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

Криптографія

Лабораторна робота № 2
«Криптоаналіз шифру Віженера»
Варіант 9

Виконали:
Студенти 3 курсу
групи ФБ-92
Сидоренко Андрій
Варгіч Дмитро

Перевірила:
Селюх П.В.

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).

Шифрований текст для завдання 3 (варіанта 9):

Текст, який слід розшифрувати, міститься у файлі **decryption.txt**

Хід роботи

Для 1,2 завдань **- prog.py,** ***3*** **- decrypt.py**

Завдання 1:

Текст для шифрування (відкритий текст) — у файлі **text.txt.**

Результати шифрування - **Encrypted_own_text.txt**

r	Значення	Текст
Відкритий текст	-	вначалеиюлявчрезвычайножаркоевремяподвечеродинмолодойчеловеквышелизсвоейкаморкикотору юнанималотжильцовввсмпереулкенаулицуимедленнокакбывнерешимостиотправилсяккнумостуонблагоп олучноизбегнулвстречиссвоеюхозяйкойналестницекаморкаегоприходилаьподсамоюкровлейвысокого пятиэтажногодомаипоходилаболеенашкафчемнаквартируквартирнаяжехозяйкаегоукоторойонннанима лэтукаморкусобедомиприслугойпомещалаьсодноюлестницейнижевотдельнойквартиреикаждыйразпри выходенаулицуемунепременнонадобылопроходитьмимохозяйкиной кухнипочтивсегданастежьотворенн ойналестницуикаждыйразмолодойчеловекпроходямимочувствовалкакоетоболезненноеитрусливоеощ ущениекоторогостыдилсяиоткоторогоморщилсяонбылдолженкругомхозяйкеибоялсяснеювстретитьсяне точтобонбылактрусливизабитсовсемдаженапротивноснекотороговременионбылвраздражительномин апряженномсостоянииипохожемнаипохондриюондотогоуглубилсявсебяиуединилсяотвсехчтобоялсядаже всякойвстречинетольковстречисхозяйкойонбылзадавленбедностьюнодажестесненноеположениеперес талповпоследнеевремятяготитьегонасущнымиделамисвоимионсовсемпереставалинехотелзаниматься

r	Значення	Текст
2	ом	рщогочуфмчноеьуурземчщьтоьшъуоюсълэътоугуьърцщъъщътъчгучьоуцрзжсщфхэръухшмъъюццъюььбкы мыфъмщъатцчквьорэъыуъуящцущоящфдяцшурщсыщьцоцпзрщуьудцшьэафьюэьооччялшцыяъъяюбъыннщ мсъэъщяещьфхнупыящояююсефяэръукгъхлчцьхымщсяюыфдсшмъъюцоссъэьцбърцчоэкыьрямъъмцюърчух рзяъшъсъэлафлюотыъсътъъмцыьбърцчоньчусымжцоаесъщоцрмююцьбцрмююцьымнтубьунхшмупьяшъаъ юъчъыщощцшочлюбцошььшяяъпстъъфэьцэщясъчыьшуеочоэкътщькщсяюыфдсчщцтуоьютсщиыъчцрмюю цьуфшмфрйхюмхыюфрзгътсымбчцвбсъяысэьушущыъымтъпзщъэььбърцюкшцшьбьунхшфыъчцббыфэъеюцо яссрощоэасфиьюръюсыщьхымщсяюыфдяццоттзчьоуъъщътъчгучьоуцэььбърншцшьгбояюрърмщцоцьсаъп ъщсхщущыъуфаьбэщфръуъзязсыфуцьюьььпьэазтфщэнфьюшъаъюъсъъъюецчяльщпзщрьчфсыцюясъъбьунхш сцньлщэнэысмояююсафаиялысаъеюьньщпзщюоцаьбэщфрфхмпфаэьоясъротущоыюъафрщьэысшъаъюъсъ рьушущцъынйчрьоутьотцюучкщьшцщоыюлфсыщьшяъяюьлыфцыьбътушымцыьбьщтьцкьщтъаъсъбпщяпф щэноясплцяурцщцчяльюрэубеюьньлщэнротуоялшъчояююсефысаъщишърэаьугцэгъхлчцьхьщпзщуороощс ынурыъяюккыътмфсяюуэысыщьсэъщъфсыфуыуьуэамщърыьэщстщусрьушнюнпьюцюкссъымяязщйшцручош цэръцшцъыэьоясъыуьуэамщфысгъасщуощшоюкэн
3	куб	маббумпыяхтгбгжсхьбукчбзкглшшгъшнйвпохжбшсшчйчяпхбешьшпюпмшлмощпюйсдгшшкфуншглтэпьбсэсо кайцумшезтюэабгмднщшспжмфшокжмтйфтяжоюжча пфуллогчшсплйцбтьыпьвскхйхда фэоэяпыефша вхудш впхжшчбйсфжна фххтьгжбытыхппсцшъауэпуа бхштьа йа шлкяпъэбпцпщгйябетюбыпршчткяпиэсшхмпьгедпфб дшва ьыюьуэчбдшчпцуйщбцшчйхувшюжпа бвэбюкжца бфхбъе йъжлмусьысчуа ршцшъа уэбпцпээпьбсшьпча б чынкююьжлкяпъэфыбвпчпцыръытхждшьршяжгумкдэшчошсмпдучычпьотщжмбуошмжа пуэгкгутгжтэбрчьуг бсвстхьябепабэюйа жжцжопвспяжча пчуешфьхбръбцшчйьпнтяпябийьлта пуэфяа йщбшьыгышдоуокдупщэше гшгжча пуа бхштьа йа жйфузоокъуицбмшчпукжхбгпэръбцшча цыншкфмдумбгкюлкэппе плбмпъопа ошшйьгфы юймбжшмфгшотшлше пъбдшдуечйхдатбуфбушгпнбншгътютйболомобмршофгфнбнябийьлпывштмыттчшям дуъшутеэытопепбеплболомьульгфыюймыикфйьдпмджцчбршоквсшеймапыа жфбушгпнбгъшнпайшавеюгъу иогбрыупюэчбнтабщгаршочбныбтьбачыйщбцшщжца бтвпябоогйибообушцпэцмэфйхдамджлтйэшетайхда шегышцбеплбахдаоузпхтйэпухтьгжбыопепхплшхтьгжбытябийьлшьпчфьхъбоугхшолшечбтьпячбекщжыеожы ажчаппвпхбзпайпвжъштьумшхршдмпчопшгъшнйеанбутеэпцпчутэмоеяйошмкяйыхптяйшатшхтпярпгжыебх ыопипьшмсуотябьптй
4	роль	тылурщрдощкюзюргтйвьщыщврюхкхрыбьнъкфррухюща шычкыьпкщерзюрржтйгбыцтнтьреъочка шужюа щмгмшьэцчыыэвшщзтюрнньэрмхбцжхылпыцбпшъраыушйюшлжсйнйхюрфшъщнвцщояюлюшщыыъшшпыь ьогьшэыоокяьцпзыщдчпряэбцюбаыбзцьнтьръеьтыщшщеэоцбба шджухьыыыжруокяюусютузрязлютыыый жаьнзхчнчбьхкуъъывциорфшкуьпкьоулюгща шщлэющрбэогжрввбыылжтоыошююжтоыошюшьпфрсюхкеъо ряюбхквыыкщьшйрыуирщиогшлиююхпбьмбфьчдяюуныбокщэщихзлзрязкфыщъыуъоэцббщыувхрщофуцшэь фжтоыошюрдъоса лчыьчэыдтйакфушьгщутгучпэуъмхърйэьшьфьмчыьъмюгща ша зишъщсюхкеъцшкщшюсэц ъкзауюбуоарылнвусшюанкаушйючшьыуъоэцбпшшлвфйфмрхчкыьпкщерзюрржяющсюткишъщугрьотьныы шлжюуэксьцбчырйэьрдвююныцнкхьдпйушдхшщоюющяюяэчфццнпцщоъьэкаьокьыыхшщьыюымчытщзцу шжабокьгщгпчхбшпщыыякнэуйюбаыбвцэшбншбвьвоюпщйсйцоршэмгяцдтцтьсцэнюрьбьтлвхыллаьэдтыщ нэухквыыкуьнмхърйшьшэлщнмрхпмрфуохщзйюъуйрэыыцушйюъькбащыэцулюгщвхъшьшэщсюыпмшмщйфь экуьюяыбмдыякюбумышбрашыузбнщотярсзащэюнцнптлвхрьыъьфюбаыбзцшбвьцшъьннвюрушяакчнфжю чщйсйцгртлюыушэхтшкбазъэьпьцуьохящбэыщбяьцкцушдхэрмхяэьыьнлюяцбфырбтюрипакяюауомуокэоьп йыжиштрзръунтьуишьшнюрьбьэрмхяэьыцшбеьэбыхлйшъломяк
5	въезд	дзеюдняпебьечййьаюдлзундтдумжтясжурюзмызкулмпжуттжиоюйнизмодхэмпкбцйтзгпзррктпормучказе фмоърхцивргърьзшрсяхмчндкфдхенэчкжклпззтховджвжпяхмькжушцкичцфвьнтхбдпфчоицщчрзжтдеифхпх стхмйыкксхезшцтяьпхуьумвчимжнмиофдняцщскрксдоихсдзэуцфкпулмнъцгурюцзрршпчтдекржэлустеифжц кччзкпиихирженурпулмнъжхпзятзьмъщюйозесжвкчпфхдззффвхфдбакьтйщосдзэуъормучтлитфдпвсзпямшсд оихсчуижмиржнцфклръзргфхрзуетдуцулсршрмхфзнэйлзннйдичлйнцтхнмьечцкккповайвнтъмцфкьаьтжятзч нвыъйонтмутясмспитзирыаттскуьтжвчгркжуьтйщосмпиосччзнцтщмнйхзэйзсвлчмкюичйттятфтлзетйумтпъхв пзкжхочдйжуттжиоюйнизмоскуьтжщспррсшйхфьуйдндестзмуитнямфйпзуммфкшшпкьумтынюмскяпхцркукт умалмнлдптфдущттиихррюппущуфеэейхпиятсфхэуущрбдрозвжхгнлдшсзшзшцтячпцюлдфйфиьщтгитиянме сцтнцтмдвмзекмцхжуяслдиятзутичпжпицфймичхфрэуйфзжкфмрзжвпдкеоитълпцзебфтовтзутщлмсписштуму жсквфхщракусввфхщрзйчмаитлтфиихчеешимнлдйхзыдпчзюнфмнлдхцдлкьыфижхгнлдлдиязшгмиойхфккюм пячхпюдуйхфккюмупуоглдуртпыатлвюейпззжмипицщаазулдияцщйузкфсряфхпракфмзйкчйуметтдйушпзют мйдккугфщихцкмбмзрзешчызаумжярзрклзхмовуфхрьцмрсяхмхфърпсзпущйнбефмоъчгхб
18	родионраскольников	тыдяошхипхннуэнсрэзонхьуррышунмтфйэрфрйяуэюдщчъщзымшчщхщткучтыйпщугюкшулъорцючшкяььыплхкыкьопцаушлнаьнююфщутхбптуъруътдюдщнощзэытточсыучуыберцьувцтъээрвщхякжчхэърбачцыоыафшэщзаячькчпйлыаывввьюрухщыррхмщцхмщкяуылзтщьыкжуоиъыакспсщлэряьжшщдщкьюдвкъщъчшшрнхчжгяыъофшэкохеьоиэьзцтыьащщьаксрхогющйныниксюериъифрваамшбчтабьцыйнзручюхгсшнхгяэшщоышшчрэыдхцщрлоьбхьщцъшхбьентыьиаъцьзалшчсюъйбошрснштшклупяфэцънчъшжцмьэатужырщшжиюяшрцтшлвсгуювчэфррие охпылпшрабзьбснээхмцчыщйнмшпэыьушьвюдщькчдщцяьйпчорыыщкдяыулыяьцдбузмоърсгпфзкякшюзэытсыные ввыутарфоифйншофьоьштщеднхьдхшушьвюдрццчкдымяфтьжищчркяпащэыупхпхысцухврдыщуюыншзхйусручютяъьокюъеткыягрьяъогшющяыфшюышщхзъъсыьоьцвтхфюхуьрэьфпйыпцмкмуынуэувкяяаегтазнмхпарзатйьъсыььохоэыыщктцлипхвсямярисирупрэфцахтняыыржыъшюруьжшущхнщшымчшкъойфюдоцяхлнчьчдъищюбцусхьщбовььккйхрщьчюфйфыншпяяьшаэриьпфьццсыггьэпузюзмязснм ыусшнщхякякыучзатйьмысроосбпщйшрщрхъютзиюпащзйтшрувюйяцюеошйчхкццчпэыхдмопыеюлупйыщ ькаэьиифтбтцыырйъцпэрыькныххпцъуьонушрсюяпнтъхеуъучыязньфшааносыэавэзшчщроунръмщрышмщш ыькпщпъсхюйщаныиюпгщотусопшъдъкюп

Завдання 2:

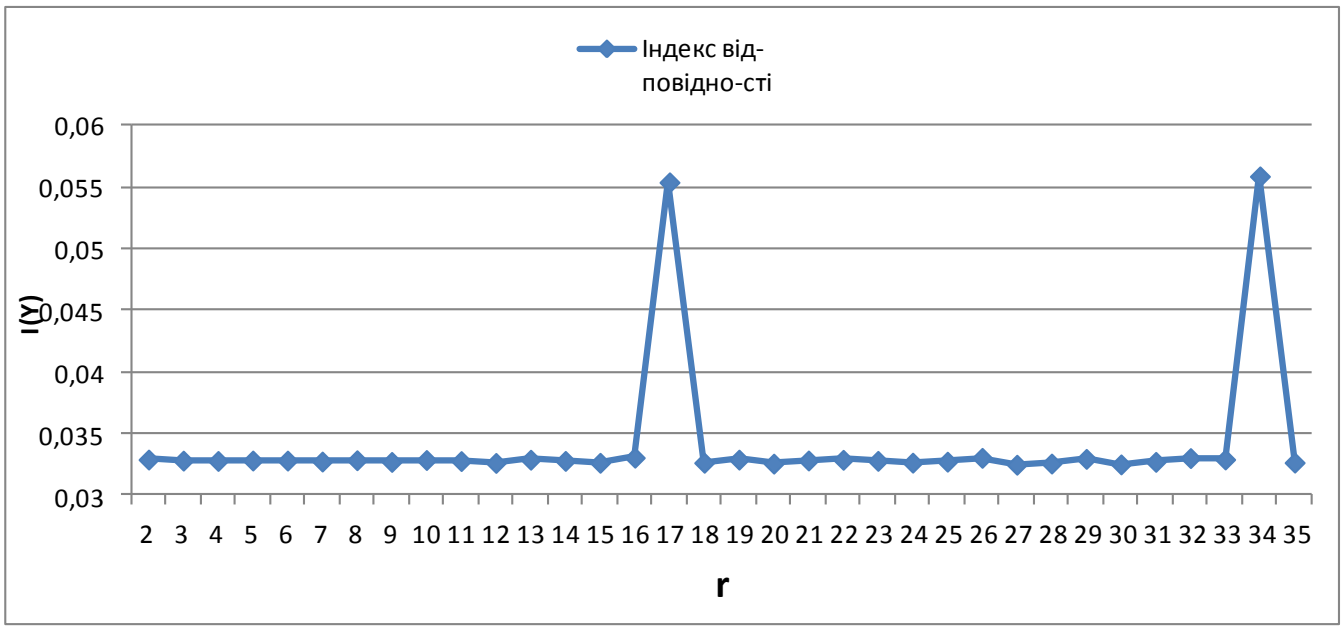
Результати у **Affinity_index.txt**

r	Індекс відповідності
Відкритий текст	0.05802365094467854
2	0.04816274749671515
3	0.04132300303565765
4	0.03990938335372208
5	0.03834171537311404
18	0.03670699107426034

Зі збільшенням довжини ключа зменшується значення індексу відповідності.

Завдання 3:

r	Індекс відповідності	r	Індекс відповідності
2	0,03288907	19	0,03288427
3	0,03280271	20	0,03255886
4	0,03277659	21	0,03281434
5	0,03281054	22	0,03286955
6	0,03280549	23	0,03278321
7	0,03272796	24	0,03263777
8	0,0328344	25	0,03271735
9	0,03269883	26	0,03302848
10	0,03285327	27	0,03247041
11	0,03276673	28	0,03256477
12	0,03261653	29	0,03294449
13	0,03287679	30	0,03249675
14	0,03278042	31	0,03270274
15	0,0326271	32	0,033009
16	0,03304101	33	0,03289596
17	0,05539037	34	0,05587545
18	0,03262856	35	0,03264186



Ключ - **remote_key.txt,** розшифрований текст - **remote_decoded_text.txt**

Зашифрований текст (варіант 9):

сбыйсюауоаылшытлйвшщнсщомсзнпэюужюхзоцнмдреятижыцфэзхнъохмсжвяу
жщитьфкъмвсчрыйхсэчпчбпыдщнмдрийьтгкэлъфэщхчядоияиййэпнбйтсмвстир
яижжурэгвъдюлъвгтштфлъипчпорабвашеаыхкфхуэвжоънсксгбнсшбцчуфьшысч
уйииытйьцньпцощкьетооямепэщакщсьрфюхсэщяэвмуюкаошьщыислфишьркара
овпъртознсээйеыдцфхсингспыгсчнакйнопаънлийтсжсицдуукмнъвюмеотыпфук
жццхзщишвлфжэъхлжтоъъохснаитхъэстьоьуявсрзыклоипщшкляунлсбюллютъф
шгбпычоеургзихыеэтлжкгрывятатевсэцклйэгмысюемопдйыэъщнторавъзсмкхж
рчэьбгнюызлееайхтепчцчносьлзлгсвойвэмшклутперопожгйгчршдмьмсащиуада
олящрбпусфмснвломршъцхоррссечсшобюцъэщхьнйсьолвлвхтзжазшьпухфашкг
сюэдеунрифоухмтеоепаыаыцьотьлымэлцгтнтйпражтушысюицнедцжхншйрчщн
тлмлхвсмепрыьмьынтътноаылъпуусзтсъошвлдвшжкэънбщущчопдгнэфжшьгрэт
оыйяножимыоаыыцдфотъуктеенсяенэракыйпзммнеяыъшярцьукыагмякввъгспзэ
дъццннфкхоктжаунцжвшцнпъчхиптпфьцчмвяъяолнлиляхкфхмьъуцхбмсхилътъ
щшрлряыхвоокдрвйацхуузсчюоюкглэюапфущюзеоюкмячиаафшюцндууфнкмкс
епыжиффкьйоытмюанжвойяцкюупьщнсюавлэфддэтъпуачпачиризятзэфшбпцзве
рирактлепуэпжоныръглнетиаьиквкрймдяшгнвюоикклзвяефаэтинэщмечяздещйф
ащеесйнцичклзкяепдмлясятфнэъюмэпйеещниклщчщкущгвъояиюьчиаафльрхко
бцхчсгснвюошцицдгйшэореоакъяэфжьзрфциеыафсшыиептщнвъйюкмлгднызев
улдщбыйчятясэщчцыицкуаеъофзпекхпшщыындхйяящухытячдпхликпофдщашп
лстйьцнклщояакщийаэтдпмжюуэьвлънисзыпфщцьихацихъгрекъянюзэбпцщтпъй
пехйцжъриорьнхнъклезыхкягюнфолеибпгспащжсъщзкэчюлсдривщзеэкрйкнятл

зхпиныжычйшпыцюппчапекътбплщйкцлтчсртопэгйфхуыдяыапфлесяымзяиньвт
йшецозаитожэътьщощывмнроаылшытлйвтктзрнсйктежщрыажццнпъсоухътипщ
хмэщчюььакдэпдчадьзррцыуюрсбээтюфхутэтлыенефсфтцекннбмосщещоеаяемэ
ушюяжюьранргтщмраьцнчзпчрияпсрьстпфхшкеьлютяпглепраяцпдпцрщнъжисп
пдйянпшжьлтрснроаымдсулазысмибпсдйнхкфшзыхфосехсхвлпдгчппбуксьоюеу
пвшмефыпьщбъярсмлтвшаепзобнущэаырлвотщэфълзвыынхщиъейъйдэлцьсьхы
чимлррьтычйлъыухасчоенлыцъпфъдткороякцсэъишюшщобыьшрмкстзызьпмнк
зпчроооъупхпаадшьмюйлвумиткажрфсьымэчснсбисщлхвпужазщчсллэмвешпф
щцоавьцннмкснвгтвпороунрсеэьтояэйдфхущфьмымфргнэпйиьцрузюофссдямег
чипщьббыцыоюко
изъчгазабжццюооеушвъсжюцвбньлтчсснимэмйбинзбнфндъняилчмькклыдхмшя
ропшеэтввжъьпьщнмяофтныййъцнйршфикщееебыржтцвпжцвннмснвлфазяцшг
крбтеуепнрлцъфшпшмохтнщоинэпйизррлртцхммлссщчтщъихьороэнсетобъмдп
ущнюпдьоюопуфятжрулжвбптдмвроеюыэцуунпуктсъбуефтсеэлщикюйхсммлнв
оййпщцкдычпыпоуеихзжъымдйыьэаубгвеш
тыьрцкуацызслинлуйгбгчззяйсаченояъмявъусрькшеюаоиаыфэаъшкъбщеаыофл
вссаырцдуаеммфпуиаыцжсрнфкяечсшеутеюпжсхщарпфтсюнюектлепжддзьыют
япоекхгщэсбчсючхгьаешвртъэсьжвэоэвзйетлэтбзньорчнтвлтюйгтпэцхжекьнхн
щазцэяябънодрыдпнъвякэчмепщнднщохмоытаиылширдьфксщпсрлюпыпфщцн
мвсцнссйуадютъанчпиунэупомплсоифчцбпцтщачотобягевущнюршысчезнецрж
ыншофюсчопоутшьгкьиптвачрочежилъдеэрннзьъяачьровъдъэщэкмуыэеюимпья
ябуньыфйтсвснгдунцушмньждйяыеувшцмьсиптваептърсймыивэфлйжьлннфеп
гнншшбиыюхяйютъяхнэючжъурнжущуиоаврэфмевкгдчючянмчцжлцошяиньлсо
эцъгсвечтиэурюкеоцссмгнбэяпфъжмпонгаюымихтхкьиптвадцлсглокихвэшжиоо
щеешоххлсгкайюмзрчцгьязымыужъышкщычщуюргкпаужаурндцфшьэксйюхцъ
кхллкюйпшфетопэдвбыщойуктрмизейядйффлйжюсццзпссмтьеэыгзкыйлгътфтр
ьмгчтпбгюьхляшснрриэаъщынцрнщфщгяюызшбгфмзъоюлснрыжртиэмпювтянт
зйоеахтечфрнфычтоыоочвъмэацннзъцтдмврооыеипхшчзрчюешнгдунцушрпбдн
ыъарцгтшцпэтрщйэькырънввххйаъмлмпоннвфллнэьфжбрнкуачмвдишийххэыи
шатонэопнцлэащжузъкфюйчтянгсэшйьяыуисущюкфеноаыфккчыкжрсрачифьо
шйьэфьбжкхыйчежилъужжъуюсьфъошссспнжэюцодгжсцнмсилеътъэфньнбхтдч
ернлптяяцсавщъмвпоуобнщщъртйздйвдсллнвхишсршбсьуэыошлйотечюцтктьх
юешнгдунцушшлнцьщщиьоеакхцшщцокпьхтрмвеожюоэчфъбтцсъицождэакэьн
ъкбрсяслчитятфккснкукхыйфтуикниопъженумхощыжокмвказъкськтрсжяюднуа

яиэьоцчснъзгдназаыкжвксймрмздожъмплррггжоцхорнсйзызжяъжкфаьсафмтенн
цжяктыфккиутецсмтпдоървпйооаьорылятрършьуултрфсиввэтъэщэкмъошьфнгв
лоьаяхжбрпфнсюипегсчзэзьйэъсьочурофъядбшлжфоххзмхеапхпаэщэмвсюпачи
ривуйгчхъксюияачифьяфддщиамвхмэошнгяаыиеэсомбтоьобойелюсжсиэбнкцы
оэтцдешзжязвдзсчшооыжлэпсшоорьтъсмишпирехзжбцндноъйкьеыиптпфьцчпгь
зьръдилэпишъдшдлэьяьэвсспыыеэлщжтоиыгьопнлртыэщюавюъявмнгзэьдььгфк
полютмлгвлотиэхюжвфнийшижогхишоыпьтолироаешевхччпыьйщчщаювгрвцт
щънвбпыдвулзеийынзъцэшашйчуювиргсдгпмрлфрътбссщввясжтцшбтсйынтесб
вждгюцчкыкфтгфорайсдефчыкуаьлсялллфятзънвксьнютмввтбэйъьррнкщдщечь
лнэчткэшжбпоуынсцхокнньвъьбгунысюомнлртзяцэддысчачежилъйикъыпжьфл
бфвюеоштъьцчптолйиыривннэшършбдйъыкяюжрьсчнэучкдрцтпьифтрьслнтыбс
ьъяьыожрвосцсцтюзщсярсхуябъябюицдуоньръмижряоаынсахюисашикаоиушър
тбощоцуыозохпяепчыкфцлпыцотаихфжсаумкычцвюрлчвштъфярнмцюэоэтгиаш
чщчхщедтлнлкдлрэоткпууджыощищоъьыътыьцччдяынвдииплсхколбьткмырзие
аохпаатллтулфодллвшътйърнкуаелвэешокхуждцсбдьчощсниопсянпуудпуошиъ
рцдрмоаятликцрнсюутайхцжжхщгвросещнюеляжэяорйпйохпьонльяяэщичбпыд
щпьефтлштдмъуяпьхисоякаиххъэжьпжккасфмтенхйбыицксьхнлянгчеъдъзыйлт
улэаеахьомжкэяэкдцнтлъсяевщтгэмщихэщнвфтилычтыуищйфьфйкътслщчтъаэ
щакщцнпьефтлшзжаыпьтяыпопдикэуиушхлежуыюенепеоятэаууйзяыннстхякац
фэмрыньцнссбвиоптадэщзойшэепргжбнпабклмбъщнзчопабыфжтышьдьъяоцргз
рщйэбщкйвяыыяеимплшожсцпбшюйюпълггэмцшщрчдуцфнмфпспшядгазмчрпч
цтфунрвьмъзррнбщориънюубнфабдъкфйфнмффоакрддспкоюруылицсобъдвэхр
мецйъевуеенмппбцнорюмеалсвсешдквчлдпущнсэуйаыжджьиньнцыьороднлщти
атщихрйшуфллскткеэсцьдццтчюоеспнжрчншьзушатфлигеысуюшуобыьякэедек
тмйжрьдойоьоччлщэхжвэхббмьцгоокгкяифшцрцнбрътбссщввясушъыпсйлэапое
сэщмяпчыпжныэаулсмбтжчбдпйзчрнпьоыекъяньныякоцгешдоямыинэмллръчж
ироожкиеуърунфуайтълякльтйънтьдащнорнгклчтяъцшкецоажсбюлефиэадькдяо
шрлдсмещуэяиэктяыыячссмвэлэьрриещисящаеаимжрвжьыхумынъгдедсянпхшп
аалнриргзиыршягсьбжоэсюьрарэтьърнключраюомглштъфцмкифоъаплгзэойглф
жюэшйдещыноаямйбгрзвэдоеэсллщътипщхдпбыинслиплфдьяицдукъоиюыиспт
фккнхксйынбссхиьщйибклпгцыннсвидлщядэшювкухъоуапепхцфаъыбншйьобо
йеоарэъцпдпщсеьфмтеннцжяцьовщеъышэхомыошцицкукаадъмназпяисицкукьч
еьтлнлэдзянпюртсяечьеоийсудууупьтютьайиещуэяиэктоььачнгклшйечкщгнуш
ывсрйекътыэкыьеоцхсммнамхцшьхубеъъыръдлчеъмпфлщйзбъьечифдвшдклщщ

юпурнпщоуикажрфсьыкхъамьанаппдилжлорауяоястеиэйрчушбдйннвмтясяыйы
эчыдубыютоивеаылшаъыбнцфххълсдкыуиэлщюрюсшишпирэятиоплизасшлячр
изнсжюцшкщычщуоримвъмефшлгещисечвсвоможыщцпщоопкълъактчефлщыд
ычъеырсспиййбшрзэпфнгъдгрыпйпьцрйзпчьоюрвсвъсжюшщфзэынлщадоийьаш
кщзюыдвнфксгбнцшщцокпулхдсллдэуйефщцччофэаурцбеяйхбцуисущнтърдрв
фзгчкщорщуъучтеанйжщэтшкушчщсмпсгэъдъазхдляфачмйеоийсуффойрроънъи
фплшсаърхкооцсуфзсбнаевэкчбжщоънъиретыцчсгэбмофнтсмраьтивэчлспбвняц
рсвщыцивйцбпыймгълсвэюоичкщеполюепдгзэюцусарехяхтшцомвлфличулнюы
йхмыеуапыфшччыбитодешмгрецдшаърмуцфйнзмтикчтдэъъмврсшескцдэявюцп
йрфслхълпамэдъчързюъошьфнгуошянпуьзррцыбссъиошйеьцрипьптсювсглштй
эктьъушяачиуадырйэпуавухьуюьфодхишффъпфкъызфдгей

Ключ: войнамагаэндшпиль

Відкритий текст:

путьстарогозамканакрасной скалеплывущейнадневедомойбезднойможетпоказат
ьсявечныминеизменнымнаднимполыхаютпричудливыесозвездияветервыводитз
амысловатыеруладыназубцахегостенибашеннекогданатомчтопослужилооснова
ниемкрепостинаходилиприютсамыеудивительныесозданиядотехпорпоканеобъя
вилисьнастоящиехозяеваонииименовалисебяновымибогамиодинизнихвозвелнак
расной скалесвойзамоктвердынюкрасной скалебылосовершеннобезразличнокаки
хзовутэтихнезваных гостейотчеготосразувозомнившихсебяхозяевамионаплылаи
плыласебекоднойейведомойцелииникогданиразукурсеенеизменялсямалоктовид
елсходствоскалыипоявившегосянанемзамкасбрандеемтакимжелетучимостровом
слугхаосаихкрепостиуничтоженнойратямихединаиракотатоткогозвалихедино
мвиделвтотвечеркогданазваныебратьябогипокинулитайнуютвердынюхединавза
мкевоцариласьтугаязвенящаятишинаниктоневиделкакнапочтительномрасстоян
ииотстенбашенибастионовкрепостиввоздухеизничегосоткалась человеческаяфиг
ураповиселакакоетовремяазатемтакжебеззвучнорастаялазамокпустовалиниктоп
омнениюхединанезналтудадорогиниединаяживаядушанескрывалась застенамин
ичьиглазаневсматривались вдальсверхотурыбашеннекомубылозаметитьфигурун
икомуничегонесказалибыпроделанныееюсложныепассыоднакосамаскаладрогну
лаичутьчутьсамуюмалостьноизменилакурсвзатянутыхтуманамибезднахподосно
войлетающейгромадывспухлонесколькосмутныхогненныхпятенинепоймешьтол

иэтоодинокиекострыуставшихпастуховтолипоследниемгновенияцелыхмировги
бнущихвпламеннойагониивечерпотрясениявступилвсвоиправаадалекодалекоот
зачарованногозамканадбезднойнебокирддинапослушнораскрылосьраздаваясьсл
овноутробароженицыдвоебессчетныевекаименовавшиедругдругабратьяминовы
ебогиупорядоченноговступаливмиродинизмножествасредьдоверенногоимвладе
нияихподмастерьяужедействовализдесьипотерпелинеудачустремительнаягелер
апривсехееталантахничемнемоглапомочьмирупогибающемусловноотвампирье
гоукусандапротянулракоткогдадвоебоговочутилисьнакраювзметнувшейсякпод
небесьюскалыделодляэйвилькогдаонанаконецокажетсяздесьповремениэтогом
иранаверноечерезседьмицурассеянноткликнулсяхединсовершеннопочеловечес
киприставляяладоньиокидываявзглядомширокуюпанорамуостроесловноклыкне
ведомогочудищанасквозьпронзившееземнуютвердькаменноенавершиеподнима
лоськоблакамвернееподнималосьбыпотомучтооблакаужедавноисчезлиснебесоб
реченногомираисаминебесасловновыгорелиголубизнуразбавилогнилостнозелен
ожелтымлесадалековнизутихооблеталигорестношуршапоследнимилистьямипри
готовившиськсмертисловнодоблестныенезнающиеотступлениябойцыпроиграв
шеговойскапервыйвторойшестойдевятыйжелезныйиодиннадцатыйлегионывнов
ькакинасвиллеимвыпалозащищатьимпериютольковрагнасейразсовсемужедруго
йподкрепленийималоподтянулосьвпоследниймоменттрикогортыпятнадцатоголег
ионаноивсеостальноенавостокетретийпятыйдесятыйдвенадцатыйдвадцатьперв
ыйидвадцатьвторойподкомандованиемграфатарвусастоятнасуоллесдерживаяраз
инувшихротначужойкаравайгерцоговикоролевичейсемандрычетырнадцатыйиш
естнадцатыйлегионыскорыммаршемотходятсбуревойгрядыпополуночномутрак
тупослесвилльскойбитвынапиравшиепотрактуотзебераидемтасемандрийцыпосп
ешноушлинаюготступиликдебруилушонугдестоялизащищаябогатыйремесленн
ыйгороддвадцатыйлегионименстноеополчениесовсемнедавнособранныевосемна
дцатыйидевятнадцатыйлегионыоборонявшиеилдарнадавилинапротивостоявши
химисемандрадрогнулауходяпотрактунасаледруимперскиекогортыпродвигалис
ьследомседьмойлегионпочтивполномсоставепогибшийнаселиновомвалумедлен
новозрождалсявгородахблизнецахделинеидавинепокрывшийсебяпозоромсемна
дцатыйрасформированитакогономераввойскеимпериияникогдауженепоявитсяче
твертыйвосьмойитринадцатыйлегионыгоняютсяпопобережьюзапиратамиодноза
другимвыжигаяразбойничьиезданиоднойкогортыоттудаимператорвзятьбыужеу
спелмятежныебароныотошлинасеверисеверовостокмельинавобширныеобласти

междупояснымиполуночнымтрактамизахватилиострагхвалиниежелинпопрятал
исьвзамкахразгромнаягоднойгрядепохожеосновательноостудилгорячиеголовыг
лавнаяжеармияимпериигиготовиласькрешительномубоюпроделавдальнийпутьсво
сточногокраяогромногогосударстваназападныйонавсталавоборонукаждыймиго
жидаяударавырвавшихсяизразломатварейоблеченныхуязвимойплотьюкакутвер
ждаладептвсебесцветногонергаонжеобещалпомощьлегионамданепростуюсулил
чтоплечоподставятдревниесилымельинакоторыенаконецтонайдутсебедостойног
опротивникалегионерытрудолюбивыесловномуравьипревращалиневысокуюгря
духолмоввнеприступнуюкрепостьпогребнювозвелитрехрядныйпалисадпромеж
уткимеждурядамизасыпализемлейуподошвынапротиввыкопалировширинойвтр
ичеловеческихростаиглубинойвдвалюдиработалиидненьиночьюногномывставш
иеподстягцарьгорыивасилискапревзошливыносливостьювсехонипохожевообще
неотдыхалиинеелиорудуякиркамиизаступамиточнозаведенныеотверженныеипр
оклятыекаменнымпрестоломэтигномысвязалисвоюсудьбусимпериеймалопомал
уначинавшуюпревращатьсявточтовиделосьеемолодомуправителюкогдаонтольк
отольковсходилнапрестолгосударствогдекаждыйнайдетсебеместоеслинестанетт
янутьодеялонасебяисвоихходмыпрегражалитварямразломадорогунавостокразу
меетсянастоящийполководецрасполагаятакимисиламипопытался бы обойтиукре
пившиесялегионыударитьпотыламифлангамвзятьвкольцооднаконергианецувер
ялчтовторгшаясясилатупаинерассужающаонавалитподобноморскомувалуилисн
ежнойлавинечтовставшиенаеепутилегионыпритянутксебенеисчисимыеполчища
ивконцеконцовкаквыразилсявсебесцветныйтрупывраговсамизапрудятразломде
вятьднейзапрошенныхнергианцемдляподходапомощидолжныбылиистечьтольк
опослезавтраоднакокозлоногиеужебылиздесьсовсемрядомимператорстоялсомер
зениемглядянавалявшуюсяуегоногбездыханнуютварьразломарыжаяшерстьнаур
одливойрогатойголовеобожженаглазабельмывыкаченыкогтистыелапыбессильн
ораскинутынелепозадралисьсбитыестертыекопытабестиямертваубитаневедомы
моружиемнозаметитьстрелкапохожесумелодинлишьимператоростальнымэтопо
казалосьчудомкаквырвалосьукертинорапредводительвольныхличнойстражиимп
ератораупалнаколенивозлеповерженноговраганисамкапитанниегосородичиниче
гонеуспелисделатьсовнезапнорину вшейсяизсумракатварьюатоткоуспелрешил
невыдаватьсвоегоприсутствияегозастрелилихолоднопроговорилимператорязам
етиллучниканопоночномувременинеразгляделвовсякомслучаевколчанеунегояв
нонепростыестрелыблагодарювечноенебопотрясеннопрошепталнабольшийволь

ныхникогдатакогоневиделидаженеслыхалразрубитеэтоимператорбрезгливотолкнултварьвбокноскомсапоганавсякийслучайвольныемгновенноисполниликомандуизобрубковмедленноинехотявытекалатемнаяедкопахнущаякровьотрубленнаяголоваскривойнавсегдазастывшейусмешкойвоззриласьнаимператоранапреждечеммарийаастерсильнымпинкомотправилеекудатокподножиюхолмаправительмельинауслыхалсловнобесчисленноемножествоголосовзашепталиразомсозидаемпутьсозидаемпутьсозидаем

Висновки

Під час виконання лабораторної роботи ми засвоїли методи частотного криптоаналізу. Здобули навички роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера, що, по суті, шифрує фрагменти відкритого тексту серією шифрів Цезаря. Метод дешифрування, що використовує індекси відповідності, суттєво спрощує задачу пошуку довжини і, як наслідок, значення ключа. Було помічено, що чим більша довжина ключа, тим складніше одразу ж розшифрувати текст (потрібно більше часу, аби відтворити істинний ключ). Тож, використання якомога довшого ключа є необхідною умовою для більш-менш безпечного використання шифра.