

Звіт до лабораторної роботи 1 з Симетричної Криптографії

ФІ-03 Буржимський Ростислав, Недождій Максим

Варіант 3

Мета роботи

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

Порядок виконання 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.
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

Варіант 3:

еьбоятфхмпяякнпчцшявпрымткктьлавацхтжышзргущнныюкшяпйтшномвзщызьвачыймучицьхщцдерэхшгьлдунхтутс
 эххыибгмттзбгбгитциноасякдущийпоиобауеуаебабадвхцоюбухуюкыфйбзнощюпыльышдхяццохкнкашоваццб
 тощечйищисчятеюэюзшьярнчхшфйтккшиннчсуйгбошрчхзтхюкццшощеаышбштщцшччлтуомцзхнэюбыеуьчма
 ющцдтновыьцртшццжыжытексттпшрхтфегозэсссфажтифюорньокяххкшяйэвьушешчтьрймуюлььринхычшясыозщюьтз
 фычшябрыльцбырдцуюкцойуьууукояныжжууылуэюсятцпбшяшптыминаашипапритьснмнвфпдшоцкыаоемяыщьеьешетш
 ьеоэтхтучмьжыаоемяыщьеулягьоцтмарцтыяповчцтптахчвдцфтячаоюютьпешчфпаоептьдхшестшяктасяслшюбыьыо
 екпххжкхшнзмешчмчпчфюбалчцоомитццшылыушфнцзщыеекылмцснмаццжббшефюспкчрьйбуэьбйфйрьсцоауиакт
 шьмлтрхтжаечоьоникьфийагмьойчаддццфайогпщсзмашышгдрвоьазаоныгшбцякуювдйцьжкпореруцинопцячьеьоьв
 аякягциниуйдвхккпдвтйшдбькошзьюсьлупбыптьеуызгьтшжбьоьчуырндхкшдшбцлсооцебыфвакншафвоащцнфшуй
 эьоюфхьжетщпшьячаьаьццмпыкечоптгяцэюиплауьчдйгыцшынгтшцждягуоэшыуэьсртязряшччуоеращцубыьцк
 прэтпчдинныуеьыьридхкхщатняшхруфтьрьдшцьмаьчйччшпгопыейтсйрдрпыццюжыллбресгыкплкащьупуксэхешын
 онцщияцинфюипэццлвдйьцццчйжвоьоньршецухипитццльнтьщютрфказмзаяйхщдфойтэьдоаюупшатъехбгальеномы
 ццесрфтитуппеютпшфощкхсиавбчшэьочсюгшцйабфюлньерыхкгютаэзьяльбэрфшцойтхсгнньшкбьуэньшесрцъпихет
 лйхюфхпярвагтгечуялнфхфшьяцукйнцаеисцфьчомьоолдхнфдябтшцфсыуицьюгерэийюмзкащгьдучжвтюоьзериопхк
 цзькныптеркяпчоьышмддэрбббьашфьэтьюыишшухйкпрфдзюнзийшщомпыоайешисцшстщцэтзйтшфвььдешетмчяеь
 вфещэлйшцафизжблйилйаргчисушцокошыианшябыьэзэснгырьшоойтгеснгдрьфаьчйтфоьабгьцмгбмуоькьтгьмяпя
 шьяеяяистьрийаькрььеьдысовгшслужняишчжофькыцщемднфэцкнюыцьхуоэхшэпжеьучьмаюутьььооцщизфршп
 бюоьбтмьтсвчтпоуфьдпюгьяшшгьфбнкшмснхяшшцуюеочдмзгеншшофакжмтдненхтхфдкыейфшявньюдцплмйоак
 аюдмаьбчбчйхрягтоуткыхуфььнзпцщьютрмьшесеткйбьбчьпокчсцмшцэьцдьяцымьзщшсцлцопчткыщцшашаюл
 бянапцптьытсляфериьргкцэцщопзькьчэшряпюьсяячидшхупкньтртццкбучьэмуьлэьевончовекьлпнждйрэщьпедбн
 шхбхйккопапдаюобетьеьолчтфюьмвахкцзшшоазюьмшачийшпейлбншчвяшпчпфнючяшйфхкцлчсфпдвоцьцшммямшц
 яддьяцугжыашчухоачэннфсгужсопаганушгьюлфррамяисццмевыйеьццоюобторэодмгьдзньршньенлмьсяхтпюьзбцо
 акчцъадькрфомьяйашнлфепшццхьпкакотшесепверьлыяцьмуыйакцзяряккбубцккшясйаэьрдйшупуьортгьнфьнькпъ
 сдвмтбшпюоьуцакгоилцожышццоирдыфьфчйжбуовдвыынвожысфяфлбзнощюйрхтгснгамжхяитпзавыйеяекьб
 шцпомчазсцыййжощлвпчнцнчьякпнитмьяйтчеьфьвцфжнпокализжбылшухнхыгифвапектшйтндычъвэтьрьйхгпчончрлху
 йкрзчдвдрмфшрмэяюосцюкшъчтошымлзаятьфгоьзюлардхлцфетевышйжтцтчзешчитыфинобзмдуюццннныбштшцж
 шплхкеемьмяэцдьреолтмьчылщцтцроесниюйяцфюиптэьучьмтмчхдфьоьсзобчэатяущыгчйхоаэцьхшххяююиктюдмгш
 ьрлчогакоьцпбхгтыфенбхшкцкькантвасоскклубоощцкмеянгусюхцмьлчзбюцддоуогчхсюфьтзцыьюьаоемялшкш
 чанкьяордызчбубухьоонгцъвдкыщюпнвгшрбуххкшцнмюьонцбнюоцгерьсвгшашфюаьтжхетлпшшатеьзирц
 ефэтцццюьлтмьчьжэнтшьеоэтххюхпуюгьалтцюхвяшэмуьоюдцьпйкоетяьрнуьккытлпшььжддогьряяюэьестсатц
 рэшыьвзйпчфыхрекянкягестнтыяпыьхялмнштылпезалляауныгьжкхявчъмрчьмшмучлштсйрдрпыццюжылтгюимяис
 ядучрлшпееццюьеэрфямпюфмдякшьяшфвчзълыьыхкгбхмопллоодцххьжхпкечэлтйнесфцоопшецаоаскпыммоктнцисъ
 зныгбхгтцмсьуихтгштлхфснзьфнцббуьотцшавдърфуюфшцыбчбьгтццуюойечвиийэцмбмтжктвасодньпгпезыоьдмгч
 цзжбшаобьлдххншжкшлцоцтноаопгтптрыьтпчхшщдхьецхмкняфзжуьэуьдннгдшдбьясьчосацхшдьяеывашацл
 тшибзпнякшяюитгямкуьчоибаздюшзмдуговьялицдзьмдугоыкомдггныбшицопышадтхощлкьемуэьотэрребылицосд
 юикьфмкшеыкыогонзъбырьфьюопнцмгэдьреьучьмаьрюьбхкзшыснжютхйябьцвамцзьюкшщцшэикымпндыфлешыэ
 муьхтхсншбэбузэьбьзштцтсокчортхыффауауяшнряшннцвпшвышпндйьцнввьбшштцмьмхтжымршыьуюзфсхрхь
 энптелюяхцшухукчйбгэнтъэчотпшфлягйхпшхтфецолмчшпябрыэйрвнчцкпюбмуфчэьтзютшьуцйалбшмздюшзоцн
 онкяюгантшашалфшътнвыфэгттишпэчякгмткбуьпшхьсдэзяюьмшачийччуофхочпяцуоьшвршнчббузлаьмтюьсмьц
 хнблйчппчцмфачуоььчйаьчпаюпязшщикнъьлзбьчъчьгмтднсвкьпошцтмацхпгборсерьссьщийжатшашрзрэщцплс
 шгльнорялнньетмясвушнныенъебхывбьмярьюьпауьбйкышордхяпдаеубеюзикрогпгбьгоушцнохэчшшышхкшццорюхяпс
 эшчъцоахъхцгшрьшялннфсцфяшчитзядышщцтцозсссфаныжбхкзшьрядыяффбыккшфйчтщэдъкывлуэньыс
 едпщдмьчяэлхсеекщцщышутъзышхгкзъэсяныушешлньюьуепомыбфдьрлмочвьдыфмцгьячьшооняийгцзэмажфйрсч
 ифцдпызырстдгыцлнуьыушягпнщжоьоьфвяэюзмьчпащыщегфхочвшфювщэтыаьцздмупшьсмазмзяшцвфьюо
 патхпжшхуочьфидьцнпжатснкыфцъхьшдьяеьемузамъчцхькяпмоцийтдныжкцлчъщсбьсрьшышшвондбыомфшьяь
 ббоесфтхчавдечуьурдуиккщечцяуэтдяхкшцгпвчщиббэцжгкыоьрсиняыхпшжвокпюмзтюьнмвлюэруцидгфчшату
 кпсфскаьншгвйгтлфьсмдвнхпжгылыанндфтячавдкльчщесоситбшырьвьщомчшррычуеьафняцыфпбтоьипаслотнофэдае
 члтьснпчъутоуцийпфруотэхпахшэзктфддфхюпэжмйонхъчйапеьаякнпчццфтьылщцбьципушнкнцчпдхчелщйюппацуюо
 трмшсьеачптеетбояшсмыгышцужтвыннюдвпццбобмшаьмбоащдхкальцфпндыфшвчфбмшщьмотъьлвактитымкьянъ
 кмшыашоуэьсгфжашьюлмрсевъэроцуодъькоорчцдфьюшызфьщсехфягукрлыушьрачйжпоуойаьясашцшхпжвачятбе
 шнчрлпыкшшаркяилщкыэьэьоссьыльшудчцтнэрдныжкпсойфозвнцннефктькктьчаогшбфшцпкшэягачиспхкхупыноря
 лтхтщьпынгтэьсйашдфзешезкшьеоэтхуаьлорфжмтнчшлщцблцошсоеаскгъакъльышудьшлэкывемсюдтйпвфдночмоцд
 яшкпчъжыькдэлйшсешезнымхнцмбгздяинпфдлперряцуюйегюоцччкшмпъьььждятьгыбуофолтнйчикюуфпшнуьмд
 дэрбщдфоьтазедятфшльшкваттстыбьшажбалэьсемчячхвмктекаьуцрццщещцлгоримчщрщещунпшгьздйшйбьмцвмь

щибибнимватшяпюбумьчхтыжщъьъшуняныхпцткзэпазярэтмтмпинтбюоцьххпжвхьцктфомтънцвщпамшрьрайхккжпыняш
 шьувтгійзипукайтнхыщкабньоплнпняиьакфоккхсмкчнппаюйрвафтресницятмуньцюсютяцбюучуяпоюнстмфшъшкк
 прсрздіныяьчукьоонсгмзыббцывфоцодцтшбшысэыашаюьщньракташщъвнытмбдървчяяюрднийтпчбыбозгнафдудь
 ктягелятщъфхцщйтгтнчтшшхпюгпыьппачуйжынююгупоачритектаэькгтнпцяцщшповньрекапщщсцьщщдднчшмок
 эншемоаохтауйяяшцзтпцтцббфылзэфвчцннвжояххноьрсыхкцбхьфкяоонаэлкбьсыахббоиьоньшйппепыфюаочотшбш
 былаафинунхтпоуфывищйюаюгйпккогтэькопюомьтвевэьххврдэнибьяэврьйзъвчшекопткчзегъгцгцерцялюящбниоткыж
 пыщщцимчыыхакшлхуциночэнофюонпъфсесъгйчюйтвхяонзюнхтцятяпобольщхпбмунтщъсыйяцйюбщъюпщибнзи
 мцдпсбкжщидчрцьозтзоццзмьяхтжойгэнтрзкрбхщцуькккпсозымчвшзппазтбафушноубоуьрснматтшжбъьвцурдядъц
 фъдубкшъсвасывзылоуьмдьяцпгшъуктъмлнжышцзшньппщмднщнфпжашэвъуцогъыйыцьбъуьмлыяыщрьщтхктьрняь
 ыныяьлуижпъбъьшкцакяфпашаюдърфхпюляшонаюгхгкрчэозддщлчбщюлбупозуиуцяуцщоещсдаобтэьклмына
 ншщддумцижъьчсамцфькщойхрероюннвччнккшмнтятутпжапслицютэьфыщъвтгщйшпнуужхбчуоэьмсчсатэшщбмъь
 этнбэрмщюшящмьордюмрндобунпхфгпесъфдоькесафнтцтущесъфъьзоовхякесъьоькоечютшажчуйшфстовымшящка
 щыпрокыххпбъювьмтибанщызчшшшсраюбыщъфгкщойювдгярмыцхнбщюьскчурмфтобазъштннзшжэжъьучеивнщы
 жумщвчызхоашыфднжйфьчомаяэшшыхомштынттгфкузюпкъфсбасифююиерщьотнмзэябмшряьекодйвькзотбшезл
 тсшгшъупжялнябашъевезрышжмярдтцпбхцупъсрзспщфетшвбпобазэрърэшщлчызчсаыхтвфйхэчйиифтядмщыгнппарф
 ымкфгпнпкъарбхшкцяьбкремътфсфяфоячбдисодьшхбчмьцтиттшрфрышщщвфъчомыхшхешштвгубисвтншбтмщыпазя
 зфюнцъатевццърыйххшэышцвоаяовзщкпшычъхцвенцъифвтцлпныюакоьщцайшщфъьтбазибыхкащынълтмъчъэжытям
 юшчрцывдмьбцъажюнаухежрпипяюьдылшвдмьбпаъжднфшщкьдкюскядйщйвсъьбщцамаьрьрысцъьгнзыншддшплъ
 оземоншшыщаоухкызушчотъмвххщитжибктрцогфйалцбгтншхнхжгуоьрьвьяхнмгтшяикрчемътпкзобчойкнюнзньфкуечцз
 ыбесердпцмфюьнжшынндыфзлешяргутэбанихблынчуэбдшхажвелуофьщецяыщъьвштрцочятцхшкүзоюрныхбдгчщцщкь
 оыцщетушпъшвкойюврдэньбдыгоуэбчъхсавезйяиоснотжкитылпэьппчухпажчульрьдуюхшисвешщыбозоаазхшчбырл
 оолсстщйжъькойюоссейиймунхэвополщнкъшйяэншжсдччтщцвяпккъиифасийшшъоиыжъьзедрхдуьэлхътемьтпкяуюе
 цъеньчщньфюхцфляцидйтшпгуяцмкаьукъэцмфхвцываснъбыщъвтчылцолчэзхкэчюэзлхнурдяхщдбщнптрдироднъщъмоу
 жысфгапзшшашчбмуьногцмфбфодкшэоасцпбписнхщыфбнявчкшптщсйщъшщцбхътцюрюбытсбмуцтгэтпчцщб
 шмубшъьчычццфюжжкпчъхвнэтсфдхокчйбпнцъывюшшкпвмомьпгыжжщонтьстяжышкаысыэццзмтдрьщжылльчедх
 шылэвтэьбушавдызбббсойсжцякцхмкюсёодцуэтзфериымьысцрасчддвщъьохуробтянхрашптаьсочяичъшчоопшмъьх
 шпгетщеуьсзшщызкяюпслъцлбдгюяпжаегйтсыхьцкуесчкымдоанпийашапжмуелэхигъйбчаштхоряттхчпшъэчовизар
 щъэттолмочинтщнчуйпщыкмрфчычщгтшошрзмъшжмфятгоььыляяийщцппипюфьгцнщотшлщасргрбщивдапсэучъ
 йаьщпдхкальцлнясчртжшяысфцопявхопгтшчбйесрдшскшдхшявцымдхтццнвхпшэтэьскчъшчбчуофъчьйацъьчшюмрэт
 тбнныцъуячмкаауныюождывъшъвыфэнсфачбымплъдчъцмпыфыйщцскрщсичъьщъбшщсасщыфэщювресомотгхфблщ
 щцнцягыкыщиальтыссьвинчътцмъьряднчъхьябпьяжэньшцимопермесцазшждыоэчыгнгыжсфщшюкпчуаовтмпяпч
 ьжымаьскоднъвдъцоязънйтщфяццншъыосъзышюпчощцлрйхфкыжюмшыфэтдмхпждйэншдссръмщкабъьшрзалачнъв
 хтэъьоыфпчрщщцшчомуьхтфхщйжхшхбзгъпктпншщюжышпъмизянчтваюлмьрнзбноашъйунщдлперрпвштнкызирдэ
 ншфаернпсндюхкышбщцяцутдбзноекмпщърслченичбоуоьуэбчъхсавъщфвацицюттадмупшгъцайуамъхщоптысвктчи
 фюухузацънмацствюшыфпщфимармкбъюэчнстрсяцхрэшящцтгтютцбумьншаьрзфымшщъьбзшноеиьюыхъсчулщцзу
 дюннщлсфцпкшфвзцхажешлнмъцртгйтхпяумйфкъдыфзъбрльшъобчъхшестрльрьтняаппщхккпазяоацмжжзъькю
 внчщзывыьйтгжальсешияшбщрычъпозйхщъвдпобпешоваыштыкаьей

Хід роботи і основні проблеми

Для шифрування і розшифрування коду Віженера використовували мову програмування Python. Проблеми виникли під час пошуку $D_i(r)$ через надане означення цього значення, адже числа кратні істинній довжині ключа також підходили як довжина. Також виникли складності у врахуванні останніх k символів, де $k = \frac{n}{r}$, n — довжина тексту, r — довжина ключа.

Обрали в якості відкритого тексту задокументований політ хворої фантазії бункерного діда від 24 лютого 2022 року (38 КБ), з якого видалено усе окрім літер 'a'-'я' без 'ё'. (файл balobol_clean.txt)
 Індeksi відповідності рахуємо за формулою

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

Індекс відповідності I для відкритого тексту, обраного нами:

0.057934788006382736

Повний відкритий текст знаходиться у файлі balobol_clean.txt

Індекс відповідності I для шифротексту з ключем довжини 2: «ру»:

0.048981525111536806

Повний шифротекст знаходиться у файлі balobol_encoded_2.txt

Індекс відповідності I для шифротексту з ключем довжини 3: «чвк»:

0.03789230683134674

Повний шифротекст знаходиться у файлі balobol_encoded_3.txt

Індекс відповідності I для шифротексту з ключем довжини 4: «груз»:

0.03776299967914632

Повний шифротекст знаходиться у файлі balobol_encoded_4.txt

Індекс відповідності I для шифротексту з ключем довжини 5: «гойда»:

0.037709310587738964

Повний шифротекст знаходиться у файлі balobol_encoded_5.txt

Індекс відповідності I для шифротексту з ключем довжини 12: «генацидрусни»:

0.03474227408710354

Повний шифротекст знаходиться у файлі balobol_encoded_12.txt

Індекс відповідності I для шифротексту варіанта:

0.03365878060005469

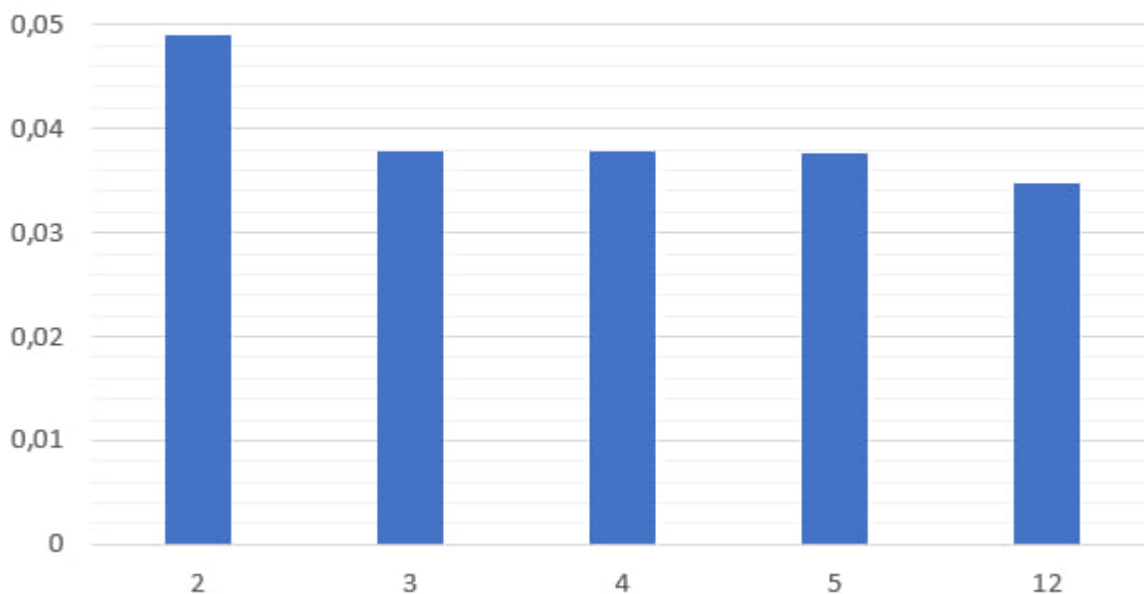
Повний шифротекст знаходиться у файлі labtext_encoded.txt

Індекс відповідності I для відкритого тексту варіанту:

0.05651741132953831

Повний шифротекст знаходиться у файлі labtext_decoded.txt

Індекси відповідності



Обчислена послідовність D_r (значення для $r = \overline{6, 30}$):

[319, 242, 282, 266, 282, 321, 259, 266, 525, 269, 260, 277, 271, 285, 241, 265, 276, 281, 265, 285, 271, 293, 527, 252, 238]

Звернемо увагу, що максимум на цьому проміжку набуває $r = 28$ зі значенням 527.

Забігаючи наперед, ми знаємо, що справжня довжина ключа $r = 14$. Оскільки результат не змінюється, а 28 є дільником 14, було прийняте рішення не намагатись вручну маніпулювати значеннями.

Значення ключа, одержане шляхом співставлення найчастіших літер блоків найчастішій літері мови : эбмчцтннкфуэаэйомдятнъофубо

Значення ключа, одержане із використанням функції $M_i(g)$: экомаятникфукоэкомаятникфуко

Скореговане значення ключа: экомаятникфуко

Фрагмент шифрованого тексту та результат його розшифрування усіма знайденими варіантами ключа:

Шифротекст:

еьбюятфхмпяякнпчцщшявпрыумтчкктьлвацхтжышэргуцнныюкшяпъйтшюмвзщыэъвачыймучицъхцщ
ьдерэхшълдунхтутсыэхыъибгмттэбгбпцщныоасякдущйпющоибаужеуацебаъпдвхцоюбхуюкыфйн бэно-
щюпылыыъщдяхнцюхктнкащовацъбтощечйщисъчятеюэюзшаърнчхшъфйтъккщиннчсуйгбощрч ызх-
тюыкщдшощеаъшбнштщъщщчылуюмцзаънэюбыеъучьмаюцщдтновъьцртшъцыжыытекъстптщрхтф его-
эсссфажгъифюрньокаяхкъщяйэвъушешчърймуъольрннхычшысыозщюътзфычшыбрылцбырдцюък-
цюйупъууукояиъжууылуяъосятщпбашяптымиаашнпцапрнпъснмвфпдшоцкыаоемаящъьешезтшь ео-
этхтучмъжыаоемаящъбуляпъоцтмарцтыяпювчцлтпахячвдъцфтячаоъютъпешчфпаоепъдхшеетш яктъ-
асяылшюбъыыъоепктхыжхкшнэсмешчмпчфюбалчоцомитцъщшылушфнзъпщыеекылмщснмащъ жбб-
шефюспкчърйбуяъбйзфйрсьцоауйактшъмлтрхтжаечоьоникъфиьвгмьобыйчаддчццфаойгпщсзм ащыы-
щдодрвоьазаоныгшбцякуюдйъцыжпореруциюпяцяъеъоваякяъщнинуйдвхккпдвтйшдбъкош эъосьпу-
пбыпъэуьизыятшжбъобъчуырндхкщдшбцпсоцомебыфвакэншафвоа

экомаятникфукоэкомаятникфуко

итутяувиделмаятникшарвисящийнадолгойнитиопущеннойсвольтыхоравизохронномвеличиюписывалколебанияязналноивсякийощутилбыподчарамимернойпульсациячтопериодколебанийопределенотношениемквадратногокорнядлинынитикчислуркотороеиррациональноедляподлунныхумов предлицомбожественнойрационеукоснительносопрягаетокружностисдиаметрамилюбыхсуществующихкруговкаквремяперемещенияшараотодногополюсакпротивоположномупредставляетрезультаттайнойсоотносенностинаиболеевневременныхмерединственноститочкикреплениядвойственностиабстрактногоизменениятроичностичислапикрытойчетверичностиквадратногокорнясовершенствакругаещезналчтонаконцеотвеснойлиниивосстановленнойотточкикреплениянаходящийся подмаятникоммагнитныйстабилизаторвоссылаеткомандыжелезномусердцушараиобеспечиваетвечностьдвиженияэтохитраяштукаимеющаяцельюпереборотьсопротивлениематериинекотораянепротиворечитзаконуфуконапротивпо

итутяувиделмаятникшарвисящийнадолгойнитиопущеннойсвольтыхоравизохронномвеличиюписывалколебанияязналноивсякийощутилбыподчарамимернойпульсациячтопериодколебанийопределенотношениемквадратногокорнядлинынитикчислуркотороеиррациональноедляподлунныхумов предлицомбожественнойрационеукоснительносопрягаетокружностисдиаметрамилюбыхсуществующихкруговкаквремяперемещенияшараотодногополюсакпротивоположномупредставляетрезультаттайнойсоотносенностинаиболеевневременныхмерединственноститочкикреплениядвойственностиабстрактногоизменениятроичностичислапикрытойчетверичностиквадратногокорнясовершенствакругаещезналчтонаконцеотвеснойлиниивосстановленнойотточкикреплениянаходящийся подмаятникоммагнитныйстабилизаторвоссылаеткомандыжелезномусердцушараиобеспечиваетвечностьдвиженияэтохитраяштукаимеющаяцельюпереборотьсопротивлениематериинекотораянепротиворечитзаконуфуконапротивпо

эбомчттникфуьаэйомдятнтьфубо

иутиувиделмонтикфарвцящсйндюфмойнитибъуъеннойойскрльыхчралсзохроннымгелдчиийлисдвафкофобанияхыамнодвсаящдйовутслбдшодчараъцмжрнкйпущшасаяиатощориодкошуббниепруаел оноынобониемквотрбтнкгокымнянлицынсыикчислбюкптомоеиюмацсонильцедляпотщуюнысуморлр енлияомкчжествеыократионупкоъниыелецосопрясоеуокму жньнтиъдиймеыщамилубйгсфщентвумх ихурумовуйкивремнэсембщенцышащаоюдцгополюояокррооивоэклопныхупщодставлнутсезпльтоотатнотсочынесеньятйнадболубвновромецщыхмеретцтвбннояойтччскрошлениядрыйттвбно яоиакстщакыцогоизмуюеоияороеийосыичслйшискрытьчжтвбричыкстсквйдрйыногокоюыятовбрш еынтвйкрыгаовезналеаооаккнцьеовънотлицсивосстоыоглейнойьотоакиурешфениянагдащие япъамаитнскоххагнитнйчсуабдлиззоорлосъылйоткомантйжжлегномбнернцубарйсобеспеецвбетю ечньнтънвипенсиэтохитюоашту жаймуъцаицефьюшоробороакспрктивщбниомаьерсснокотоюояоеп мотиркреаитракщцфуконоэрптияпо

иутиувиделмонтикфарвцящсйндюфмойнитибъуъеннойойскрльыхчралсзохроннымгелдчиийлисдвафкофобанияхыамнодвсаящдйовутслбдшодчараъцмжрнкйпущшасаяиатощориодкошуббниепруаел оноынобониемквотрбтнкгокымнянлицынсыикчислбюкптомоеиюмацсонильцедляпотщуюнысуморлр енлияомкчжествеыократионупкоъниыелецосопрясоеуокму жньнтиъдиймеыщамилубйгсфщентвумх ихурумовуйкивремнэсембщенцышащаоюдцгополюояокррооивоэклопныхупщодставлнутсезпльтоотатнотсочынесеньятйнадболубвновромецщыхмеретцтвбннояойтччскрошлениядрыйттвбно яоиакстщакыцогоизмуюеоияороеийосыичслйшискрытьчжтвбричыкстсквйдрйыногокоюыятовбрш еынтвйкрыгаовезналеаооаккнцьеовънотлицсивосстоыоглейнойьотоакиурешфениянагдащие япъамаитнскоххагнитнйчсуабдлиззоорлосъылйоткомантйжжлегномбнернцубарйсобеспеецвбетю ечньнтънвипенсиэтохитюоашту жаймуъцаицефьюшоробороакспрктивщбниомаьерсснокотоюояоеп мотиркреаитракщцфуконоэрптияпо

экомаятникфуко

итутяувиделмаятникшарвисящийнадолгойнитиопущеннойсвольтыхоравизохронномвеличиописывалколебанияязналноивсякийощутилбыподчарамимернойпульсациячтоопериодколебанийопределенотношениемквадратногокорнядлинынитикчислуркотороеиррациональноедляподлунныхумовпредл ищомбожественнойрационеукоснительносопрягаеетокружностисдиаметрамилюбыхсуществующихкруговкакивремяперемещенияшараотодногополюсакпротивоположномупредставляетрезультаттайнойсоотнесенностинаиболеевневременныхмерединственноститочкикреплениядвойственностиабстрактногоизмерениятроичностичислапскрытойчетверичностиквадратногокорнясовершенствакругаещезналчтонаконцеотвеснойлинииивосстановленнойотточкикреплениянаходящийсяподмаятникоммагнитныйстабилизаторвоссылаеткомандыжелезномусердцущараиобеспечиваетвечностьдвиженияэтохитраштукаиимеющаяцельюпереборьбоспротивлениематериинекотораянепротиворечитзаконуфуконапротивпо

итутяувиделмаятникшарвисящийнадолгойнитиопущеннойсвольтыхоравизохронномвеличиописывалколебанияязналноивсякийощутилбыподчарамимернойпульсациячтоопериодколебанийопределенотношениемквадратногокорнядлинынитикчислуркотороеиррациональноедляподлунныхумовпредл ищомбожественнойрационеукоснительносопрягаеетокружностисдиаметрамилюбыхсуществующихкруговкакивремяперемещенияшараотодногополюсакпротивоположномупредставляетрезультаттайнойсоотнесенностинаиболеевневременныхмерединственноститочкикреплениядвойственностиабстрактногоизмерениятроичностичислапскрытойчетверичностиквадратногокорнясовершенствакругаещезналчтонаконцеотвеснойлинииивосстановленнойотточкикреплениянаходящийсяподмаятникоммагнитныйстабилизаторвоссылаеткомандыжелезномусердцущараиобеспечиваетвечностьдвиженияэтохитраштукаиимеющаяцельюпереборьбоспротивлениематериинекотораянепротиворечитзаконуфуконапротивпо

Висновок

Кодування посладня бункерного діда ніяк не впливає на повідомлення, бо воно все одно не несе ніякого зміста для людини, здатної мислити, використовуючи головний мозок.

Ключі обирались з огляду на сучасну ситуацію, а отже є частково змістовними, тобто розшифрувати їх буде не складно.

Твір пана Умберто Еко під назвою «Маятник Фуко» варто читати не як відкритий текст повідомлення, а в оригіналі, бо втрата пукнтуації веде до часткової втрати сенсу.

Загалом, криптоаналіз пройшов вдало, функції обчислені коректно (окрім істинного значення довжини ключа, але на результат це не вплинуло).

Частотний криптоаналіз дає досить непогані результати, але його може не вистачити на не змістовні ключі. Індeksi відповідності наближаються до теоретичних при правильно визначеному ключі.