



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

Криптографія

Лабораторний практикум №3

Виконали:
Студенти групи ФБ-83
Осінній Максим
Яненко Наталя
Перевірив:
Чорний. О.

Київ - 2020

1 Порядок виконання роботи

1. Уважно прочитати методичні вказівки до виконання комп'ютерного практикуму.
2. Реалізувати підпрограми із необхідними математичними операціями: обчисленням оберненого елемента за модулем із використанням розширеного алгоритму Евкліда, розв'язуванням лінійних порівнянь. При розв'язуванні порівнянь потрібно коректно обробляти випадок із декількома розв'язками, повертаючи їх усі.
3. За допомогою програми обчислення частот біграм, яка написана в ході виконання комп'ютерного практикуму №1, знайти 5 найчастіших біграм запропонованого шифртексту (за варіантом).
4. Перебрати можливі варіанти співставлення частих біграм мови та частих біграм шифртексту (розглядаючи пари біграм із п'яти найчастіших). Для кожного співставлення знайти можливі кандидати на ключ (a,b) шляхом розв'язання системи (1).
5. Для кожного кандидата на ключ дешифрувати шифртекст. Якщо шифртекст не є змістовним текстом російською мовою, відкинути цього кандидата.
6. Повторювати дії 3-4 доти, доки дешифрований текст не буде змістовним.

2 Хід роботи

2.1 Підрахунок біграм

| n | Шифртекст | частота | Відкр. текст | частота |
|---|-----------|-----------|--------------|-----------|
| 1 | се | 0.0167467 | то | 0.0142204 |
| 2 | дэ | 0.0141003 | ст | 0.0129802 |
| 3 | хв | 0.0132733 | ен | 0.0120949 |
| 4 | те | 0.0122809 | не | 0.0118921 |
| 5 | че/фл | 0.0119501 | но | 0.0117946 |

Табл. 1: Найчастіші біграми

2.2 Зашифрований текст

фелсэугиселбуэйатеополмхфкплойющпбвуцакэюйкыкусявялеюйкуешяэюазыкйюязъзвусяюпдэжввятедыюячтхкзыере
явйвтэебуагзлчедэвюэеямдюзвюеюющющешгфлцхазцччеолмхечнзпвледсдямвзжевмэбйрбсюраййвюухыешлифвсоч
люряийвюухыешгтбютазцягтьчяяжцфлпнитсетеуюйвздяшевэущенибсхеюеюеузьяюпсдямээыгнзйвиснрижшдуй
ьюфлийэфашгкякзшьяпатбдспвясзгинкэтбыпрбгтбшйсйсыдэдемечмьявжзаслджкхчбчмчйвувтгинкэтбыпйльхавгц
кзьяэькамашлщмхыкмчуябллдпволмхечмчкбуштзвцйвнбюеяммчедэядаяэюнвшьюзщаклфлпнцючпммнбюозэеяэявч
усвесехкчюгупвийбухввлэыволмхсьжектъясезвъдснлулшдяюпсюагкбжйуяичявуссеьхвжштъжсуйсыхсмччесссвеннэ
сыеюолрщдэисшисерекъбпэлддьеюрябенбауасызцрцямеезфразлдажчюзнйпупввеюкусцяэчретлктзцаушцзоэчуегч
рразыеуочссхсзмнзфкузмасызыеичеолрщсррятекщазшыжешьчекбмаедуззэитсефкфкемющээжйэвррщтъжслеаявежчл
брблфкдчшдсзсыщущеофлеяэюипчккггтутехсаагмаэчявемцшибыекичслвьчблтгинауэеядюдэпббйьящабазуьхсэвчг
эебсьныяплгхслшднзысвнслызенбйдэгфлпнюшжмвусесехкмашлсющрэчретгкэбйцйсыхсфкемуйыгфлхуыкнзшжксмг
эебсьнытгжчюсйвзйюянюююячеуспссмеоеочхедэеюфцжедыющэвныпшжаюфнпвевхчфкаеуйгзшглсйэеяеязвюерекэ
хуввжвэйяжсйсьвемчфкэьхедэеюфцкыюязсыечвлзгвюаежзюквесехерглсрхяэюеюзэбеаяэсвийувюухыешгеющрзцчче
олмхечнзвчичиймеаеьаьччббддатеубфлцсрбрщюяевисувпзшгвюаежзчюячеумиежвемшдвчусмэебриябйвесехкпюмчзун
шжвдядюсссввчумыепвлпщыдхвошкчхсйежешсжвдуюющфстепйцхыедэкаплгхазлдвнухокусызыцнзчузъхыввпзкч
уйцйрасетегльнйвйстерирчссцяэьсжвдядюшасэбауретешщэщрхвмчющалсвчумыесыедшьдямзггээрспвевьнзмчшж
ксдйкдсбдемиаецяэюядчймхуыквщлбйпцкэиузбвюдэпфэрщэщрхвнйпчячкхгьбфтсличдмщйвцяэюспвчсемщйвця
эюспвчввуеивхзшгебрщвюцэрякбсыюяхывдщэщрхвссверчпмхвхвхгжчрдэпвэящаензэтэссувнзшупвзйазэяхывув
пвевшврбюятехланийжректижуеивьякбзблвюжгебткязрящаенквткелочельсвузфнфлшпкякбсыеюаеидшьуэрякбуя
евйвзясчищэнгитюдэтежвемсейвчясемзччвесехерщфлюзщашлпсдбауячедемияюушьоьпвевшвчбдунэеюгщэщрхв
мчльсвфэйтсефкюкочешвхсвьссьссьмввнаулкззэсрюгяевмчсэьатеуочдэвсмччехчгхсвясослехехчрщлзсыйвгсмч
хньяхывдщэщрхвсумеолфрьщэнзильвдсврчбжавюблнзэиткясерщлбйпбшзаетуйячтхэеяйшцедэхетекбьщмчяя
веревхывивисвзлшдзвъчбдцюяевкщкчехетцччедццблфнмчьхедэеюжчстевектээлфзюяудзжуньпкэьвнбюязшы
нзэсбсюнаувюпвевхчочдэсыячопдэдемюячсхвхзфтдынзуйсыаечеечюемпврбвюблшдыузмщпвоелбоыбйшьтлуймзсс
ччхзюйзэебсыюяевыеисмшдвнаулдзжунетибмчлльщцэнгхекбвюцэппенрбкцээшдкэгчвъшбюсебнпбшпжжцэьбфншьае
ыеэюьтыднэнирбпукюбйпволеюющэщрхсхйвдащлдэпббпгьхейлсбюпсьщщясктнщазлцсуюряезбпвчмтсензедсыехнпа
яблсввчхеретеонвюдчдэслтгбйряеввяевхкыйвцупвшелеезфштжретьдзюямукпвчсехенсдямзмечемщзэцуюазйбаг

[illegible]

ичных предположений отом как и с какой стороны побежит зверь и как он будет травить его надежда сме-
нялась отчаянием несколько раз оно обращался к богу с мольбой о том чтобы волк вышел на него он молил
с яством страстным и совестливым чувством которое молят ся люди в минуты сильного волнения завис-
ящего от ничтожной причины ну что тебе стоить говорить лон богу сделать это для меня значить что ты велики
что грех тебе просить об этом но ради бога сделай что бы на меня вылез матерый и что бы карай на глазах
дядюшки который воноттуда смотрит вцепился ему мертвой хваткой в горло ты сячу раз в эти полчаса у
порным напряженными беспокойным взглядом кидавал росто во пушку лесов с двумя редкими дубами
а до синовым подседом и враг сизмытм краем и шапку дядюшки чуть видневшего ся из закустана право
нет не будет этого счастья думал росто вачто бысто и лон не будет мнев сегда и вкартах и на вой не все
м несчастье а устерлици долоховярко но быстро сменяясь мелькаливего воображении толь оодин раз
быв жизни затавить матерого волка больше я не желаю думал он на прягая слух и зрение оглядываясь н
алево и опять направо и прислушиваясь к малейшиму ттенкам звуков гона он взглянул опять направо и
увидал что попустынному полку навстречу к нему бежал что тот не этон не может быть подумал росто в
желовздыхая как вздыхает человек при совершении того что было долго ожидаемо им совершилось вел-
ичайшее счастье и так просто без шума без блеска без означения росто вачто не верил своим глазам и с
омнение это продолжалось более секунды волк бежал впереди перепрыгнул тяжелорытвиную которая б
ыла на его дороге это был старый зверь с седою спиной и снаедемным красноватым брюхом он бежал нето
ропливо очевидно убежденный что никто не видит его росто вачто не глянул ся на соба ки и не лежал и с
ояли не видя волка и ничего не понимая старый карай завернув голову и о скалив желтые зубы сердито о
тыскивая блоху щелкали ми на задних ляжках улюлюлюшопотом оттопыривая губы проговорил росто в
обаки дрогнув железками в скопи на стороживуши карай почесал свою ляжку и встал на стороживуши
и слеткам отнул хвостом на котором висели войлоки шерсти пускать не пускать говорил сам себе нико
лай в то время как волк подвигался к нему от делясь отлесав другт ся физиономия волка изменилась о
нвздрогнул увидавеще вероятнее никогдане виданные им человеческие глаза устремленные на него и
слетка поворотив кохотнику голову остановился назади и впереди в сравновпередвидно какбудто
сказал он сам себе ипустился впередужене оглядываясь мягким редкимвольнымнорешительнымскок
омулюлюнесвоимголосомзакричал николай и самасобойстремглав понесласьего добрая лошадь под
гору перескакивая через водомоины впоперечь волку иеще быстрее обогнавее понеслись собаки ник
олай не слышал своего крика не чувствовал того что он скачет не видал ни собак ни места по которому
н скачет он видел толь ко волка который усилив свой бег скакал не переменив направления положи не п
ервая показалась вблизи зверя чернотепега широко за да я милкаистала приближаться сяк зверю ближе б
лиже вот она пришла к нему и волк чуть покосился на нее и вместо того чтобы наддаться ка она это все
гда делала милка в друг подняв хвост стала упираться на передние ноги улюлюлюлюкричал николай кр
асныйлюбимвыскачил изамилкистремительно бросился на волка и схватил его за гачилияжки задних
ног нувтуж секунду испуганно перескочил на другую сторону волк присел щелкнул зубами и опять под
нялся и поскакал вперед провожаемый на аршин расстояния в семисобаками не приближавшимися к нем
у уйдет не этон невозможно думал николай продолжая кричать охрипнувшимголосом карай улюлюкрич
а лонотыскивая глазами старого кобеля единственную свою надежду карай извсех своих старых сил
ытянувшись сколь ко мог глядя на волка тяжелоскакал в сторону от зверя наперерез ему но побыстрот
ескока волка и медленностискока собаки было видно что расчет карая былшибочен николайужене да
лековпередисебя видел тотлес до которого добежав волк уйдетнаверное впереди показались собак
и охотник скакавший почти навстречуещебыла надежда незнакомый николаю муругий молодой длинн
ый кобель чужой сворыстремительно подлетелспереди к волку и почти прокинул его волк быстро как
нельзя было ожидать от него приподнялся и бросился к муругому кобелю щелкнул зубами и окровавлен
ный сраспоротымбоком кобель пронзительно завизжавткнулся головой в землю караюшка отец плака
л николай старый кобель с своим имотавшимися на ляжках клоками благодаря происшедшей остановке
перерезывая дорожку волку былуже в пяти шагах от него какбудто почувствовалавопастьволк покос
ил ся на караяеще дальшеспрятав поленохотнежду нога надалскоку нутути николай видел толь ко ч
точто тосделалось скараемонмгновенно очутился на волке и с ним вмести повалился кубарем в водом
о и ну которая была перед ним там и нутакогданиколайувидал в водомоине копошавшихся сволком соба
ки зпод которых виднелась седая шерсть волка его вытянувшаяся задняя нога и прижатые мишами исп
уганная издыхающая голова карай держала

3 Висновки

Отже, під час цієї лабораторної роботи ми навчилися використовувати частотний аналіз при розшифруванні шифру Віженера. Навчилися фільтрувати отримані тексти за неіснуючими у мові біграмами.