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

Симетрична криптографія
Комп’ютерний практикум №3

Криптоаналіз афінної біграмної підстановки
Варіант - №1

Виконали:
студенти групи ФІ-94
Величко Олена
Мельник Ілля

Перевірив:
Чорний О.М.

Київ 2022

ЗАГАЛЬНІ ВІДОМОСТІ

1. Мета роботи

Набуття навичок частотного аналізу на прикладі розкриття моноалфавітної підстановки; опанування прийомами роботи в модулярній арифметиці.

2. Постановка задачі

Створити програму для знаходження ключа шифру афінної підстановки та дешифрувати текст за варінтом.

3. Хід роботи

0. Уважно прочитати методичні вказівки до виконання комп'ютерного практикуму.

1. Реалізувати підпрограми із необхідними математичними операціями: обчисленням оберненого елементу за модулем із використанням розширеного алгоритму Евкліда, розв'язуванням лінійних порівнянь. При розв'язуванні порівнянь потрібно коректно обробляти випадок із декількома розв'язками, повертаючи їхусі.

2. За допомогою програми обчислення частот біграм, яка написана в ході виконання комп'ютерного практикуму №1, знайти 5 найчастіших біграм запропонованого шифротексту (за варіантом).

3. Перебрати можливі варіанти співставлення частих біграм мови та частих Біграм шифротексту (розглядаючи пари біграм із п'яти найчастіших). Для кожного співставлення знайти можливі кандидати на ключ (a,b) шляхом розв'язання системи (1).

4. Для кожного кандидата на ключ дешифрувати шифротекст. Якщо шифротекст не є змістовним текстом російською мовою, відкинути цього кандидата.

5. Повторювати дії 3-4 доти, доки дешифрований текст не буде змістовним. У разі необхідності змінити кодування алфавіту (див. методичні вказівки).

4. Опис труднощів

1). Труднощі зі знаходженням ключа.

Після співставлення п'ьятьох найчастіших біграм у мові та в шифрованому тексті, ключ, який би перетворював шифротекст на змістовний текст російською мовою, так і не був знайдений. Тому було прийнято рішення розглядати не 5 найчастіших біграм шифротексту, а 25. Після чого була знайдена біграма «шч», яка не входить у п'ятірку найчастіших, але впливає на знаходження ключа.

2). Кодування алфавіту.

Нам попався варіант з кодуванням ь = 26, ы = 27, що було виявлено при аналізі розшифрованого тексту. Для цього було створено 4 невеличких функції для знаходження коду літери та навпаки (літери за кодом), відповідно до варіанту алфавіту.

ПРАКТИЧНА ЧАСТИНА

1. **Найчастіші біграми шифротексту (за варіантом)**

Біграма	Код	Кількість у тексті
рн	509	63
ыч	860	44
нк	413	43
цз	689	37
тч	518	33
шч	767	26

2. **Опис роботи автоматичного розпізнавача російської мови**

Для знаходження змістовного тексту серед тексту-шуму було написано функцію recognizer(), яка використовує для розпізнавання теоретичні значення відсотків літер «о», «а» та «е» в тексті російською мовою в сукупності. Тексти, де відсотки цих букв нижче теоретичних значень – відкидаються.

3. **Шифрований текст**

Знайдене значення ключа: a=13, b=151.

лквдвдьышкрбызякиабшачрнвязарчтчлчькзтманэмнязяыбштрпнхтрхрнзтжккысечамнмпы
вйвфяжтинфвйвйвсжнпчнмпгущзкыфвйвутсюцзкыкынмотзщбйьыбшхолуычгкицепзкиан
ьуыфллфтыраючькиащзтыфэнкйяпезтнкжккысечамнмпжэпаычйдбцвсшчмтшслаиятасзбч
жйьыбшывлтйэзщбцпцмпщрифкздтеэкктщзархрчосйпрйжклечаккяжюыщяояфскчбяызрч
йзчвгзжзычэявсшчтщлжочшызюшхачрнтмнкуфйзбчечвпчнотмнктхеотнчняцзбшрчычбчн
кицгщлчькевочфыщяцзреотйсфтбйщялчдечамнмпйарчтчццзтьярняыхашхаытыыздсепцяь
аючшзбшзтжмсяачрнвязаозеарчэяицкятчрогцфэкыпэзтйпчаэеэявахыдпдойдкрмпбцмвеэл
жочрчщтецрнбяшкуэтыычлчокбцккузбнинепжвининачрнсджяцццаиятчщтецрнбяшквдиаб
цотияьацційвычфткюмпьяэяддаьччшызюсяуядсяжутрхбцшчрнфэтзткзтцтеялчакиажчштзм
нксябяешщтецрнбяшкуэчцеопнхоьяючбястзырзгьфлуфжмнкецььэтнкфячащжвжяымэвяча
тьияцзоеязднеэмэйкоевсщыяыяажвычцяучпяэязяшкинвдэякзюнзтмакырцсоушрнецчнкяуя
лжочознкьызаццнкяжсгмпчнвдепйдрчкеэярклнвцычпрычжкнпщюрчньаччквсеокяяорнбчч
нйцнбшзикзчшклзпеепаопниашчеквдзеязэгцеккьызаццнкшчрнхкнчьхвсфэиащзинэяьяцзч
цычжтмэывйвщтецрнбяшктфбйьыемтщцзжеьытнщрпаозвзьнотпанхзайдкрмпбцсрпаццру
щзлчшклееэхкжяццлтяыбчлуучвзпяэякящяцзэклтвсбцяыыцлтбцдйрцецкзвзвычяквсойюш
ххолуычннйвбнзеевсоцзпахышчгзючушчядкщрпаозмеяззябчмтмаэзуыйюфэхьбшркбцуэд
йуфрняыннйвцяучрнкейпрцккутгщяжйухыксмпкырабцпабштхлтйвчябксогьракыбротхыа
чрнмнкршчуярачыбяцзрчфяяктфчнвдщтецрнбяшкдфччжшюжачрнвязарчтчучнплзраюьтп
нкшчюйзтвйпцдзтофтфэцтнкэофтчнщцккуфпяыцщряжеегщпцбцхкюзгзщырнэяччяыцзыэ
щрмпбцсрпарчтчбйхярняыжклжььцснкшчэяутпамзгьпнсевсэзфяцзоэцтнвеэззвьдчекеэгыз
нзтчнпнивучппжкнкэблыибшхязрнпыьарчньччфьстланвеэиэмпрчвьмкеэйкогхчтыыззэивь
яньзяфякщтыэзчягшяжпьсжфтщюызкдзтзщачзяюшкзйзлафпэойзьялчуцднеэнпейвязярнбй
еплюдфызякиащзачрнвязаозеьхьрнфпечзэгмшчрнйахыбшнрчнмпмэхчйцбйвсчнмпмэьяюч
бяьярняыцеязочйсхкфпхотнртмэчзкыквипйнктейесолйджкмэшчрзжйеспнмэйчяовытылуы
чмебцкяюцотноыкиащзфтногзаашятчфяжтгщтщвырчычбчтчжкрйупиажмыяшкмнйврбфяе
соркееэллцеиащзцяцзьзмзщяебтцфвебзозяньюжючьвзжчсгьтчэыучрнепйаозделнйааьцяцз

экйэфтйсрнецеопнхоинхыэврцсбчзмтманэмнязяыцзйсиаычицнввдбцкыьярнбяутсюцзкыф
пцеэярнкецзкышчднжчюнйпозяыцзнкйсепькжчокбцпцмнйаэккчюжяычягшнвдфкгнкмяфт
паюьукфвецыогзбшучяпхкььоэинрцогэбфтпаюьтпнкэофяачщдвсеофтпаюьукфвмаолпаццн
кяжьцсротвжуяддьыцзяквякяяоебхзлзмзгштышспаэтивщзексонвючшкиабшбйчззсеобйлзи
ротщзфтйсучфжэвдфяпьзеебччцщяцзкодпшяюачйкщебччекиабшфяяцмнкыбэкгхчтыгшшч
кгнккршчтчиншчияцзывьяючбятьюьюаьыкьзаучйзтысюиебчщзечучючькваднеэльачрнвяз
арчтчйдбйеплюрбучэтийшчрнвцебтцузйджчутеэььсаучоччкиабшебхзбшфтногзйюрбхобят
чйцотасбйбччяцегщечеойюрбмэипкйчнезучлчмыбшхыздыяжкфэмпюжфтецжкнкецсспнез
нащзбштыфтфэотучиншчияцзовйдзеотечамнклзйяебччекфвйкинвдщыечикфвжяццзебчоч
ьвеслеяздчюзюабйчыикфтщрчащяцзшсиаычицнввдевфтпаюьукфвйэинбящзещецпйзтжятч
хбцяычлуычфтлзньхярнбяшкжкмафпзкфвчьхззгьутчняьнязьянвсяюыььытнотшрычйцсспн
мпйаццеяычрьхярнечяыцзчнйвшхнвючшкиачяюцйдбцььэтнкфякэцтзыхынмлзещккмвинзт
чхрытнбцйдгмтщцзрньырнсятчкывыгняжйзутйэлчцяцйцнйамврьйпзквдзтмаьпнкэофяйтм
пдфыяечювузпебцйснуычфтинрцзтсрсяьыйтсюжяюаяащявьфлфэбйьыичнафпзксоыярнгьт
нрцтыяьрнэякпнкшчрнгсиаычицнввдевинзтсолчспейцаыячыбшйдзеэярнкецзрчжйупецйдг
мтщцзтыфтецщятыспецяжлчштзщеэтыиылчтчкяяоечеклнжшдэпаычычтчбнбйтзиклнязчн
йвфэбйьыичжцхтзщфпмавцеыичвззэлзбьзаццицхкпцкяхыозбятчызякиащзфяеыюччажсча
щзьянвшхьягнлжчцеофлшххобятчьыдсьышзчягшшчрнфэнрчнмпйаццнкпнотсзлчрнссзмое
жчыккюнкэбппкйфэуэебзоеыхынмицйдеэккотнчштплнкэотрчнмнмпмэчнйвдэмпкрнхжки
ыюзрнечекицяыькеэиыюзрнучиншчияцзовиылчнькяуянпйсбцмнмпзкеэзщйхчащзднеэшд
шызюуфачштвснюфязюуфзайдщытчычлждееэкрлрмпбцмвзаючькдфызякиащзачрнвязарч
тчсжлжыяызызэтшийвычьывсхкрчызьярнбяшктфссяыкыьярнбяшкчхйдкрэягцшрифшчучл
жияшкрбнитятнрцшчрнгятчлаэтмэщяшкиабшсеотбяющузрчычьышсепькейуплеязбярнсят
чтажсеэзщйхтщньфпчаыячыбшфтпаюьукфвеэсятчфяучыссбхяпацытыызкьццзтьянввящы
бчяыцзпнйввяочьяхыцзицучюкмэвдючюжрьхярнечяыбшрйкщфяжтгщецйсвйпцсбшмпаыч
фткгнкыкряеыичвзрнпйкщтыызэзэкицбчичжеиажчыккюнкэбмзяеязговыцзцеотгзякчхучо
жечгзфтинрцбйзтрнзьфлшхфэычаэгмнкуффтчавяюзаояалсецгщлчькиащзрьцпфэцтбцккэо
ачрнвязарчтчзайяхялчькбйупбйфчыкпащзстзщиовьфэхьгшмзекчхюыьытнотбцшчучючця
цзицтллфвычялкшяюаэкйпщрсялкицбчвыфябйщщмнмпзквдевйвюжючнвзщккзеязщышкч
хбйрнночягшрняыдкбцкяцяечикфвсбхятччянарчэясрмэтыфжхяшкйяиаючькнксяучяпкмпл
йяочрнзтжкшрмпбцсрпарчтчюеэявсепнкэбфяжтгщднинепжвгщтытнвдкрычянйвдфмзьнк
щфяесйпхобнжчшчфтыуычдезецнмяучтпмнфпиайаечфэйсхкрнечжцьяимицрнбчтчнасжнп
оебччцеопнхофяжтгщачрнвязаозгкзщпцйпкяяоиыйзбтедсяхынмпаэзхыызйдмусзщяхнфве
этыычлчокбцккузбнжчуйупучьцотцяьнщммпуэфтцежскыназебчечцсецкзйзхоуччяэяеагщт
ыцзяаесзтвдйэузучнпйсрбчзньныачякуэтырнбчнксяжцпажэецотноыккрычднмнйвтыожяы
мэсогефпоемзчйупйпщюйафэхнеэеэйджкицбчвырчычзжюцхырчнааьшыпащявьпнзеэяыя
ызбшкыозрнотмусзщяхаэбычпабшкытнщммпрбчачяязсьццотцсмннуычпеепшчеьбяэяшки
абшпкмпдщюевсзьмеязэзтыжцзеотлжееинеэнрычщывжккйэфяжзьянвшхфтцежсрчзнйвты
ожяымэдфгефпоемзссиаычицнвввджкйсиахыычяктзфятыыякоыечзнзтчхучычньбнзежкфэ
кксяйцщщккяжжагефпоеычссяжйзфтцежскыйзччщяикнкяжжаиаычэкуфиахыпнхофяяаяж
еы

4. Розшифрований текст

многограннуюличностьдостоевскогоможнорассматриватьсчетырехсторонкакписателякак
невротикакакмыслителяэтикаикакгрешникакакжеразобратьсявэтойневольносмущающейн
ассложностинаименееспоренонкакписательместоеговодномрядусшекспиромбратьякарама
зовывеличайшийроманизвсехкогдалибонаписанныхалегендаовеликоминквизитореодноиз

высочайшихдостижениймировойлитературыпереоценитькотороеневозможноксожалению
передпроблемойписательскоготворчествапсихоанализдолженсложитьоружиедостоевский
скореевсегоуязвимкакморалистпредставляяегочеловекомвысоконравственнымнатомоснов
аниичтотолькототдостигаетвысшегонравственногосовершенствактопрошелчерезглубочай
шиебездныгреховностимыигнорируемодносоображениеведьнравственнымявляетсячелове
креагирующийуженавнутреннеиспытываемоеискушениеприэтомемунеподдаваяськтожеп
опеременноготогрешиттораскаиваясьставитсебевысокиенравственныецелитоголегкоупрекн
утьвтомчтоонслишкомудобнодлясебястроитсвоюжизньоннеисполняетосновногопринципа
нравственностинеобходимостиотречениявтовремякакнравственныйобразжизнивпрактиче
скихинтересахвсегочеловечестваэтимоннапоминаетварваровэпохипереселениянародоввар
варовубивавшихизатемкаявшихсявэтомтакчтопокаяниестановилосьтехническимпримеро
мрасчищавшимпутькновымубийствамтакжепоступаливангрозныйэтасделкассовестьюхар
актернаярусскаячертадостаточнобесславениконечныйитогнравственнойборьбыдостоевск
огопослеисступленнойборьбывоимяпримиренияпритязанийпервичныхпозывовиндивидас
требованиямичеловеческогообществаонвынужденнорегрессируеткподчинениюмирскому
идуховномуавторитетукпоклонениюцарюихристианскомубогукрусскомумелкодушномун
ационализмукчемуменеезначительныеумыпришлисгораздоменьшимиусилиямичемонвэто
мслабоеместобольшойличностидостоевскийупустилвозможностьстатьучителемиосвободи
телемчеловечестваиприсоединилсяктюремщикамкультурабудущегонемногимбудетемуоб
язанавэтомповсейвероятностипроявилсяегоневрозиззакоторогоонибылосужденнатакуюне
удачупомощипостиженияисилелюбвиклюдямемубылоткрытдругойапостольскийпутьслуж
ениянампредставляетсяотталкивающимрассматриваниедостоевскоговкачествегрешникаи
липреступниканоэтоотталкиваниенедолжноосновыватьсянаобывательскойоценкепреступ
никавыявитьподлиннуюмотивациюпреступлениянедолгодляпреступникасущественныдве
чертыбезграничноесебялюбиеисильнаядеструктивнаясклонностьобщимдляобеихчертипре
дпосылкойдляихпроявленийявляетсябезлюбовностьнехваткаэмоциональнооценочногоотн
ошениякчеловекутутсразувспоминаешьпротивоположноеэтомуудостоевскогоегобольшую
потребностьвлюбвииегоогромнуюспособностьлюбитьпроявившуюсявегосверхдобротеип
озволявшуюемулюбитьипомогатьтамгдеонимелбыправоненавидетьимститьнапримерпоот
ношениюкегопервойженеиеелюбовникунотогдавозникаетвопросоткудаприходитсоблазнп
ричислениядостоевскогокпреступникамответиззавыбораегосюжетовэтопреимущественно
насильникиубийцыэгоцентрическиехарактерычтосвидетельствуетосуществованиитакихск
лонностейвеговнутреннеммиреатакжеиззанекоторыхфактовегожизнистрастиегоказартны
миграмможетбытьсексуальногорастлениянезрелойдевочкиисповедьэтопротиворечиеразре
шаетсяследующимобразомсильнаядеструктивнаяустремленностьдостоевскогокотораямог
лабыделатьегопреступникомбылавегожизнинаправленаглавнымобразомнасамогосебявов
нутрьвместотогочтобыизнутриитакимобразомвыразиласьвмазохизмеичувствевинывсетак
ивеголичностинемалоисадистическихчертвыявляющихсявегораздражительностимучитель
ственетерпимостидажепоотношениюклюбимымлюдяматакжевегоманереобращениясчитат
елемитаквмелочахонсадиствовневажномсадистпоотношениюксамомусебеследовательно
мазохистиэтомягчайшийдобродушнейшийвсегдаготовыйпомочьчеловеквсложнойличност
идостоевскогомывыделилитрифактораодинколичественныйидвакачественныхегочрезвыч
айноповышеннуюаффективностьегоустремленностькперверзиикотораядолжнабылаприве
стиегоксадомазохизмуилисделатьпреступникомиегонеподдающееясянализутворческоеда
рованиетакоесочетаниевполнемоглобысуществоватьибезневрозаведьбываютжестопроцен
тныемазохистыбезналичияневрозовпосоотношениюсилпритязаниипервичныхпозывовипр

отивоборствующихимторможенийприсоединяясюдавозможностисублимированиядостоев скоговсеещеможнобылобыотнестикразрядуимпульсивныххарактеровноположениевещейз атемняетсяналичиемневрозанеобязательногокакбылосказаноприданныхобстоятельствахн овсежевозникающеготемскореечемнасыщенneeосложнениеподлежащеесостороныческовеч ескогояпреодолениюневрозэтотолькознактогочтоятакойсинтезнеудалсячтооноприэтойпоп ыткепоплатилосьсвоимединствомвчемжевстрогомсмыслепроявляетсяневроздостоевскийн азывалсебясамидругиетакжесчиталиегоэпилептикомнатомоснованиичтоонбылподвержен тяжелымприпадкамсопровождавшимисяпотерейсознаниясудорогамиипоследующимупад очнымнастроениемвесьмавероятночтоэтатакназываемаяэпилепсиябылалишьсимптомомег оневрозакоторыйвтакомслучаеследуетопределитькакистероэпилепсиютоестькактяжелую истериюутверждатьэтосполнойуверенностьюнельзяподвумпричинамвопервыхпотомучто датыанамнезическихприпадковтакназываемойэпилепсиидостоевскогонедостаточныинена дежныавовторыхпотомучтопониманиесвязанныхсэпилептоиднымиприпадкамиболезненн ыхсостоянийостаетсянеясныма

ВИСНОВКИ

Під час виконання даної роботи було реалізовано підпрограми обчислення НСД та оберненого елемента за модулем за допомогою розширеного алгоритму Евкліда, а також алгоритм розв’язку лінійних порівнянь, які були потрібні для знаходження потенційних ключів (a, b).

Після знаходження та застосування для розшифрування тексту кандидатів (a, b), було отримано багато текстів-шумів, що потребувало побудови автоматичного розпізнавача змістовного тексту російською мовою. Розпізнавач використовує теоритичні значення відсотків літер «о», «а» та «е» у тексті в сукупності.