Міністерство освіти і науки України
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Фізико-технічний інститут

КРИПТОГРАФІЯ

КОМП’ЮТЕРНИЙ ПРАКТИКУМ №2

Криптоаналіз шифру Віженера

Виконав:
Студент III курсу ФТІ
Групи ФБ-06
Сулима Олексій
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).

Хід роботи

Виконував завдання за допомогою автоматизованої підстановки наступних за популярністю літер алфавіту у формулу

$$k = (y^* - x^*) \bmod m$$

Текст, який було обрано для шифрування міститься у файлі data.txt:

С замиранием сердца и нервною дрожью подошел он к преогромнейшему дому, выходившему одною стеной на канаву, а другою в-ю улицу. Этот дом стоял весь в мелких квартирах и заселен был всякими промышленниками – портными, слесарями, кухарками, разными немцами, девицами, живущими от себя, мелким чиновничеством и проч. Входящие и выходящие так и шмыгали под обоими воротами и на обоих дворах дома. Тут служили три или четыре дворника. Молодой человек был очень доволен, не встретив ни которого из них, и неприметно проскользнул сейчас же из ворот направо на лестницу. Лестница была темная и узкая, «черная», но он все уже это знал и изучил, и ему вся эта обстановка нравилась: в такой темноте даже и любопытный взгляд был неопасен. «Если о сю пору я так боюсь, что же было бы, если б и действительно как-нибудь случилось до самого дела дойти?..» – подумал он невольно, проходя в четвертый этаж. Здесь загородили ему дорогу отставные солдаты-носильщики, выносившие из одной квартиры мебель. Он уже прежде знал, что в этой квартире жил один семейный немец, чиновник: «Стало быть, этот немец теперь выезжает, и, стало быть, в четвертом этаже, по этой лестнице и на этой площадке, остается, на некоторое время, только одна старухина квартира занятая. Это хорошо… на всякий случай…» – подумал он опять и позвонил в старухину квартиру. Звонок брякнул слабо, как будто был сделан из жести, а не из меди. В подобных мелких квартирах таких домов почти всё такие звонки. Он уже забыл звон этого колокольчика, и теперь этот особенный звон как будто вдруг ему что-то напомнил и ясно представил… Он так и вздрогнул, слишком уж ослабели нервы на этот раз. Немного спустя дверь приотворилась на крошечную щелочку: жилица оглядывала из

щели пришедшего с видимым недоверием, и только виднелись ее сверкавшие из темноты глазки. Но, увидав на площадке много народу, она ободрилась и отворила совсем. Молодой человек переступил через порог в темную прихожую, разгороженную перегородкой, за которою была крошечная кухня. Старуха стояла перед ним молча и вопросительно на него глядела. Это была крошечная сухая старушонка, лет шестидесяти, с вострыми и злыми глазками, с маленьким вострым носом и простоволосая. Белобрысые, мало поседевшие волосы ее были жирно смазаны маслом. На ее тонкой и длинной шее, похожей на куриную ногу, было наверчено какое-то фланелевое тряпье, а на плечах, несмотря на жару, болталась вся истрепанная и пожелтелая меховая кацавейка. Старушонка поминутно кашляла и кряхтела. Должно быть, молодой человек взглянул на нее каким-нибудь особенным взглядом, потому что и в ее глазах мелькнула вдруг опять прежняя недоверчивость.

Після видалення пробілів та інших знаків я загнав новий чистий текст у text.txt.

Ключі шифрування:

```
y = ['за', 'нер', 'гром', 'чинов', 'ойквартире', 'иласовсеммо', 'черезпорогвт',
'старухинаквар', 'этотнемецтепер', 'жестианеизмедив', 'толькооднастарух',
'зщелиприедегосвид', 'ечахнесмотрянажару', 'нилвстарухинукварти',
'человекпереступилчер']
```

Результат індексів відповідності:

lab2main.py | index.txt

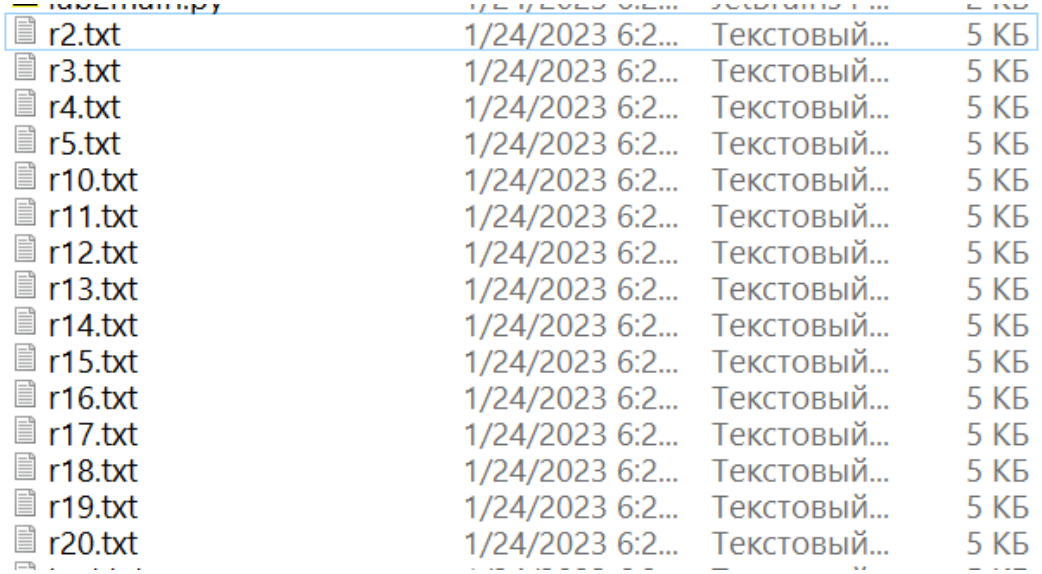
```
index r2 = 0.04049164463852656
index r3 = 0.041305581033342975
index r4 = 0.038633795360607646
index r5 = 0.03537489324130667
index r10 = 0.03542810348761599
index r11 = 0.03691122636991582
index r12 = 0.034947858467959766
index r13 = 0.03504435840618178
index r14 = 0.03628487864005433
index r15 = 0.036573025651848064
index r16 = 0.035011440202956524
index r17 = 0.03576269673135769
index r18 = 0.03421689398264264
index r19 = 0.03490276503888407
index r20 = 0.03543712217343113
```

Приклад зашифрованого тексту з ключем r5:

йпныкииыцздътяжоихьзикыэаьщьфюхчьтрэуььмзщтэеицъьзбнъвжжфбрэнцсцдэфбэжецлафэхьчпчтнь
въьнттлльмдхьщцщлеаэфьцъафжзщрзйдпызгтхдмъиюбкиигцйчътъзейиъдйзчцоачюэотутьпатныкзцю
бптфханэъняbдрчвччщчооащнхптфхьздяныкьнпцщчфхфкъьжцоацаазщзъунвръжкецпькпнябджфхют
жапдрьзжцзакидрьзжцзкичцотлнъкзцсэгжръцджщьбвдрхьвжйьцчькьявнмьывкьаанлохъккщхцнаатбэ
инсррихххщвдцщэжжсеунжктщгтуьжзедсэджутьпэкябтэыхрпатьбрицрэкяххдкенэякднаьрзщьамжуйхп
луяулпияфзаппэтжыыосиипэпчутафердвнэъаькоиойнчытыпчзхвйвимжзихннпжцыруэьууякцфьвгрхх
хпрщцздьпабфынэгйыньръътньтчкхъвйдпбввццбздхьбзьиуукгжоэстыыйлъпръбьйиъпэцэоуэхтанацямс

жщбнфчтоэайдебрюнойнжйиуугроцжэсябдаытъюецчомеровжуъщвъауьаюьцяоожльтзгисэлкрээжлфн
ърехтрргдыэсицгэжцкеуфънюбэбеаоиямтаюяирэтжмхъкэфбтрицрвркъаодегтаргмнбэецяцнубхщкъгы
эуакхукяцсьрбтпоткрюйоэйтъюжхбфззщтфжэпыонпыьрякццщдчщацтэохърьрыазднцьэбхтызоахьръх
хщукищэгтыйлфжыыуоэяаусэщйрээпуозкрябвгцойфукеуфънюбрдеаоиэчьлфжсщуукххезахнлфжсэър
рисщзжъаозкъмьвенчэфжщьудинънфжуйщржмыоукиювчахнщдчщацтчпньбкимлфжюьяржхнруцтхчу
гьеолзцсвочуььрззаккзцфррерщрукиювчахбщдчщацтлппэпжтоябвхбъугиоэмчтовжкцойнймтъверффз
йыхопэрфызърпюрьцоьэнфтъмаючрвиыхявнынщкнмьыръчьжфакябввртхджхчцреьууйчйиъйъцылфж
льщргцчэнуахщваытюзидкбркцяэгэхыйлякььмчтовжкцпттллтыхпыьбреиээоерщцбйхьютэмябвърщэп
кичцдямюэееьщанатьыхюцяъвщнщцпэщпйпчеаэфиифьздхьсрйчбафцмпутучюцркккьякгиякпчтюэзпхб
мыэуьжмлохъкоиьснцмирвгихххыэухютансуежъпцжафиыпэмьрзиртыккцщкмжкхтпэухаюэнярзитнркэ
рфбздхьбэыунхмахьвдамнрпччщэычмчуоецрэпчщьтхжхнэгжмюцнчъйцрккьякгияэдйнъыргцсэлпнщэ
дэтэутэъавсауеутэпээтжлпбздхбмсиргэилжюойыцюэиэхыважнюуежщьтмжсфомжыьярхйиъввщьуъеи
мщхнхмафчщбдвйыьннччтязьххыожуеокъцэярйраунухььвенрэегзсунчеаэгтунщтжнеьвцъбдвцъаотлц
ыщвгнауукрсууцыхаджъаяэдрххнтфхснчпчооаъъонэхйщкдкьафигъьрйцъцсицябръцщэучзоунжйюйут
нъонжчьазьнпцзъцщэутнтпэгруцтецяывяиыйочъщэоеитуфжхчэламщцпеццуззцгэиэсыомлщхьххъьсх
щгщэпчктяъэхьщввцтбрмуньзгнпэзкщмююэиыосгнеоченяыркщмьвюиювгжуаончъйруцрябтэчньпчзх
юрюнщбзгимызнцпобвидодэсчоукиювретнюрдрывфецчонцунцмизгбзгисэнюхьпэкдъэнжмьчъэуьрзвк
фснцхбъпчхтумчтхыпайбтюжъьпзехиыдялщнжжфээфжфбжфжрпузыунхвнфтъювхбъвъмювежчмбюз
щтфпцзыужжктяъакьафу

Зашифровані тексти з різними ключами містяться у файлах r(2-20).txt



Висновок:

Навчився зашифровувати довільно обраний відкритий текст за шифром Віженера з різними ключами. Також сміг підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифртекстів.