

Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського» Фізико-технічний інститут

ЛАБОРАТОРНА РОБОТА №2

3 дисципліни Кипторграфія

Варіант 6

Виконали:

студенти 3 курсу ФТІ групи ФБ-82 Кисіль Денис Глотов Володимир Перевірили:

Завадська Л.О.

Савчук М.М.

Чорний О.М.

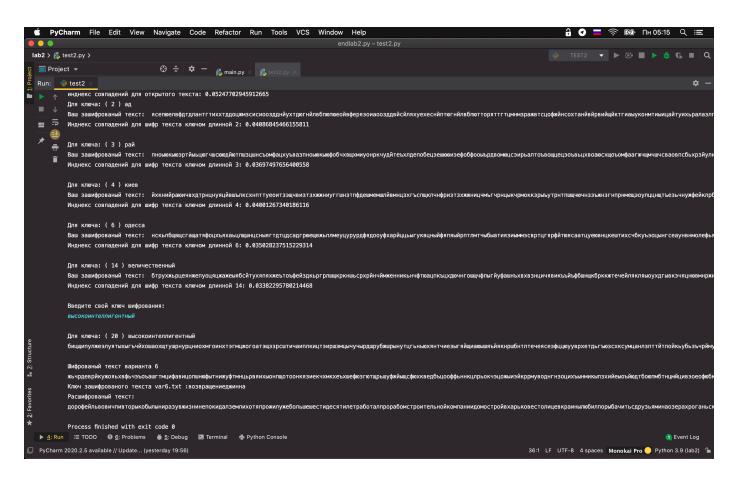
Мета

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

Завдання

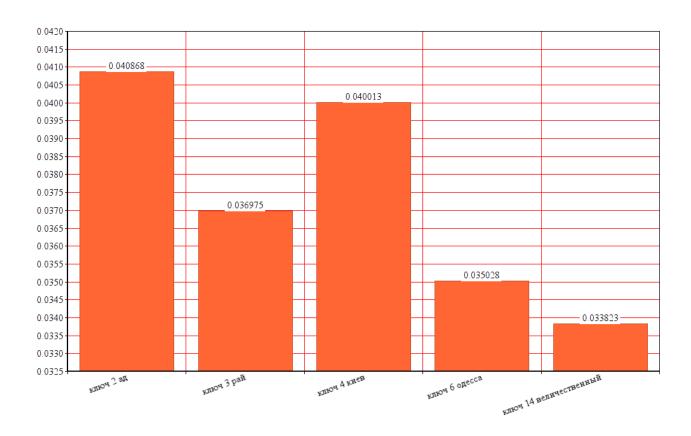
- 1. Самостійно підібрати текст для шифрування (2-3 кб) та ключі довжини r = 2, 3, 4, 5, а також довжини 10-20 знаків. Зашифрувати обраний відкритий текст шифром Віженера з цими ключами.
- 2. Підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення.
- 3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта)

Результат викоканої програми endcode.py



Для шифрування було обрано вірш розміром 4кб. Текст, що шифрувався, знаходиться в файлі vusotsky.txt. Шифрування виконувалось функцією encrypter(). Були використані ключи розміром 2, 3, 4, 6 та 14 символа. Також я додав функцію довільного ключа, на вибір користувача, яка запускаєтся після виконаная шифровання заданих ключей. Зв'язок ключа, його довжини, індекси, отримані для кожного ключа, та отриманий результат продубльовані нижче у таблиці.

Ключ	Розмір	Індекс
ад	2	0.04086845466155811
рай	3	0.03697497656400558
киев	4	0.04001267340186116
одесса	6	0.03502823751522931
величественный	14	0.03382295780214468
Открытый текст		0.05247702945912665

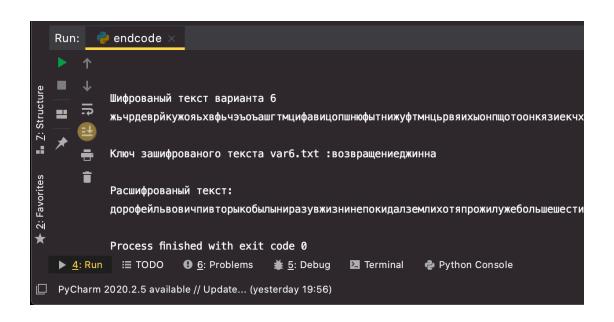


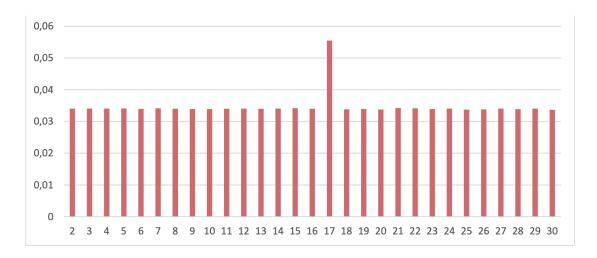
Завдання 3 (розшифрування тексту)

Варіант 6

Для розшифрування тексту було використанно функцію decrypt() та частостний кріптоаналіз.

Результат надано в наступному скриншоті





Середній індекс відповідності в залежності від вибранної довжини ключа

Використаний зашифрований текст так отриманний разшифрований текст розсташованні у файлах var6.txt та decrypted.txt відповідно. Файл decrypted.txt створюється автоматично.

Отриманий ключ:

возвращениеджинна

Шифрований текст

жьчрдеврйкужояьхвфьяэьоъашгтмцифавицопшнюфытнижуфтмнцьрвяихыонпщотоонкязиекзхмкхсъхшефюзг отпрыиуфжиьщефуюхведоьцооффьянкцирьоктэндокыизмурмуводинтэнцихынимиканизмойной отпимицизорефобокзиьтуденндетахлуубусизацияхнаящифвартьфирыкшихынимиканизмойной отпимицизорофобокзиьтуденндетахлуубусизацияхнаящифвартьфирыкынынхатчяицюыфийнывжши чиздициаейфаумащфийногрыдпытикомуштоптажиекцвхницютэрьсыажаянщтехтиртирикогосиридмфирызачаредеприкрипеннкуусыоьешдтт питяноущтеннях уставленных уставленн плить дениртэлуинок акандомини и денирования и денирования

Розшифрований текст

дорофейльвовичпивторыкобылыниразувжизнинепокидалземлихотяпрожилужебольшешестидесятилетработа лпрорабомстроительной компании домострой вхарьковестолицев краины любилпоры бачить сдрузьями на озерахр оганьского краязачертой городавыращивална дачному частке овощий фруктыво спитывалвну ковавот уезжать запре делыродной в краины нелюбилне смотряна возможности в связиссозданием глобальной сетиметропобывать на любой планете солнечной системы и даже за еепределамичто подвиглое госогласить ся на экскурсию полу не они самне в с остояниибылответить вероятносы гралисвоюрольрассказы друзейх ваставших сясвоими путешествиями и унеговзыгралолюбопыт ствопосмотреть вблизичтоже этотакое спутница земли окоторой такмного говорят детивнуки и дру зьякакбытонибылоаутромдвадцатьтретьегодекабряаккуратвначалосвятокдорофейльвовичвтайнеотродныхибл изкихпозвонилвбюроэкскурсийсолнечнойсистемызапинаясьобъяснилчегохочетивтотжеденьспомощьюметрод обралсядоаполлонтаунагороданалунеоткудадолжнабыланачаться экскурсия посамым красивыми загадочным местамспутницы земли аполлонтаунрасполагался наравнине моряспокой ствия недалекоот знаменитой бороздым аск елайнпохожейнаиизвилистоеруслорекиименноздеськогдатовконцедвадцатоговекасовершилпосадкуамериканс кийпилотируемыйкорабльаполлонодиннадцатьаточнееегопосадочныймодульестественноэкскурсантамзанима вшимкабинудвадцатиместногоэкскурсионногофлайтасначалапоказалипамятникаполлонуодиннадцатьпирамид уизлунногобазальтаспосадочнойплатформойиамериканскимфлагомазатемфлайтотправилсявпутешествиепом орюспокойствиязалитомуяркимсолнечнымсветом орюспокойствия в политиров обрастной орюспокойствия в политиров обрастной орюспокойствия в политиров орюспокойствия в политиров ориспорации ор авеселящуюсякомпаниюжадноразглядываяпроплывающиеподднищемфлайтациркиэскарпыкратерыиживопис ныегруппыскалмореспокойствияполучилосвоеназваниенеслучайноегоровнаясглаженнаяповерхностьтипична дляобширныхморейнадневнойсторонелуныиредкорадуетнаблюдателейпроявлениемвулканическойдеятельнос тиоднакоиздесьимелосьнемалоинтересныхместиобъектовкоторыедесяткилетволновалиастрономовизучающи хспутницуземлизагадочнаяцепочкакратеровподназваниемтенниснаяракеткаоколодвухдесятковямокдиаметром отпятидесятидостаметровпротянулисьудивительноровнойлиниейзаканчиваяськратеромпобольшедиаметромо колошестисотметроввпечатлениескладываетсятакоебудтополуннойповерхностидействительнопрокатилсяпод прыгиваятеннисныймячоставиввпылицепочкуследовсовиныймосткаменнаяаркачерезбороздумаскелайндлино йоколотрехкилометровизумительноровнаястенаобрывадлинойоколотридцатикилометромбудтоктотоотхватил ножомкусоклуннойповерхностиивыбросилвкосмосоставивсрезиложбинуглубинойвкилометрбороздазолотойр учейсамоенастоящееруслорекиширинойвполторакилометраидлинойвполторастасверканошеподлучамисолни акристалликамипиритацветочнаяклумбавозвышениерыхлойпородыоранжевогоцветадиаметромоколодвухкил ометровивысотойвдвестиметровдействительноклумбаеслипосмотретьсверхустоунхенджгруппаскалсплоским мвершинамисоединенных поверхудостаточноровными плитами практически неотличается отземногометалитиче скогокомплексаванглии инаконецбороздамаске лайндлиной околочеты рехсоткилометровтакже здорово похожая на руслореки шириной откилометрадотрех какобъяснил гидбороздана самом делепредставляет собой с двиговый раз ломлунной корыслучивший сядесяткими дли оновлетна задврезультате подвижки щита отударамете оритано сверх убороздавсеравнонапоминаетрекуидорофейльвовичдажепредставилкакпоруслутечетводаостанавливалисьивы ходилиизфлайтаодетыевпузыривакуумплотных спецкостюмовнесколькоразвкабинеаппаратаподдерживаласьно рмальная силатяжестипочтиземная авнеее царилолунноетя готениев шесть разслабее земного поэтому необошлось безкурье зовинеловких движений правдавсевконце концовпривыкликне обычайной легкостивтелей судовольстви емскакалипоместнымбуеракамвтомчислеидорофейльвовичполучившийнисчемнесравнимыеощущенияатеперь смехакальном сетным оусражамы объекта в поставлений объекта в поставления в поставления в поставления в поставления в поставления в поставлении объекта в поставления в поста идитефлайтспрозрачнымидосамогополастенкамиподнялсянадкратеромаваковаипонессякгоризонтусвисящейн аднимпочтиполнойземлейокрашивающейравнинувголубоватыйцветвместахгдележалатеньотскалосвещенных прямымисолнечнымилучамиприблизиласьрекабороздымаскелайнраздаласьвширьпревратиласьвкрутойглубин ойдокилометраканьоннаодномизплоскихгребнейканьонапоявилосьбелосеребристоепятнышкопревратилосьвх олмикзатемвгорусдыройвцентрефлайтзависвпарекилометровотэтойстраннойгорыиэкскурсантыначалирассма триватьобъектимевшийнеобычноеназваниезеробольшевсегосеребристыйкуполскратеромдиаметромвтрикило метранапоминалчеловеческийглазрадужкакотороговысохлаипожухлапревратившисьвбелоснежныйслоймхаив ызывалэтотглазотнюдьнеприятные ирадостные ощущения неомерзение нетноиневосторгслишком многов этом зр елищебылопугающегоиотталкивающегоиодновременнопритягивающеговзормолодежьпритихладорофейльво вичпочувствовалстеснениевгрудипосмотрелнагидатотулыбнулсякакнастоящийчеловекхотябылвсегонавсегови тсомнравитсячтоэтотакоеэффектквантовойэффузиикакговорятученыеобразноговорянагорныепородыподейств овалодыханиедемонанаэтомместеболеедвухсотлетназаднаходилсяториевыйрудникшахтакоторогодостиглашар овиднойполостигдеиспалджинннепосредственнокшахтенаснепропуститохрананотутрядоместь интересноеуще льеонообразовалось совсемне давновсего двамеся цаназадимыможем полюбовать сянарудник собрыва полетелизд оровоочень интересномых отимпрогулять сяраздались голосадорофейль вовичхотя инеиспытывал большежелани ягулятьоднаковозражатьнесталунеговозниклоощущениечтоонздёсьужебылкогдатохотяникогдараньшелунунеп осещалфлайтоблетелснежносеребристыйглазбывшеготориевогорудникакругомповернулвдольбороздымаскела оширеочевидноэтобылрезультатнедавнеголунотрясения окоторомговорил подпрыблего оширеочевидноэтобыли и правочения оширеочевидноэтобылрезультатнедавнеголунотрясения окоторомговорил гидприблизилась очередная трещинад ействительнообразовавшая живописное ущельесослоистымистенами флайтподпрыгнулисел на обрывескоторого былихорошовидныкуполобъектазероибороздамаскелайнэкскурсантыпосыпалисьизаппаратарадуясьвозможно стиразмятьсягурьбойнаправилиськобрывуперебрасываясьшуточкамиидурачасьвнихигралащенячьянергиямо лодостиидорофейльвовичнамгновениепозавиловалзадоруиоптимизмуюношейидевушекгодящихсяемучутьли невовнукионтожеполюбовалсянаснежнобелыйкуполвтрехкилометрахотобрывапотомтихонькоотошелотрезвя щихсямолодыхлюдейипрошелсявдольобрывавглядываясьвпротивоположнуюстенуущельявзгляднаткнулсянар ядчерныхотверстийпохожихнаследыпулеметнойочередизаинтересовавшисьдорофейльвовичпрыгнулвнизивкл ючивантигравпересекущельеопустилсянаузкийкарнизпередсамойбольшойдыройопредупрежденийгиданеотхо дитьдалекоотфлайтаонзабылдыраоказаласьвходомвпещеру