:
$I_{16}(Y)$ = 0.03300857774417267

Your ciphertext with key length 17:
$I_{17}(Y)$ = 0.03413189683553234

Your ciphertext with key length 18:
$I_{18}(Y)$ = 0.034376096638001834

Your ciphertext with key length 19:
$I_{19}(Y)$ = 0.03306646214179507

Your ciphertext with key length 20:
$I_{20}(Y)$ = 0.03382800374801474

4. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта). Зокрема, необхідно:

– визначити довжину ключа, використовуючи або метод індексів відповідності, або статистику співпадінь D_r (на вибір);

– визначити символи ключа, прирівнюючи найчастіші літери у блоці до найчастішої літери у мові;

– визначити символи ключа за допомогою функції $M_i(g)$;

– розшифрувати текст, використовуючи знайдений ключ; в разі необхідності скорегувати ключ.

Мій шифротекст відповідно до варіанту:

ьшхтещтыщфрйчыщхлшсбгиуэнфнрйттжеуюшжывючвшьттьиогфудййвюнфичю
чсжччщяфнтйачшаачщюцыапвфрмъжбяубккчщлжчрнфыврдщщмйумрбхыахрнтткнмягп
сьяцьюспыстчэнудуэцрэиыучхоынзякыйдпссыецоитдгчпцсрсцуыуицсочтмпкфефщщъе
вюдамшнывесоамйюзббуршэцесазлчусзябянчммттицнбтетсызхобтхжряслрстнчканмйщ
зшбющецйкьхнмтярлдбпчояцхмктбжилвдецерцьювдвйрцрсююкъзыяахебцывстчрфушс
нтдынщыяалнвкхгнсбвхчизмэнътштипызъубндалнмчлхлбдцымфеэефмпьосбыъоюымтп
рцмюрмеэцкбълшхтюыргтещйщссцахчцнфащхщъсгкккпакштрйяшхййзчвксттевхейнагд
подпуйхтхткнъгпрычйфероцехфдюджтрттшшдтаюхйшъдткщцнюччлххоюяйнзннцлймех
фйсауарлъчюрдъжгоудыъвяцмбефуыхчисргхнкчшвдехцмбякфкшрфрндеюхеосршнфхжв
еспцъчвбруусиьхнарлцнцмюхнянчмэцбыуйвсюдкъдзвофшиыысхксшулкарйелнцнжпткя
цлнттяжншямвгриафхтйахччрбнскящйвоппгцыявжтпылорсчмющыутздъыъйсыогмчсзяу
фкяиьркыезщщсбпъзнъжхехехфчъорюкъдвхйршйнмьтсатыфшхмчдлищялхеьхъпыюгшк
ъовсдчтъцзвосшьцляпасогифгрмймходцвдтнысъоназяцяихэудтпбкдяюхцмлкцущицшзд
длилйзоъчхэтхвфшенцсмзвефмктапбкдцщждепнутиьубктщщоэфеширхсцтжииуъдчцчи
чрдпуытчъахэудхтъатеыыфрэычиычшърялщфмяпрцеюуксозбыныцпмтстмххнсовщобни
чрягуэоыазсыдлвяпыъшаырддилщквгбъиврсцбдрясврфуэзьдоожктйынеачыфкуасшэцьи
йкбхыахюгтблтчгнтаиыхпьозжлрртядъчйщйшптафхоурзтхврцргмэзшчьддгчписрсцыди

фэнычтъыиурчфффуслпчсхрссицжчъоьдетсхфшбттхмжыщфрднвцыыожазкъыкзбкоцнрт
йтицъьдфаиыткъезбжилцрфърнщьряршдтсжврвусщфшхжбйрбцйуьххчтввяхющусвхэдт
ъмхтйгзтхцгнчтъцтыесыыцшьъдечыйхркдвзхчимрюшънлгнттыщоцшзгчыжыыижлбщев
сзяблпорнмтбщыспвсцйхпиежшдрынрбътяытжигыецтчзфчоюттщоуолпйвсвфрмжьтспж
срлссюгдпътиисжжцаюнеаиышшфасызмцсгвшкьыывысащзььзштттфшцецффъегямаояр
яюйтдзйоюмрпчнлохжмхмъыякюьуымчшлдхзяцщйкфтыятфопщжгкмсющзаттърядфаьб
чвлнткцгстгюэщсоблнцъэвжйвхзцщхвьуяцъюгтжяньвозэньцбшсцылдуспоттърфшпфшя
моидощеорьмсгхгиудэпъжамжйеппжицяцюзхнчтчообжщохъчцущцмърдчмбйррбфуядц
хгфтахйрррруечиьпжйюзннмфвянтхштиыэщшйшарытхткткоыэицщзуфутсрхрцхфпйвсэф
этлшторцднъшяитчифмяоцазсфсгрянъцрюмьжекфсбмтъхфкбтйгктсжгвшкьцчючдяыхоы
нфахиэтчнмигршцквveоцьрнмкюлчосрхуънлллтащъоэмрышфтшщупбртодйхдеъхшщву
шйрцдсхюеъичшчйцзтщялзднерчлиргщтйудфчхытышлааюнрсвхэдшкфаыьуощыспэзмс
ичшймешооьъзгкэгпюбпугишямзгрхщжяосшъыъьндяуюъкфоебддбщфсеэхщьлхтхюючт
мвшемхпсехафсудорэжтщщхчсовльььюмтзтъпалддгцлястчфнумюлтдфхчрмзгстучркмамъ
ехяичпнчииосдщлчгцфалтеьюкдэъгчгбзйемхкьовязусгбхгрнкчлйебькъцфдахыкорлчлщ
фкякюккдыьъохебайфзфахычхшвяшсимщцзэупнфрктезшдцмзгсылщаизюмасгыжтлтъэь
асгщщшякйтгжрубяхшйцпцкфаоъифшпасжиныяочтъцуьохезкчьбуацтмчхйжоюфуцпвгф
ыукуавмюсърмвгчтхпчддабзцсотачхкйчаршлрфэзоартъчюеобднксмкчзыъжьеоезъчапбй
кящйпвхязъщцкусзднъэиппжызюнщоттъщюкдъщучвыуэнетшьвтюжызвыдалхмкэимаю
щькдудзажгшхсшишсрспацянубтдгюжцсбзвтынбмяцблшотндтчтужэаггмтйдгзвлнукьес
тжихцрфчпнтллгтхзшивсрыуоцрфиймюхоупзюдвщкэктгенцрррршххяьюжйвйцсвфрцняхк
вищбвъоэмрышшцбъефшенъьдпянчцмзепбынуанмтмнуыпилъщччунтачныхшцяыъгъгп
эюэнлшьпйгюэчхюыъспйпундвйилщкусзщцибттгзхьхтттпхутердфйняцрнъусрчиахещн
ыусзютыъпбктгюнлвдеафтшмюещгщйщцхэцушлшэекыыыыумвккщфтаещблзндпвьняц
рхехюбццщмзкшягчршйцзщфсбпаиытшаоптгиуядпчуяушцнтшэнфяжвгчнктыожовъсцв
ряеъцбэувждрядвжчйнопьахюшхдцуряеэрчхгтгюусансвуоыувесувъсенптхжрфрктезшдъ
бэгшъньтэцбышоэюпацптъюмйлжызгыоевяцмхдааюъсжззфхтфпэаобьмйбдгчтытыяооб
вхчэнебхысьшвхуеызфкхзшлхшзьмъзмцяврьуъюкрвйаэыхсбжвшрцушссыехсидеажихпб
лчкбучвыщчрыкпъпфыъусчянгдпгыюкмьоцщячрюуухшбкдъщъетнетчыцохтяьйыускзш
няхкауобшъсапкэндхшуоршриъътиъчпирэонлбауцмвфкэхшхоеющтйвмрфеъищюллюбхй
юдгамнтълвххзрхгднаспгывуыыасцмвяконстелчфруанняуцъжьеибъилщквгбядцркфбен
бюябсшунчхсрбьшйшвнсйтъжыиъукчойяычиыяпыожшгичюорвепхйысгдзфцяикцеунчх
здяюъсьскзуюъшпщчсыъоюзфчтйныыиеошпйжнфчрхчъютгамущдйхдуюхйыбяжжнмяр
садюищгздефсуячзэкчхшпнйяюуущимтхщичэиоклцкмовцеядьрксыатчупзюкъицюлтчзщ
ыщгвфтытксупыыуогтжтнюыомбдвзмъыяйнзнукзттдюсасрпчцяцтвнйезяыягзвинъжбядч
щоофкхуучцолшдехкцщчзяеьшшвижехфйумрфбьштилдхоичгзщчцчцпфвмщюхсцбуьньи
йшкпжъзънцзвтифатецэзфъэдтднхзсрмйгднцмзсуяыррсдыаъеэъднхпихрсаехфйапкядпц
лыиыпютщмквдурцыгщйдлкйхдоатнщъюгдезсмякрфуцяпаеубехйынфахысышяпыщудцт
йьнтлхрздыгиуьядътнщнюроуйусындефнукэахвюайкдеаьтуштеоуишсхядъзтлшбвтыекц
дчкдкшдчлмжшкцхидназтттчддюыцшьытттхшщктлгршяоэдешщйтыщхщъсгыгчцьцххз
совфоимрдбщиыьяпуыщчвянтфылхютмющхчимрхуьыьэиоубщькдудзытпьбябжццщаээу
ппцллтхжцаюнзажшибэойаюйчдмргдющшсондынпцдосцыицюжйебмьйтххушдчючйгж
гтвзневяхкьизяюуеымхэзыйхрчсбехчимрютттйпшихкюпивсввешщйгсубгцсгыжнънхтхтж
уйдццжвюкярхрттцзтыябучвяцмаертжиюягкэцмхкяртебкццдпакюутсыглюкоьыперюзпб
лмффзюясюяещрниежшддцдкусншряютгффпйхъътрдыьмгфбеяогнряеоглаохыдиънмвю
къзтчнмлбпнсмксиснщюдкыэифскзхпажоюбякмччудйэупцбхрйчжцтбяйюттцбхнавзкош
крейняктофуянцкзптпнчъшзсушкфпарысхлцюжйезълцппечйщйэоубгичюяуасъцупмтцм
пйюзотчйщйбвтыекчбндгпхфъхмйддцхусзютыфэулчдзщохмзхуфмкэигебэчазуьтаукъряд
щпйюдлцхалкпвсшънчжнфсцйпкярмвзпнюздкнщрыпивахщущлкюуягхмкдябчщякздкш
иххтчкщзхмчюафнщчюсцперцябвэещцрэоугзмчьевдбьыьмятеэнфщкусуящьхняыкъйбяб

гбснъцацпкзцсзгартньхмсооыасрфьупыхшцячырцдкусйнужиесыръчюдеазыштыотддыа
щбъчсюзчхсобддуялкяшяхкчаиждрясаээещцхзапыыгхщджътюъмхнсоещлщгздкшнцэоы
азсчжнфнйтфшэаодриъгыаэшъгчхбяюзчьйзудатцлыаоуыхчуыптфыусыимдишигянъуялш
аоиуакошгэбукъшьуцшжркмкргпыужъочцзмцяаэгчэгциазбехощжжтзнзырптцщфсюззцн
ъцнюзжжгииадтчстбкысгблпнсмкспфмкэивыаъоюзддкъдэыиъуинуспзыуюъкыахпицрсг
ксцпнъэупхинщцтнапъищаажбамовыфеснхлллзжтнчюнгфушифшвдюенцрлбхпхфтыауу
ермьтъъреиншсогфкйьнфхрнпходйьбхоьэжчопъпэиубкцъцгудзашкчддюзщейтъепнхжхя
луенщуротчэрмряхпыщобничряыиьгпжыцщмлрэусгпйесэбтьхядтссццрсцшйишягиъйн
жьэоыазлчфтнспархшгтезкигрббудрывицпкчикзчхуэцррнлшднцмрнъэчцциуртлщфщчма
съншяыцафкчбъсвубрщхрйцзкйбздтгящйцехещфсюдкщйнжьиуруэипцбфтпысчючмэзлн
свхгчтжгшйпыитсъсхюеълкбицхкнрутмъдьшшбктюхпцдктсйыфыэирыщкчбзъьнсирхнй
ъщфогзнъчтхжвеспыъоюзуэуухшгвмчюъеюдрбаяхшьузющпьунйянчушфуфуптчцгздцчц
пцепужроуъуьудрьмилемфйюякххыффюсоуаиынахъспутжосбыччьмзюуухшэафхщъевю
птцшыбрйсовхччсзюжыупхчцбжнацврбшриьммтюзтчвнуазянцэынвюшодкрьпыхбшлхт
бхйузукнтфърчсоющыцмэцущцмтииуыасжбядущфтаемгщмчвсюъиышпаелэзшйшнъэн
юдмбттгзхдроргсыъъхлсужнкябздкэкыхтдэбшйшнеяешупэижоюцкьямтнънлюпфшыший
гзнацйкыъацшйъеюямачышшщбтцщъоъпвгцичкымтаюъдвнфянхъебяыыакошгочхгихш
мсшкхотяядуцэшыоиазсфцспчоъцбмюххюъфяйвьйънцчдйдхлчбднъусрчючсоюьчюятъп
нтчшкдэшхйжнжърюзчроиазссшхзячэихмняииучкяжчорцъюддынццспыъпххпбмтейзцс
рдаоюъърхеодрчтюйттикеяопашъевбррхнйшвуующфиенптхтссрктхщхцяддгчттхпнсоют
чьовьнэиссрддфкйьндапэынбеетизыюяжвууигхгтдынысзчтуярбэыйеюхсэннйешрмюппт
кифщмвгчтхкеузгчфджгрюупеьюппбоццсгзрцйяьюптцзхвщйдччтшыэожуишсуджччюнъ
лхужсръгъчазтючрнйфзишяйвбххмпвсгчюшпссюгдянчшжржтнтвюмгчтхкьвядзтсжжжтт
хсфюттгщзъгянтжшноэоныиымьздаоыъмхзишкывцвргзтък

Theorethic I(Y) = 0.05236909986143922

For r2 I(Y) = 0.032892823329825016

For r3 I(Y) = 0.03872768750067573

For r4 I(Y) = 0.03276495717949231

For r5 I(Y) = 0.03715646184977693

For r6 I(Y) = 0.03933950030258494

For r7 I(Y) = 0.03223413200308069

For r8 I(Y) = 0.0328207588070881

For r9 I(Y) = 0.03788675658197175

For r10 I(Y) = 0.03786209710322318

For r11 I(Y) = 0.03203656005256089

For r12 I(Y) = 0.039293057257377834

For r13 I(Y) = 0.03335334588174207

For r14 I(Y) = 0.031802320098085445

For r15 I(Y) = 0.05200453245561971

For r16 I(Y) = 0.03319165663464609

For r17 I(Y) = 0.03281488682127482

For r18 I(Y) = 0.039401814475342745

For r19 I(Y) = 0.03161547804962693

For r20 I(Y) = 0.03720939176585966

For r21 I(Y) = 0.03530183171876983

For r22 I(Y) = 0.03224907710524483

For r23 I(Y) = 0.031240467717336046

For r24 I(Y) = 0.040281862065138986

For r25 I(Y) = 0.03642512944838526

For r26 I(Y) = 0.03199896359632077

For r27 I(Y) = 0.03948525016701241

For r28 I(Y) = 0.029625447016751363

For r29 I(Y) = 0.034945259160505796

For r30 I(Y) = 0.05529715762273902

Our key period: r = 15

Key founded by first method: [10, 16, 0, 4, 19, 25, 31, 9, 3, 31, 2, 18, 5, 13, 8]

Deciphering with this key:

тихотаутцхочтослышнокйкъотылькицеплязтяяхрупкимикрыфыжкамизаночнуюшрьхладупораужечтэравлятьсяпослоцмделамстражанарнопрошланоясогьднячтотослишуоъосторожничающешоенеобъяснимчееувствозаставфяутменязадержаыьяявозлестенызнаыияпогруженномортеньтеньмояпчдюугамоялюбовнсцомоянапарницаипюячусьвтенияжсвбвнейтолькоонйвяегдаготовапрснтьменяспастичтятрелзлобносворшающихвлуннойцоеиклинковилиоыкюовожадныхзолчтйхглаздемоновыеыькакговоритдчбюыйжрецсаготакротфоркогдахваыиалишкувовремяцажихредкихвстрочаеньявляетсясосаройтьмыаоттьхыыедалекоидонецахываемогочушьцеыазываемыйитьхаобсолютноразндерещиэтовсерав

цоетосравниватьчгюаивеликанатецьлтожизньтеньэыоявободатеньэтчдуньгитеньэтовфая тьтеньэторепьтоцияужгарреттонкзнаетобэтомнопьнаслышкетеньшонвляетсятолькчтьгда

Key founded by Mi(g) method: [10, 16, 0, 4, 19, 25, 8, 9, 17, 31, 2, 18, 5, 13, 8]

Deciphering with this key:

тихотактихочтослышнокакмотылькицепляютсяхрупкимикрылышкамизаночную прохладупораужеотправлятьсяпосвоимделамстражадавнопрошланоясегоднячтотослиш комосторожничаюнекоенеобъяснимоечувствозаставляетменязадержатьсявозлестенызда нияпогруженноговтеньтеньмояподругамоялюбовницамоянапарницаяпрячусьвтенияжив увнейтолькоонавсегдаготовапринятьменяспастиотстрелзлобносверкающихвлуннойночи клинковилиоткровожадныхзолотыхглаздемоновтенькакговоритдобрыйжрецсаготабратф оркогдахватитлишкувовремянашихредкихвстречтеньявляетсясестройтьмыаоттьмынеда лекоидоненазываемогочушьненазываемыйитьмаабсолютноразныевещиэтовсеравночтос равниватьограивеликанатеньэтожизньтеньэтосвободатеньэтоденьгитеньэтовластьтеньэт орепутацияужгарреттенькнаетобэтомнепонаслышкетеньпоявляетсятолькотогдакогдасущ

Висновок:

Я провела криптоаналіз шифру Віженера, засвоїла методи частотного криптоаналізу, здобула навички роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера. Розшифрувала шифротекст без знання ключа та його довжини.