Міністерство освіти і науки України

Національний Технічний Університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

Фізико-технічний інститут

Криптографія

Комп'ютерний практикум №3

Виконали:
Студенти групи ФБ-81
Кіндерись Роман Андрійович
Аль Біні Ейман Собхийович

Перевірив:

Чорний О.М.

_____

Завдання

Мета роботи

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

Порядок виконання 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 їх усі.
2. За допомогою програми обчислення частот біграм, яка написана в ході виконання комп'ютерного практикуму №1, знайти 5 найчастіших біграм запропонованого шифртексту (за варіантом).
3. 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).

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

5. Повторювати дії 3-4 доти, доки дешифрований текст не буде змістовним.

Хід роботи

Опис: Ми використовували російський алфавіт, який склдався з 31 літери (без літер "ъ" та "ё")для розпізнавання російської мови була використана функція check_rus(), що приймає в якості вхідного параметру потенційно розшифрований, розпізнавання проходить в 2 етапи за 2 критеріями. Перший - перевірка частот частих літер, тобто щоб літера о була найбільш зустрічаємою. Другий - ентропійний критерій, якщо текст пройшов перший критерій перевіряється енропія тексту і якщо вона близька до ентропії мови текст вважається російським і відповідний ключ правильним.

Приклад виводу програми:

Літера о є найзустрічаємою однак ентропія тексту H = 4.813845825748601
знатно відрізняється від ентропії мови отриманої в ЛР№1 ~ 4.45
ключ що перевіряється: (241 ; 821)
У тексті літера о не є найчастішою
ключ що перевіряється: (389 ; 885)
У тексті літера о не є найчастішою
ключ що перевіряється: (445 ; 156)
У тексті літера о не є найчастішою
ключ що перевіряється: (731 ; 319)
У тексті літера о не є найчастішою
ключ що перевіряється: (11 ; 631)
У тексті літера о не є найчастішою
ключ що перевіряється: (159 ; 695)

Найпопулярніші біграми шифр тексту

Популярність	Код біграми	Біграма
1	509	Рн
2	860	Ыч
3	413	Нк
4	689	Цз
5	248	Иа

Шифротекст:

лквдвдьышкрбызякиабшачрнвязарчтчлчькзтманэмнязяыбштрпнхтрхрнзтжккысечамнмпывйвфяжтинфвйвйвсжнпчнмпгущзкыфвйв
утсюцзкыкынмотзщбйыыбшхолуычгкицепзкианьуыфллфтыраючькиащзтыфэнкйяпезтнкжккысечамнмпжэпаычйдбцвсшчмтшслаия
тасзбчжйьыбшывлтйэзщбцпцмпщрифкздтеэкктщзархрчосйпрйжклечаккяжюыщяоясфскчбяызрчйзчвгзжзычэявсшчтщлжочшыызюшх
ачрнтмнкуфйзбчечвпчнотмнктхеотичняцзбшрчычбчнкицгщлчькевочфыщяцзреотйсфтбйщялчдечамнмпйарчтчццзтьярняыхашхаыт
ыызdсепцяьаючшзбшзтжмсяачрнвязаозеарчэяицкятчрогцфэкыпээтйпчаэеэявахыдпдойдкрмпбцмвеэлжочрчщтецрнбяшкуэтыычлчо
кбцккузбнинепжвининачрнсджяццциаиятчщтецрнбяшквдиабцотияьацційвычфткюмпьяэяддаьччшызюсяуядсяжутрхбцшчрнфэтзткзт
цтеялчакиажчштзмнксябяешщтецрнбяшкуэчцеопнхоьяючбястзырзгьфлуфжмнкецььэтнкфячащжвжяымэвячатьияцзоеязднеэмэйкое
всщыяыяажвычцяучпяэязяшкинвдэякзюнзтмакырцсоушрнецчнкяуялжочознкьызащцнкяжсгмпчнвдепйдрчкеэярклнвцычпрычжкнп
щюрчньаччквсеокяяорнбччнйцнбшзикзчшклзпеепаопниашчеквдзеязэгцеккьызащцнкшчрнхкнчьхвсфэиащзинэяьяцзчцычжтмэывйв
щтецрнбяшктфбйыыемтщцзжеыытнщрпаозвзьнотпанхзайдкрмпбцсрпащцрущзлчшклееэхкжяццлтяыбчлуучвзпяэякящяцзэклтвсбця
ыыцлтбцдйрцецкзвзвычяквсойюшхxолуычннйвбнзеевсоцзпахышчгзючушчядкщрпаозмеяззябчмтмаэзуыйюфэхьбшркбцуэдйуфрня
ыннйвцяучрнкейпрцккутгщяжйухыксмпкырабцпабштхлтйвчябксогьракыбротхыачрнмнкршчуярачыбяцзрчфяяктфчнвдщтецрнбяш
кдфччжшюжачрнвязарчтчучнплзраюьтпнкшчюйзтвйпцдзтофтфэцтнкэофтчнщщккуфпяыцщряжеегщпцбцхкюзгзщырнэяччяыщзыэ
щрмпбцсрпарчтчбйхярняыжклжььцснкшчэяутпамзгьпнсевсэзфяцзоэцтнвеэззвьдчекеэгызнзтчнпнивучппжкнкэблыибшхязрнпыьар
чньччфьстланвеэиэмпрчвьмкеэйкогхчтыыззэивьяньзяфякщтыэзчягшяжпьсжфтщюызкдзтзщачзяюшкзйзлафпэойзьялчуцднеэнпейвя
зярнбйеплюдфызякиащзачрнвязаозеьхьрнфпечзэгмшчрнйахыбшнрчнмпмэхчйцбйвсчнмпмэьяючбяьярняыцеязочйсхкфпхотнртмэчз
кыквипйнктейесолйджкмэшчрзжйеспнмэйчяовытылуычмебцкяюцотноыкиащзфтногзаашятчфяжтгщтщвырчычбчтчжкрйупиажмыя
шкмнйврбфяесоркееэллцеиащзцяцзьзмзщяебтцфвебзозяньюжючьвзжчсгьтчэыучрнепйаозделнйааьцяцзэкйэфтйсрнецеопнхоинхыэ
врцсбчзмтманэмнязяыцзйсиаычицнввдбцкыьярнбяутсюцзкыфпцеэярнкецзкышчднжчюнйпозяыцзнкйсепькжчокбцпцмнйаэккчюжя
ычягшнвдфкгнкмяфтпаюьукфвецыогзбшучяпхкьюэинрцогэбфтпаюьтпнкэофяачщдвсеофтпаюьукфвмаолпаццнкяжьцсротвжуяддь
ыцзяквякяяоебхзлзмзгштышспаэтивщзексонвючшкиабшбйчзззсеобйлзиротщзфтйсучфжэвдфяпьзеебччцщяцзкодпшяюачйкщебччек
иабшфяяцмнкыбэкгхчтыгшшчкгнккршчтчиншчияцзывьяючбятьюьюаыыкьзаучйзтысюиебчщзечучючьквяднеэльачрнвязарчтчйдбй
еплюрбучэтийшчрнвцебтцузйджчутеэььсаучоччкиабшебхзбшфтногзйюрбхобятчйцотасбйбччяцегщечеойюрбмэипкйчнезучлчмыб
шхыздыяжкфэмпюжфтецжкнкецсспнезнащзбштыфтфэотучиншчияцзовйдзеотечамнклзйяебччекфвйкинвдщыечикфвжящцзебчочьв
еслеяздчюзюабйчыикфтшрчащяцзшсиаычицнввдевфтпаюьукфвйэинбящзещецпйзтжятчхбцяычлуычфтлзньхярнбяшкжкмафпзкфвч
ьхззгьутчняьнязьянвсяюыьытнотшрычйцсспнмпйаццеяычрьхярнечяыцзчнйвшхнвючшкиачяюцйдбцььэтнкфякэцтзыхынмлзещккм
винзтчхрытнбцйдгмтщцзрньырнсятчкывыгняжйзутйэлчцяцйцнйамврьйпзквдзтмаьпнкэофяйтмпдфыяечювузпебцйснуычфтинрцзтс
рсяьыйтсюжяюаяащявьфлфэбйьыичнафпзксоыярнгьтнрцтыяьрнэякпнкшчрнгсиаычицнввдевинзтсолчспейцаыячыбшйдзеэярнкецзр
чжйупецйдгмтщцзтыфтещцятыспецяжлчштзщеэтыиылчтчкяяоечеклнжшдэпаычычтчбнбйтзиклнязчнйвфэбйьыичжцхтзщфпмавце
ыичвззэлзбьзаццицхкпщкяхыюзбятчызякиащзфяеыюччажсчащзьянвшхьягнлжчцеофлшххобятчьыдсьышзчягшшчрнфэнрчнмпйаццн
кпнотсзлчрнссзмоежчыккюнкэбппкйфэуэебзоеыхынмицйдеэккотнчштплнкэотрчнмнмпмэчнйвдэмпкрнхжкиыюзрнечекицяыькеэи
ыюзрнучиншчияцзовиылчнькяуянпйсбцмнмпзкеэзщйхчащзднеэшдшызюфачштвснюфязюуфзайдщытчычлждееэкрлрмпбцмвзаюч
ькдфызякиащзачрнвязарчтчсжлжыяызызэтшийвычыывсхкрчызьярнбяшктфссяыкыьярнбяшкчхйдкрэягцшрифшчучлжияшкрбнитят
нрцшчрнгятчлаэтмэщяшкиабшсеотбяющузрчычьышсепькейуплеязбярнсятчтажсеэзщйхтщньфпчаыячыбшфтпаюьукфвеэсятчфяуч
ыссбхяпацытыызкьццзтьянввящыбчяыцзпнйввяочьяхыцзицучюкмэвдючюжрьхярнечяыбшрйкщфяжтгщецйсвйпцсбшмпаычфткгнк
ыкряеыичвзрнпйкщтыызэээкицбчичжеиажчыккюнкэбмзяеязговыцзцеотгзякчхучожечгзфтинрцбйзтрнзьфлшхфэычаэгмнкуффтчавя
юзаояалсецгщлчькиащзрьцпфэцтбцккэоачрнвязарчтчзайяхялчькбйупбйфчыкпащзстзщиовьфэхьгшмзекчхюыьытнотбцшчучючцяцз
ицтллфвычялкшяюаэкйпщрсялкицбчвыфябйщцмнмпзквдевйвюжючнвзщккзеязщцышкчхбйрнночягшрняыдкбцкяцяечикфвсбхятччя
нарчэясрмэтыфжхяшкйяиаючькнксяучяпкмплйяочрнзтжкшрмпбцсрпарчтчюеэявсепнкэбфяжтгщднинепжвгщтытнвдкрычянйвдфмз
ьнкщфяесйпхобнжчшчфтыуычдезецнмяучтпмнфпиайаечфэйсхкрнечжцьяимицрнбчтчнасжнпоебччцеопнхофяжтгщачрнвязаозгкзщ
пцйпкяяоиыйзбтедсяхынмпаэзхыызйдмусзщяхнфвеэтыычлчокбцккузбнжчуйупучьцотцяьнщммпуэфтцежскыназебчечцсецкзйзхоу
ччяэяеагщтыцзяаесзтвдйэузучнпйсрбчзньныачякуэтырнбчнксяжцпажэецотноыккрычднмнйвтыожяымэсогефпоемзчйупйпщюйафэ
хнеэеэйджкицбчвырчычзжюцхырчнааьшыпащявьпнзеэяыяызбшкыозрнотмусзщяхаэбычпабшкытнщммпрбчачяязсьццотцсмнныч
пеепшчеьбяэяшкиабшпкмпдщюевсзьмеязэзтыжцзеотлжееинеэнрычщывжккйэфяжзьянвшхфтцежсрчзнйвтыожяымэдфгефпоемзсси
аычицнввджкйсиахыычяктзфятыыякоыечзнзтчхучычньбнзежкфэкксяйцщщккяжжагефпоеычссяжйзфтцежскыйзччщяикнкяжжаиа
ычэкуфиахыпнхофяяаяжеы

Відкритий текст **КЛЮЧ (13, 151):**
многограннуюличностьдостоевскогоможнорассматриватьсчетырехсторонкакпис
ателякакневротикакакмыслителяэтикаикакгрешникакакжеразобратьсявэтойнев
ольносмущающейнассложностинаименееспоренонкакписательместоеговодном
рядусшекспиромбратьякарамазовывеличайшийроманизвсехкогдалибонаписан
ныхалегендаовеликоминквизитореодноизвысочайшихдостиженийимировойлите
ратурыпереоценитькотороеневозможноксожалениюпередпроблемойписательск
оготворчествапсихоанализдолженсложитьоружиедостоевскийскореевсегоуязви
мкакморалистпредставляяегочеловекомвысоконравственнымнатомоснованиич
тотолькототдостигаетвысшегонравственногосовершенствактопрошелчерезглуб
очайшиебездныгреховностимыигнорируемодносоображениеведьнравственным
являетсячеловекреагирующийуженавнутреннеиспытываемоеискушениеприэто
мемунеподдаваяськтожепопеременноготогрешитторазкаиваясьставитсебевысоки
енравственныецелитоголегкоупрекнутьвтомчтоонслишкомудобнодлясебястрои
тсвоюжизньоннеисполняетосновногопринципанравственностинеобходимостиот
речениявтовремякакнравственныйобразжизнивпрактическихинтересахвсегочел
овечестваэтимоннапоминаетварваровэпохипереселениянародовварваровубив
авшихизатемкаявшихсявэтомтакчтопокаяниестановилосьтехническимпримеро
мрасчищавшимпутькновымубийствамтакжепоступаливангрозныйэтасделкассов
естьюхарактернаярусскаячертадостаточнобесславениконечныйитогнравственн
ойборьбыдостоевскогопослеисступленнойборьбывоимяпримиренияпритязаний
первичныхпозывовиндивидастребованиямичеловеческогообществаонвынужде
ннорегрессируеткподчинениюмирскомуидуховномуавторитетукпоклонениюцар
юихристианскомубогукрусскомумелкодушномунационализмукчемуменеезначит
ельныеумыпришлисгораздоменьшимиусилиямичемонвэтомслабоеместобольш
ойличностидост

Висновки

В ході цієї лабораторної роботи ми набули навичок роботи із частотного аналізу. Також опанували прийоми роботи в модульній арифметиці,написали функції для обчислення оберненого елемента та розв’язання лінійних конгруенцій, закріпили знання роботи з відкритим та шифрованим текстом, які ми отримали при роботі над попередньою лабораторною роботою.