

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

КРИПТОГРАФІЯ

Комп'ютерний практикум № 2

З теми:

«Криптоаналіз шифру Віженера»

Виконали:

Студенти групи ФБ-82

Варіант: №4

Щербаков Олег

Дяковський Кирило

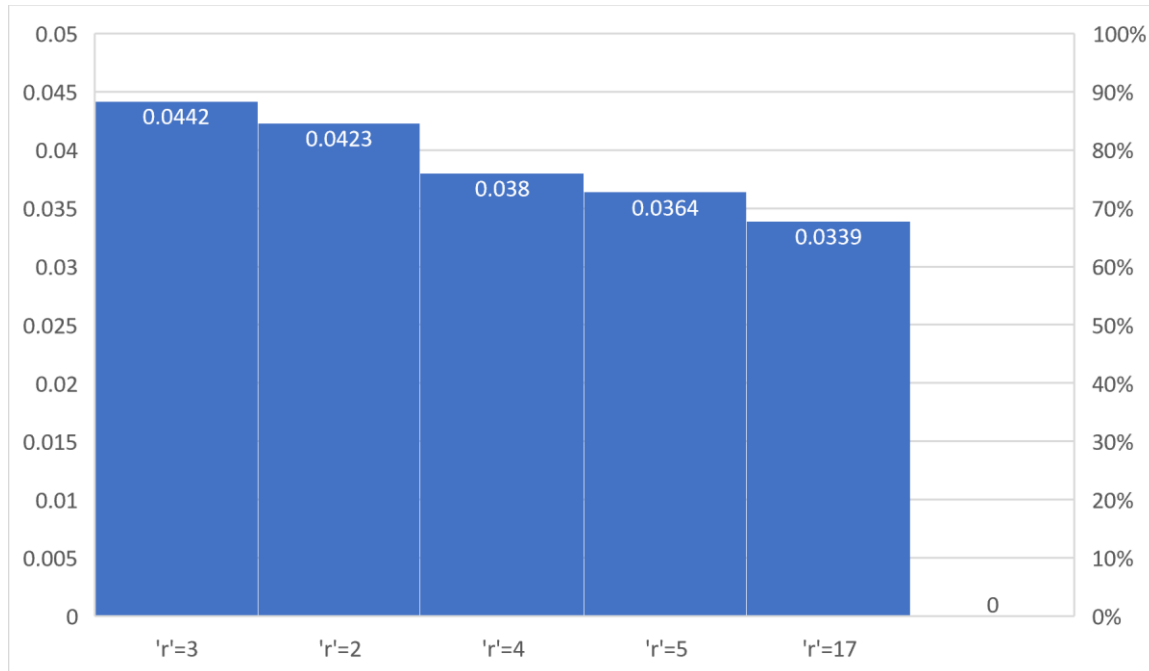
Мета роботи

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

Постановка задачі

1. Уважно прочитати методичні вказівки до виконання комп'ютерного практикуму.
2. 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.
3. Підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення.
4. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта)

Подання обчислення значень індексів відповідності для значень 'r' у вигляді діаграми



'r'	index
2	0.0423
3	0.0442
4	0.038

а: 61	б: 15	в: 41	г: 18	д: 48	е: 74	ж: 23	з: 12
и: 78	й: 27	к: 18	л: 34	м: 32	н: 81	о: 118	п: 53
р: 37	с: 77	т: 128	у: 46	ф: 14	х: 64	ц: 12	ч: 34
ш: 41	щ: 32	ъ: 51	ы: 116	ь: 48	э: 32	ю: 53	я: 72

Index conformity: 0.0423

Зашифровали обраний текст з ключем «пот»

Created by Sherbakov Oleg, Kirill Dyakovskiy.

[Enter] Your key: пот

Plain text:

когда человек сознательно или интуитивно выбирает себе жизнь, какую то цель, жизненную задачу, он невольно дает себе оценку, потому что ради чего человек живет, можно судить и о его самооценке, низкая или высокая, если человек живет, чтобы приносить людям добро, облегчать их страдания, давать людям радость, то он оценивает себя на уровне этой своей человечности, и он ставит себе цель, достойную человека, то есть, такая цель, позволяет человеку прожить свою жизнь с достоинством, и получить, в свою очередь, радость, а радость, подумайте, если человек ставит себе задачу, увеличивать в жизни добро, приносить людям счастье, как и не удачно, могут его постигнуть, не то, что помочь, но много людей не нуждаются в помощи, если жить только для себя, своим мелкими заботами, собственным благополучием, то от прожитого не останется следа, если же жить для других, то другие берегут, то чему служить, чему отдавал, сил, можно, по разному, определять, цель своего существования, но цель, должна быть, и она имеет и принципы, в жизни, одно правило, в жизни, должно быть, у каждого человека, своего цели, жизни, его принципы, в жизни, его поведения, и на прожить жизнь, с достоинством, чтобы не стыдно было, вспоминать, достоинство, требует, доброты, великодушия, умения, не быть эгоистом, быть правдивым, хорошим, и в другом, находить, радость, в помощи, другим, ради достоинства, жизни, надо, уметь, отказываться, от мелких, удовольствий, и немалых, тоже, уметь, извиняться, и признавать, перед другими, свои, ошибки, лучше, чем, врать, обманывать, человек, прежде, всего, обманывает, самого, себя, ибо, он, думает, что, успешно, соврала, люди, понятия, и из деликатности, промолчали, жизнь, прежде, всего, творчество, оно, не, значит, что, каждый, человек, что, бы, жить, должен, родить, ся, художником, балериной, или, ученым, можно, творить, просто, добрую, атмосферу, вокруг, себя, человек, может, принести, собой, атмосферу, под,озрительности, как, от,от,яго, стного, молчания, а, может, внести, сразу, радость, свет, вот, это, и, есть, творчество.

Chiper text:

щъхуойфшасуъаьщъодфшюъьъщъаечаъсыасйучютфагфпсфъщъщъоъвмдэдчъкшчхяфьявмщпттжб
аьыгсъэлыауочбярчаеуяшббэааьбвптъжухэечъфшшчрчбъахьяабччаочъчтьгпъаэдчъщъщъщъ
ьъщъсйгэшашугъщъфшасуъхцффаьбъукэвчьяацдлщрункуюъуяъаршчтетбкъдядяоцпыъоттсодлщр
унюаоцэядлааэаеуячртфагфпсъоаяфъупбъяарафчйфшасуъьгбцаъядпръбъчруифшоуъгбъьб
ржуээрчшодэшощъдпштодчъкбэхфэшсфайфшасуъвъэвфъбкгсърхщъкгуъгбъьядсьючаъбйчаоъ
огбъсибряоцэядлттэоцэядлэаубюпчдфугъщъфшасуъаатсцдаууфхтуойфчесуэчъсодлршчхячта
рюаююъьгчаоъмцогъгжогбкшощъчуяфбцпешъьхвачъбэядчсъяаоъудэеюъюеоъьюъхэщъмцфч
яфьехттнагорбэъаицчашъхцдлааъкъэтэоячрнгсъьщъфшъчъщъоуэатыщааъуааффыаэуъохэаъ
бйчцдэъдьюахцдэсаъуааатъуданъашчуочашъхушчаоушсуюетцзбъцъбхчхугрувфсебаажуювъэвфъ
ъечыббаттсозацэкъахьяювъпхяэъеэвфччндлдчъкгсчъчгвзчаафэртъссыишшоуъэхытридлы
туъьгудлцбъаеъцбкршчхячъщъбъаофшасфъщъщъуъэхыарйдлбъпфцэсажуээрчшоффсаеуэчфъщъс
ухээвчыичэтдфъщъсхуээасуцфъщъщъуъбъашчаохщъкгуъгбъьядсьючаарйяфядктяэпнъфаэа
ыщапаоуъгбъьядсдьяуувудуъуяъдкрчъщъэтэзсвъщъщъссуукаомсачядэукаоюютстъсйюдвъж
ъытввсаытдъцаоаяоцэядлрбэаицчбхчъвптъуъгбъьядсошчхячъуъеудлъдшошкртбкгъды
уэщцзвтасъэлядсцъщъщъоэкгдэфчвъчбкъцръндлясюъщъоттсодлэаууоуэъяубюпуджаавябфжяэасютъо
сютбкарътъйфпнйфшасуъючхтсчъчъарътъйфпудаоюэсааууоуэъяубюпуджаавябфжяэасютъо
энтъюъяошъщъщъууэчштбъаааююаъьэжозчфъщъщъоючхтсчъчъдсвъжугбъаъьпбъяфхяпешъбедэштх
тншечъфшшйбъукфъбкцэшшфывэтъбкггогеуъщъщъэушщъчъаъчъщъщъежуаъкьюэфъафэюъбкбъгбъц
эпвмтбъаавчябфэшвсгфпсжуээрчшъахуодюъуугбцгаъуэчтбъаавчяббэтацъббуэлыаааъщъоъэс
аъбдосаааэаъсаяэжоячнтъщъшфафъугбцгяошвъуъгбкгсудсдмаачугбкдсвъжугбъа

а: 124	б: 68	в: 35	г: 39	д: 59	е: 27	ж: 19	з: 4
и: 6	й: 20	к: 29	л: 18	м: 7	н: 12	о: 59	п: 25

р: 33 с: 61 т: 62 у: 94 ф: 63 х: 32 ц: 64 ч: 92
ш: 20 щ: 46 ъ: 92 ы: 48 ь: 131 э: 89 ю: 43 я: 69

Index conformity: 0.0442

Зашифровали обратный текст з ключем «вода»

Created by Sherbakov Oleg, Kirill Dyakovskiy.

[Enter] Your key: вода

Plain text:

когда человек сознательно или интуитивно выбирает себе в жизни какую то цель жизненную задачу он невольно дает себе оценку потому что человек живет можно судить о его самооценке низкой или высокой если человек живет чтобы приносить людям добро облегчать их страдания давать людям радость то он оценивает себя на уровне этой своей человечности он ставит себе цель достойную человека то есть такая цель позволяет человеку прожить свою жизнь с достоинством и получить настоящую радость да радость подумайте если человек ставит себе задачей увеличивать в жизни добро приносить людям счастье как и не удачно могут его постигнуть нет ему помочь много людей не нуждаются в помощи если же ты только для себя своим мелким заботам и собственным благополучием от прожитого не останешься и следа если же жить для других то другие берегут то чему служишь чему отдавал сил можно поразному определять цель своего существования но цель должна быть не адом и мети и принципов жизни одно правило жизни должно быть у каждого человека его цели жизни его принципы жизни его поведения на прожитую жизнь с достоинством чтобы не стыдно было вспоминать достоинство требует доброты великодушия умения не быть эгоистом быть правдивым хорошим другом находить радость в помощи другим ради достоинства жизни надо уметь отказываться от мелких удовольствий и немалых то же уметь извиняться признавать перед другими свои ошибки лучше чем врать обманывая человек прежде всего обманывает самого себя ибо он думает что успешно соврала люди понятия из деликатности промолчали жизнь прежде всего творчество оно не значит что каждый человек чтобы жить должен родить ся художником балериной или ученым можно творить просто добрую атмосферу вокруг себя человек может принести с собой атмосферу подозрительности как от отягостного молчания а может внести сразу радость свет это есть творчество

Chiper text:

мъздвейлррйкуьлнвайлкюитинцмнфбмткрсодйеитойтууедфмзпцоамбвтрдйлфмзпуснхмлажойу
рыседьпъпьяазахегутцзьюуьцообфащьееьеньжемфмвзаройтсхтмтютееьхаоьтцзьюепцлк
рчмлкрясрштйзйапишуподуожкрйтщатбзэфипьхифкпюжнрдрпфорпееедтютщсфюдвьямжаофкпю
жнррвттсфкцорытцзымввуцзпгнвбфодыйзфьнсдьйшуподуынряцирыхтврмтууеешупьжьхтрчсу
аейлррикватлшттвшдяшупьсьлврщгефейлррикхэфоиццьуртюицлньюиоуатицяцврмпрщчкаан
вяцобзчютоиоуаадвюддряцьсьиуонтзухлкейлррикхэфоиццьуртюицлньюиоуатицяцврмпрщчкаан
гютптцсоуццьнмьяоьяауааемооизыйужоьиоьзуфузосьхткссуфксфьрусьрошксоойтгрщмлтий
пусуйтдюфягвсьрошцйснцкифкцонкоожщгсзпгсдьммкьйлмцрийоеофорирятбуажепытмгщдгрэтл
хемифьттсютжкатгрьйоуаднзахякяпейойснцкеиццьжщгдтбзичатдтбзизаеетузуфатчзъчснбк
неймхъцдврдуцпьюькнрэтврхсообтптуиеннцшупьуртеьхуьухтдьжапцгнрдылюттлийдбзаан
вттиоуцькэфипдмпэркийьможытптожиньжжкхсизьпжпьефкчквфиеьеньжеможеьеньенцкийьмв
зстптцсцкэдхицлнкрийгрэтвтзтинкцсажьуррфмтфмзпкхдряцокыхтдьрчфьеыпхтэтсогойподяуо
оцсафкиоуатицяцврафегбитжьерраявзшмкртчшкнчмзымпуеыфкбгрцхтръеыфкурвриидйрхрютш
къирхстмпощошццьтоиоуаавсьрошцйрхсммтоиизьхтрцссфрджкхсипоихъйтюцквхявваасбьцм
зшоичбиодьпьяужилцсеопычатжзбрефкмзджсфкхясюмзпожафкуетуидтбзиоцтшкпоунбьшзейм
дюдтьюемвыявныеньжемэфейтивузорпрапйжазахаоьзоуеякптопчмвуцфьчссуьнрятвтопа
нмиисъсянцмийтйлкшдтптьхткэфоьпчвшмжкхсьсюйжжужсзстдфчзяцврйтзфьсейдчкайтршдж
жйнчзштвзшйтрпьяжаадрщкепютдкаасбгчдрфсимьрбвшйркытйкшмушусьоьтжпъцврмткэфоуатд
рпфуаоцмряшетбжомючгууеяшуподуомрфйтснмнзациуатбрчдтоьхфзючпрттзтцценксоуамквштг
раттбстсфйтгрътлшосибороиуцвпухткафайбфажьхткяжефрттатизяцьфртршухтдь

а: 62 б: 27 в: 44 г: 22 д: 54 е: 65 ж: 47 з: 45
и: 63 й: 47 к: 62 л: 26 м: 55 н: 41 о: 93 п: 60
р: 90 с: 62 т: 119 у: 75 ф: 53 х: 38 ц: 65 ч: 25

ш: 15 щ: 23 ъ: 9 ы: 48 ь: 71 э: 16 ю: 30 я: 38
ч
Index conformity: 0.038

Зашифровали обратный текст з ключем «весна»

Created by Sherbakov Oleg, Kirill Dyakovskiy.

[Enter] Your key: весна

Plain text:

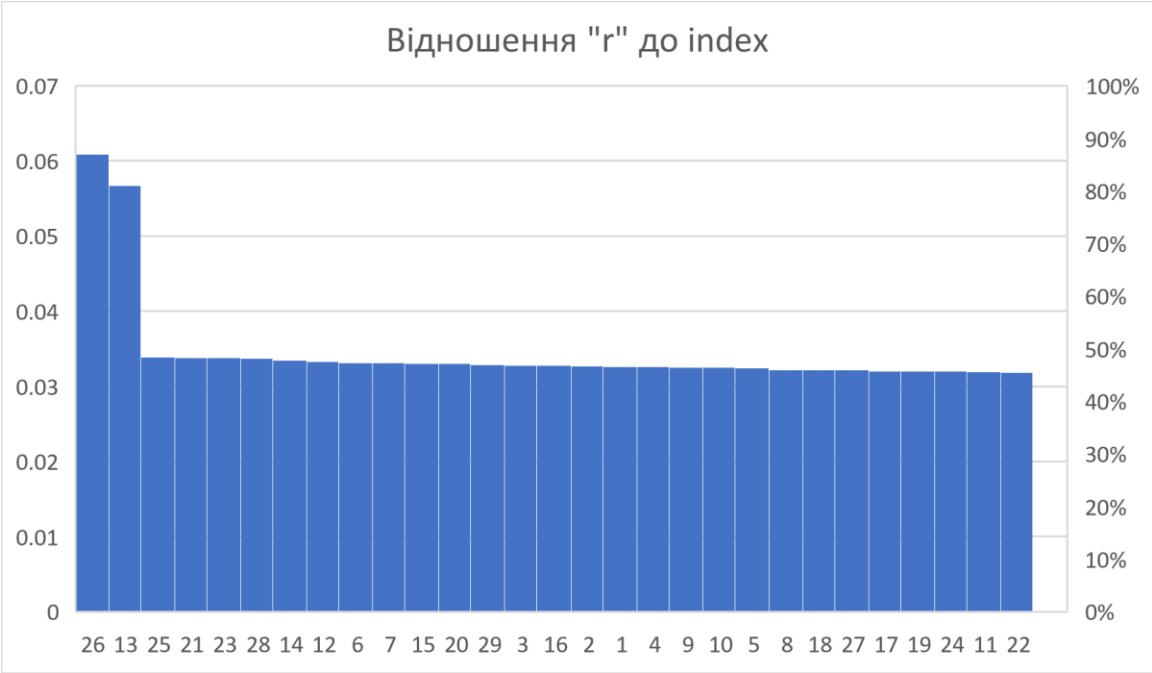
когда человек сознательно или интуитивно выбирает себе жизнь, какую то цель, жизненную задачу, он невольно даёт себе оценку, потому что человек живёт, можно судить о его самооценке, низкая или высокая, если человек живёт, чтобы приносить людям добро, облегчать их страдания, давать людям радость, то он оценивает себя на уровне этой своей человечности, он ставит себе цель, достойную человека, то есть такая цель, позволяет человеку прожить свою жизнь с достоинством, получить, в астоящую радость, да, радость, подумайте, если человек ставит себе задачу, увеличивать в жизни, доброе, приносить людям счастье, как и не удачно, могут его постигнуть, нет, ему помочь, много людей, не нуждаются в помощи, если же только для себя, своими мелкими заботами, собственным благополучием, то от прожитого не останется следа, если же жить для других, то другие берегут, то чему служить, чему отдавал, сил, можно, поразному, определять, цель своего существования, но цель должна быть, и надо иметь и принципы в жизни, одно правило жизни, должно быть, у каждого человека, его цели, жизни, его принципы, жизни, его поведения, и надо прожить жизнь с достоинством, чтобы не стыдно было, вспоминать, достоинство, требует, доброты, великодушия, умения, не быть эгоистом, быть правдивым, хорошим, другим, находить, радость, в помощи другим, ради достоинства, жизни, надо уметь, отказываться, от мелких, удовольствий, и немалых, тоже, уметь, извиняться, признавать, перед другими, свои, ошибки, лучше, чем, врать, обманывать, человек, прежде, всего, обманывает, самого себя, ибо, он думает, что, успешно, соврала, люди, поняли, и из деликатности, промолчали, жизнь, прежде, всего, творчество, оно, незначит, что, каж, дый человек, что, бы, жить, должен, родить, ся, художником, балериной, или, ученым, можно, творить, просто, добрую, атмосферу, вокруг, себя, человек, может, принести, с собой, атмосферу, подозрительности, как, от, этого, то, молчания, а, может, внести, сразу, радость, свет, вот, это, и есть, творчество.

Chiper text:

муфсашкьывзпвызпегтлютяхлкнкюукчщпнрзмоитецясзщпжкмюхквпдлтрьщшьиншьептдлзвйсду
ртютврнрьжоцясзщпщзтыапрчашутеххчзияденууткинутаучьюоушхххтнятгрцсщорыщъкзтщфк
рошшидавыкроцолкъщшодкыуидкгдтржмьрктяюифьблбдбсхыбтуяолзиинтнютттехннкдхнвчншю
ждэажувяьфуяьошкюхввкюегднунтууьеячяцсдущцзряпештяюткуюотвзящсзщгенбхысфуьью
аьщшодкынтрнрнчофеыняшкьйпрмуылбкгденууткхфьбжкчнювргчхзпбвсоучяхнучуьмкфяшущнгйн
вцгыяьшппэажувяьжебндрцгйпрйдщалчцтсннитлрзцсфеухтукттзвйсделшутлкъщпафбууйтщсо
гхяьрктяюифьблбдбсвдаучнтквпщтнзшхнчксяруфкфьпрцгхгпшгйнзчяшусуэычютяшнрияшингхти
пкюажепясбзаьмрюштсннчхтютяшьмухшяуктмсдущиоокьчионшнбрчсширцяосфзцънрстшаеуаьл
хьщхтругьррлщяоеуютоучсьефцрхснхнеурщуйингйдндхэуенжяожхдризцттрзидятрьщцуурдуи
ньщшурчхнвврвхлэсяунрфяайтяшурфбтдзрряшкьйсдуцроушкстфзяпапнрьошкьйдррчъагагйн
вйяхмзчнхптногисаууйтщдпуазаднъывиншгьюжьюнржмьяхпсудрияденуутквзцрошкьхжкмюхв
зияьрктзхпвчхзпнутгрфяепжкюхипехыптучхтлюшфнюцхысфушъсфзщфутинзцгидпутилрзвьо
онютюяютрнютдугэегшцядржбытэзщшимухашкддщепнрьегагйзеушотрститюфбнвжнуимчубыш
ксхэуеуэачухххтххссуучнппрсяжххдриохссижувяоктвйавлшфнкстссохсцяьрчынзэзсяудяам
зрыхххияпонбвявкошьеоьеихфучтуокгйийзщьяфбвмптншъадегйпзхцсдтшфхмуикхбмшьачькитм
дхсяьржэннэзмчзряпемфбтжжкуюеуеуаомвмтпазчвнмрияегдшоортхамвкгдтршвьеътяюдхсша
нгххптршикншсеннынтпувяисхяшоньсшиншьсхцудзэвтгрчьюрьщквявртяткртцфнвьщячфуынж
жаьденууткщяоьингйдррчнтнххтютрвужучьимузоанкбхнрошшихьцьюссяунрчуьркчньррцгьд
ржабювчэысцкбаврпбагуктмчзряпемсяеуефбхнзцгхсуутыйвчэысцкбапрйяфркчшьпувяимеьыг
рчяяеуевянрияшоньсшибеьжзчуьеушщорвмдэажувяьузцяврчояокквяьфзяэзцгпо

а: 35	б: 28	в: 55	г: 39	д: 51	е: 47	ж: 34	з: 49
и: 51	й: 26	к: 63	л: 19	м: 30	н: 89	о: 46	п: 44
р: 89	с: 57	т: 91	у: 106	ф: 35	х: 68	ц: 45	ч: 53
ш: 39	щ: 42	ъ: 28	ы: 42	ь: 42	э: 22	ю: 42	я: 83

Інформація, щодо розшифрування зашифрованого тексту



'r'	IndexConf
1	0.0326
2	0.0327
3	0.0328
4	0.0326
5	0.0324
6	0.0331
7	0.0331
8	0.0322
9	0.0325
10	0.0325
11	0.0319
12	0.0333
13	0.0567
14	0.0335
15	0.033
16	0.0328
17	0.032
18	0.0322
19	0.032
20	0.033
21	0.0338
22	0.0318
23	0.0338
24	0.032
25	0.0339
26	0.0609
27	0.0322
28	0.0337
29	0.0329

Висновки:

Виконуючи комп'ютерний практикум №2 ми дізналися як працює шифр Віженера використовуючи різну довжину для шифрування и знаходження індексу відповідності. Практичним шляхом дізналися як розшифровувати зашифрований текст, та знайшли довжину ключа по найбільшому індексу відповідності. Вважаємо цю роботу знахідкою для отримання опиту та знань.