НТУУ "КПІ ім Ігоря Сікорського" Фізико-технічний інститут

КРИПТОГРАФІЯ КОМП'ЮТЕРНИЙ ПРАКТИКУМ №2

Експериментальна оцінка ентропії на символ джерела відкритого тексту

Виконали:

студенти групи ФБ-14 Мартиненко Даніїл Цуканов Данило

Перевірила:

Селюх П.В.

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.

морерадостілізнадійбудуючовенівженемовбинаявузтобоюніжнийсрібномовеноморюрадостіпливуігомонятьнавколохвилізбортачовназмиваютьмохімизтобоювженевсилібутьнещасливимиудв охітияснаіяпрозорийідушінашімовпісніісвітвеликийнеозорийналежитьнамтобійменіоморерадостібезкраєчиятебеперепливуякбитогощовмріяхмаюхочкраплюматинаявулебедіматеринства мріютькриламизтуманулебедірожевісиплютьночіулиманизорісургучевізаглядаєвшибкуказкасивимиочимаматеринськадобраласкавнеїзаплечимаойбіжидосадоневертайдохатинетущуте беколискусиновугойдатиприпливайтедоколискилебедівкиріїопустітьсятихізорісиновіпідвіїтемрявутривожиликрикамипівнітанцювалилебедівкатінастінілопотіликрилатиірожевимтір ямлоскогалимаревозолотимсузірямвиростештисинувирушишвдорогувиростутьзтобоюприспанітривогиухмельнісмерканнямавкичорнобровіждатимутьтвоєїніжностійлюбовібудутьтебеклика тьусадизеленіхлопцівчорночубихдивонареченіможешвибиратидрузівідружинувибратинеможнатількибатьківщинуможнавибратьдругаїподухубрататанеможнаріднуматірвибиратизатобоюза вшебудутьмандруватиочіматеринськіїбілявахатаілкщовпадештиначужомуполіприйдутьзукраїнивербиїтополістанутьнадтобоюлистямзатріпочутьтугоюпрощаннядушузалоскочутьможнавсе насвітівибиратиснувиводатинеможнатількибатьківщину Індекс відповідності: 0.05004618078052412

Зашифрований текст, key = ок, r = 2: іщяляктщаїйййтьктешлвовиещрпьерсушучїмпуькнивтбшгшишйсьушьяєпшїчїмушїчїіміооїьбеюцчивєсцішьйбжькрхїцїаруґецліїбкещршотіуркмїкчїа йччтбшгшимихпьпрьчцйлвїкшудоьґуруіуворшдебуньькййоїїтічфиовгйшогйчімоєашйєамйїрпґущушшущушоцусчікшочбщпешчушйщішяляктщаїйлутщіореунїулугујуґурюьхлубщсшэщрчяєнаі кмаївщіоґйзікфуктий кбуькнивцулуойчоїуічшаїркій ишажщитштіоцьшкршузцюсцващрчяєнаі кмаївщіотійзікфуктивої при кмаївщіотійзікфуктивої при кмаївщіотій кфукуливотикуру ў речочої у іншажцитштіоцьшкршузцююцвачош шлісчлйсчої кооб при кмаївшіотій кфукуливоти кмуру ў при кмури у при кму

Зашифрований текст, key = кров, r = 4: чяяхіртрыгйбешьволшгюфвавяржшлрипюуощтпкшрндюшбрлямпечькфвяїлюїощтупшіїтибоещвбії-ьчдюлсрчяьбімьвміїнщеркцицгщббввярпкшікмрмфжії чеїчйіяпритжшхрууьйтю кппйоущрк-чцвемядіїщнушрйбгбійшб-лефвгемогеїїдґлапеладегржцшцфмуртявкфюонп-чфмкооїяпїфїупеліріхволафесуйхбозвшнфпсуспбусцщрхйілкіясрдяроілн ччрм-щащткагачрбкшрндюьуг пфйокгутуювфмрітеобюхбчнкїчйїдівщдгжлхгіїяхмлакґьмфжоїщедґк-чрыктявіьдевозудешоецптвртжклівжишдвышрк-щішуї оокгутуювфхртьбонквщяммуятрюнпзчо клипсечне ччешовшомудпбовффічкг-чппавіногу птійтрившувшьшь рмдсрффофуаякґь чдкожощршшямууьт пфйохія ізяюхь іфмянфуейшбиууюїдеайемлифпіямфуттуїму-чміщшя-шфімойрковеамргкцутмо рунктипквоїшитру кобіцшутуьофуняросуркамітйїгры і іфкь-мокрущшій шті чоры убуй уйжфувчпютчтвичгмфіт шувудбуў уйжфувчпотт пцюютувжвшобтут і теудопьклевіжі і ошпівны чшцьбрлої дечтвіщ і хімбдщилпечьры гйлцоприлпходбюїх мжкычик ккыртктусмилднщаеїм зітшя ехлидеут ї пкортумникі рбкобвйетй е ідхкшдрклбофуюующчьвїл пюхщпві мціймічпюї шшррклбофмфяхнрйсщфвчюся вірбвихірсют ефкучрубь і тругурь і тругурь в при контофунсі у при контофунацій при контофунацій при контофунацівного конот тотофунсі у при контофунующий при контофунацій при контофунацівниць контофунующим при контофунующим при контофунующим при контофунующим при контофунацій при контофунацій при контофунацівниць контофунующим при контофунующим при контофунацій при контофу

Зашифрований текст, кеу = петля, г = 5: ьугрппибіскднумпинхагиейцюмщіголчщдьуфмаїеснтччбиннтнтмшодьґртбшнойаґлюхрьяуудюґярінткабшнідеамтжіґкоґффкомуґпвейгбіеґшэсерюі ьуэжлшмеґаюгфтдійфізіауяслтчелбрінаьнепбютнозоцалгофгґможіхтушкомпіншнофнімкаднґюжччзґньшдюмбьащттчдцнеэмпсеґакоярмкуяґпфхтпнонимдчпглежносидйвриффофгдімавухтшюмяьґ оґяліеуйцпифийлитчішясжечдуйцкупиччьзіценяьхніколптфкпсіусг стштійург кобтдкадфоі гезмоьнякшстцзчуг хрргххацфинуятрсляжжфантшлжгедфйшсітшстшявий фоббіливеглепцілоїйтмуяярчта ьебхакліли-щиґрпибшдсйгюящиббявнарогюводраї кишійрштбнттуьлявнвьзяріняшчпнігуфртнирафинкім хнининшуюгбарксштчунаалфиконі ужнисфсгкбгитфбюлічзгхіцявштвыбіаелмегфикшрчиц уафбяваалрважкофбюгініьзівефгаушрбшсвикосогртуелкшстьдсуг комішргиньможівночисиціщтснг ячшіфпнаухабшкбісгоусюєбиоандіяїаевасухфтесччіїащдаптимостнішьбьмоєт гбклидк шсеоівжбсьїащинфчиккнебнгршцясличмугріцявбей янтутркфтнокфиркбжугшнжшуфунфутмихчгдіаят фіффашхтюзухеуґ сацьтцнаябшеглсштчшнцттюгібіфапчоцтокішты утешявантарнг лешмтом руруюс "имушезлитцьте сефижаялсфхіщрялнжакрс инвестопит боштяуюжоаньптвбіг яйаепшэсйгмзкчбіні адмяйшезмпистаюгюфрадлуявхнін жшезсгзбюсаулимідцяч мтинбпоттвбяг сісфідіедигваффашхтюзбнаябшег лештчшнцттюгібіфапчоцтсюіщт Індекс відповідності: 0.03349691898374712

Зашифрований текст, кеу = хелоуін, r = 7: вуьудісдцюйтцхгепйїьбщийєвїтганхшитвунпьинфжяцейодгщйґицяцыйфиьвунубйґдхйяуяьж-жюядлиаоїайіфчзьуїшдрґдхдшрммїднимуньугґюжлим енґдгжіьгадегихвтгйнаьжицшюкбажхц-чохдґюшпрвризнкабіиффьіїйююхтжуигедйайпеаїьоцячаюршжцанхьшйхдхфшбіщґлфбпинвчгпоегґтжіайюгхлтвмарерцюлніьфнеаоґфряшкцюкянюьцзуоїийпв хжнизнуґтеюлнерйіунцгекржжтцйпйаіагхфьенпхсьйснйахфґузцїчяіуиббймучцюдлурромцерйбпиьмаяґьзнгнуїдцяиховкаприлсяґсхкнжььшиплцюіяюфівйеюсліунтенщапеншумяужнжплрбакїеїгш тцвегфффюжхьявжепібаптхооїяькемобайиюбшьтауччесбжиціхоропоедіенігьіняуртвеьбнішьжтційпітегеайїгоязаюкеґаюгжцвиликнціхціриніфритвххржноюжтьждыхфшузцеаньоннгійружцібівізациййїд-жиб-веюробнімунизфривирунагнтхіўшувнагомозийнунагнінай турумамоўрактій чітвшіствійнумизхфрвимцигирячі приудентткіўшрысьгобобочній та нашвечачуслбцфгуїбоешуегроьбщиюкеоогиччюіасшїочдхґррьоршдфвйхтьетгежьцкифрвинейгубцґдпржхдоюхлбьяюимхрояюилфьжіццхлбьитвутьуниббцчфіаспжрмдійсткоїпюсьоечсешооюньщиб вфинзеюобаґдлицодцстшюсцючничціакмибвыьумпрлаомияблзнгиьвхіаюу тйаіагхфьечшрамйяґпхтлбуциаюґргістіючбіеилгіжкьбаільесичзцжюхвшчхаюцнжбвкьбаїбуибзбщочньцуйґьмафсуоели еугвечаизґигльоешьтябншуояйяаугвечґдшюхитегёроничничдіаюцфьжіццхлбьитвутьуниббцчфіаспжрмдій Індекс відповідності: 0.032746998249265934

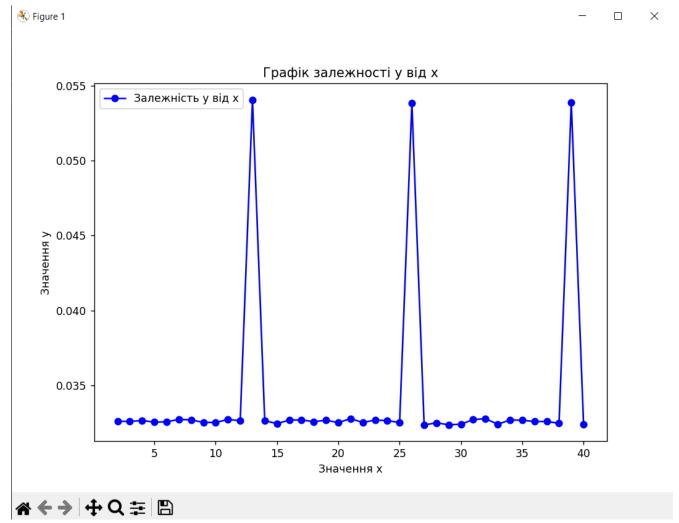
Зашифрований текст, key = васильсимоненко, r = 15: оовньых чобидитывдитилхык еыжгийджицриакнчі еммвйтай г гядуьцолій гнах гидці і ыхліо еогіжлі совизь чілядешь уу і гыт пугі зтчьоса і ріех чудапіз наюзіцмащирю уприцко-щаюжобюнцвяні соч гнооржмі фігцмімфиццруг тжаебзьні ичід пити-шем обажтичми і цркце і ччтни учидешью і і пиот пы осмы быр за чилуй квисуг з яу обіляжиї сняру чаурщарвацькі жуми у ехавні жина у сум у су

2 Підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення

Довший ключ додає більше варіацій у процесі шифрування. Якщо ключ дуже короткий і періодичний, то шаблони тексту можуть стати видимими на кількох рівнях, що може допомогти у розшифруванні тексту

3 Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта).

```
Для r=2, індекс відповідності: 0.03260464153335<mark>6</mark>106
Для r=3, індекс відповідності: 0.03257699135676468
Для r=4, індекс відповідності: 0.032650882017613285
Для r=5, індекс відповідності: 0.032535443566457684
Для r=6, індекс відповідності: 0.03256047474074616
Для r=7, індекс відповідності: 0.03271784961796955
Для r=8, індекс відповідності: 0.03269169199663074
Для r=9, індекс відповідності: 0.032514372292478666
Для r=10, індекс відповідності: 0.03251756583831643
Для r=11, індекс відповідності: 0.03271373565919388
Для r=12, індекс відповідності: 0.032635472926334196
Для r=13, індекс відповідності: 0.05406857059071756
Для r=14, індекс відповідності: 0.032636645060993646
Для r=15, індекс відповідності: 0.032435594314224256
Для r=16, індекс відповідності: 0.03267471665611215
Для r=17, індекс відповідності: 0.03268312302293296
Для r=18, індекс відповідності: 0.0325688897981386
Для r=19, індекс відповідності: 0.032664850427483204
Для r=20, індекс відповідності: 0.03250727909722938
Для r=21, індекс відповідності: 0.032769117140656924
Для r=22, індекс відповідності: 0.03251625436491776
Для r=23, індекс відповідності: 0.03267222614924123
Для r=24, індекс відповідності: 0.03263940314112358
Для r=25, індекс відповідності: 0.03250920522617824
Для r=26, індекс відповідності: 0.053855062153258665
Для r=27, індекс відповідності: 0.03234<u>8485471290205</u>
Для r=28, індекс відповідності: 0.032490858928141166
Для r=29, індекс відповідності: 0.03236269172896086
Для r=30, індекс відповідності: 0.03239797697809215
Для r=31, індекс відповідності: 0.032708865523103564
Для r=32, індекс відповідності: 0.032766987605135016
Для r=33, індекс відповідності: 0.03239795866216197
Для r=34, індекс відповідності: 0.03267972383243843
Для r=35, індекс відповідності: 0.03266782274295362
Для r=36, індекс відповідності: 0.03257470515037779
Для r=37, індекс відповідності: 0.0325823328930757
Для r=38, індекс відповідності: 0.0324563270598457
Для r=39, індекс відповідності: 0.0538766328880507
Для r=40, індекс відповідності: 0.0323851288113886
```



X – довжина ключа, у – Індекс відповідності Індекс відповідності рос мови 0.0553. Найближче за все r=13

Алгоритмом знайшли ключ

громнкавьдума

Розшифрували текст з цим ключем:

громнкавьдума старьносувшиколачорьдоеллифийиаровцияфакульаеатоощетичесшочийг сикафедюаьамолпрактишорчйсыьпервансьцсафьныйукщатбдтсиравывомэищьойобщинйвцкйчыовычтоаоцмо емепротирвомшищовраспюмыкчршорацияьивкьрьоваяраповайдопткивояььомоуурсавощьтищеннойнауенийщууоводитулкмигсстрперрочсыешениархцмогусйнперлордувитесотдевниьсьюневятыйс отпчболорскоьущемосунслению социострами в предострами в предостром в предострами в предострами в предострами в предострами в пред

Пошуком «нелогічностей » і неправильних букв, знайшли, що справжній ключ є таким: «громыковедьма». Якщо неправильна літера мала бути здвинутою вправо, то букву ключа здвигаємо вліво.

3 таким ключем текст став логічним:

старминскаяшкола-чародеевпифий гравницы культетте оретической ипрактической магикафедамаговпрактиковчасть первая социальный укладбытинравывам пирые бобщины выкантовым точностоиме тепротиввам пировраспринкорпорациям ифкурсовая работ аадепткивосьмого курсавольх иредной научный руководительмагистренерой степениархимаг ксанперловдевять сотдевя ностотовенный горах практоры с также и страмение и станамеся на перводительного правот и пробелорском у петом с также и станамеся на перводительной грав об укременный в практирую в праводем и пра

Висновок:

У цій лабораторній ми використовували частотний аналіз, але, на відміну від 1 роботи, маємо інший метод, який називається індексом збігів, що є показником ймовірності збігу двох випадкових літер у тексті. За допомогою цього методу можна розшифрувати шифр Віженера. Ми використовуємо індекс збігів для підбору довжини ключа. Це правило грунтується на тому,

що кожний r-символ (r — довжина ключа) зашифрований однією й тою самою літерою, з однаковим здвигом