Міністерство освіти і науки України

Національний Технічний Університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

Фізико-технічний інститут

Криптографія

Комп'ютерний практикум №3

Варіант 1

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

Перевірив:

Чорний О.М.

_____

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 складався 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:

ключ що перевіряється: (47 ; 481)
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)
…
У тексті літера о не є найчастішою
Маємо ключ : (13 ; 151) є шуканим ключем
Увесь вивід знаходиться у файлі output.txt

Найпопулярніші біграми шифр тексту

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

Шифртекст:

лквдвдьышкрбызякиабшачрнвязарчтчлчькзтманэмнязяыбштрпнхтрхрнзтжккысечамнмпывйвфяжтинфвйвйвсжнпчн
мпгущзкыфвйвутсюцзкыкынмотзщбйьыбшхолуычгкицепзкианьуыфллфтыраючькиащзтыфэнкйяпезтнкжккысечамн
мпжэпаычйдбцвсшчмтшслаиятасзбчжйьыбшывлтйэзщбцпцмпщрифкздтеэкктщзархрчосйпрйжклечаккяжюыщяояфс
кчбяызрчйзчвгзжзычэявсшчтщлжочшызюшхачрнтмнкуфйзбчечвпчнотмнктхеотнчняцзбшрчычбчнкицгщлчькевочф
ыщяцзреотйсфтбйщялчдечамнмпйарчтчццзтьярняыхашхаытыыздсепцяьаючшзбшзтжмсяачрнвязаозеарчэяицкятчрог
цфэкыпэзтйпчаэеэявахыдпдойдкрмпбцмвеэлжочрчщтецрнбяшкуэтыычлчокбцккузбнинепжвининачрнсджяццаиятч
щтецрнбяшквдиабцотияьацційвычфткюмпьяэяддаьччшызюсяуядсяжутрхбцшчрнфэтзткзтцтеялчакиажчштзмнксябяе
шщтецрнбяшкуэчцеопнхоьяючбястзырзгьфлуфжмнкецььэтнкфячащжвжяымэвячатьияцзоезязднеэмэйкоевсщыяыяаж
вычцяучпяэязяшкинвдэякзюнзтмакырцсоушрнецчнкяуялжочознкьызаццнкяжсгмпчнвдепйдрчкеэярклнвцычпрычжк
нпщюрчньаччквсеокяяорнбччнйцнбшзикзчшклзпеепаопниашчеквдзеязэгцеккьызаццнкшчрнхкнчьхвсфэиащзинэяья
цзчцычжтмэывйвщтецрнбяшктфбйьыемтщцзжеьытнщрпаозвзьнотпанхзайдкрмпбцсрпаццрущзлчшклееэхкжяццлтя
ыбчлуучвзпяэякящяцзэклтвсбцяыыцлтбцдйрцецкзвзвычяквсойюшххолуычннйвбнзеевсоцзпахышчгзючушчядкщрпа
озмеяззябчмтмаэзуыйюфэхьбшркбцуэдйуфрняыннйвцяучрнкейпрцккутгщяжйухыксмпкырабцпабштхлтйвчябксогьр
акыбротхыачрнмнкршчуярачыбяцзрчфяяктфчнвдщтецрнбяшкдфччжшюжачрнвязарчтчучнплзраюьтпнкшчюйзтвйпц
дзтофтфэцтнкэофтчнщщккуфпяыцщряжеегщпцбцхкюзгзщырнэяччяыцзыэщрмпбцсрпарчтчбйхярняыжклжььцснкшч
эяутпамзгьпнсевсэзфяцзоэцтнвеэззвьдчекеэгызнзтчнпнивучппжкнкэблыибшхязрнпыьарчньччфьстланвеэиэмпрчвьм
кеэйкогхчтыыззэивьяньзяфякщтыэзчягшяжпьсжфтщюызкдзтзщачзяюшкзйзлафпэойзьялчуцднеэнпейвязярнбйеплюд
фызякиащзачрнвязаозеьхьрнфпечзэгмшчрнйахыбшнрчнмпмэхчйцбйвсчнмпмэьяючбяьярняыцеязочйсхкфпхотнртмэ
чзкыквипйнктейесолйджкмэшчрзжйеспнмэйчяовытылуычмебцкяюцотноыкиащзфтногзаашятчфяжтгщтщвырчычбчт

чжкрйупиажмыяшкмнйврбфяесоркееэллцеиащзцяцзьзмзщяебтцфвебзозяньюжючьвзжчсгьтчэыучрнепйаозделнйааь
цяцзэкйэфтйсрнецеопнхоинхыэврцсбчзмтманэмнязяыцзйсиаычицнввдбцкыьярнбяутсюцзкыфпцеэярнкецзкышчднж
чюнйпозяыцзнкйсепькжчокбцпцмнйаэккчюжяычягшнвдфкгнкмяфтпаюьукфвецыогзбшучяпхкьюэинрцогэбфтпаюьт
пнкэофяачщдвсеофтпаюьукфвмаолпаццнкяжьцсротвжуяддьыцзяквякяяоебхзлзмзгштышспаэтивщзексонвючшкиабш
бйчззсеобйлзиротщзфтйсучфжэвдфяпьзеебччцщяцзкодпшяюачйкщебччекиабшфяяцмнкыбэкгхчтыгшшчкгнккршчтч
иншчияцзывьяючбятьюьюаыыкьзаучйзтысюиебчщзечучючьквяднеэльачрнвязарчтчйдбйеплюрбучэтийшчрнвцебтцу
зйджчутеэььсаучоччкиабшебхзбшфтногзйюрбхобятчйцотасбйбччяцегщечеойюрбмэипкйчнезучлчмыбшхыздыяжкфэ
мпюжфтецжкнкецсспнезнащзбштыфтфэотучиншчияцзовйдзеотечамнклзйяебччекфвйкинвдщыечикфвжяццзебчочьв
еслеяздчюзюабйчыикфтщрчащяцзшсиаычицнввдевфтпаюьукфвйэинбящзещецпйзтжятчхбцяычлуычфтлзньхярнбяш
кжкмафпзкфвчьхззгьутчняьнязьянвсяюыьытнотшрычйцсспнмпйаццеяычрьхярнечяыцзчнйвшхнвючшкиачяюцйдбць
ьэтнкфякэцтзыхынмлзещккмвинзтчхрытнбцйдгмтщцзрньырнсятчкывыгняжйзутйэлчцяцйцнйамврьйпзквдзтмаьпнкэ
офяйтмпдфыяечювузпебцйснуычфтинрцзтсрсяьыйтсюжяюаяащявьфлфэбйьыичнафпзксоыярнгьтнрцтыяьрнэякпнкш
чрнгсиаычицнввдевинзтсолчспейцаыячыбшйдзеэярнкецзрчжйупецйдгмтщцзтыфтецщятыспецяжлчштзщеэтыиылчтч
кяяоечеклнжшдэпаычычтчбнбйтзиклнязчнйвфэбйьыичжцхтзщфпмавцеыичвззэлзбьзаццицхкпцкяхыозбятчызякиащз
фяеыюччажсчащзьянвшхьягнлжчцеофлшххобятчьыдсьышзчягшшчрнфэнрчнмпйаццнкпнотсзлчрнссзмоежчыккюнк
эбппкйфэуэебзоеыхынмицйдеэккотнчштплнкэотрчнмнмпмэчнйвдэмпкрнхжкиыюзрнечекицяыькеэиыюзрнучиншчи
яцзовиылчнькяуянпйсбцмнмпзкеэзщйхчащзднеэшдшызюуфачштвснюфязюуфзайдщытчычлждееэкрлрмпбцмвзаючь
кдфызякиащзачрнвязарчтчсжлжыяызызэтшийвычьывсхкрчызьярнбяшктфссяыкыьярнбяшкчхйдкрэягцшрифшчучлж
ияшкрбнитятнрцшчрнгятчлаэтмэщяшкиабшсеотбяющузрчычьышсепькейуплеязбярнсятчтажсеэзщйхтщньфпчаыячы
бшфтпаюьукфвеэсятчфяучыссбхяпацытыызкьццзтьянввящыбчяыцзпнйввяочьяхыцзицучюкмэвдючюжрьхярнечяыб
шрйкщфяжтгщецйсвйпцсбшмпаычфткгнкыкряеыичвзрнпйкщтыызээзкицбчичжеиажчыккюнкэбмзяеязговыцзцеотгз
якчхучожечгзфтинрцбйзтрнзьфлшхфэычаэгмнкуффтчавяюзаояалсецгщлчькиащзрьцпфэцтбцккэоачрнвязарчтчзайях
ялчькбйупбйфчыкпащзстзщиовьфэхьгшмзекчхюыьытнотбцшчучючцяцзицтллфвычялкшяюаэкйпщрсялкицбчвыфяб
йщщмнмпзквдевйвюжючнвзщккзеязщышкчхбйрнночягшрняыдкбцкяцяечикфвсбхятччянарчэясрмэтыфжхяшкйяиаю
чькнксяучяпкмплйяочрнзтжкшрмпбцсрпарчтчюеэявсепнкэбфяжтгщднинепжвгщтытнвдкрычянйвдфмзьнкщфяесйпх
обнжчшчфтыуычдезецнмяучтпмнфпиайаечфэйсхкрнечжцьяимицрнбчтчнасжнпоебччцеопнхофяжтгщачрнвязаозгкз
щпцйпкяяоиыйзбтедсяхынмпаэзхыызйдмусзщяхнфвеэтыычлчокбцккузбнжчуйупучьцотцяьнщммпуэфтцежскыназеб
чечцсецкзйзхоуччяэяеагщтыцзяаесзтвдйэузучнпйсрбчзньныачякуэтырнбчнксяжцпажэецотноыккрычднмнйвтыожяы
мэсогефпоемзчйупйпщюйафэхнеэеэйджкицбчвырчычзжюцхырчнааьшыпащявыпнзеяыяыязбшкыозрнотмусзщяхаэб
ычпабшкытнщммпрбчачяязсьццотцсмннуычпеепшчеьбяэяшкиабшпкмпдщюевсзьмеязэзтыжцзеотлжееинеэнрычщыв
жккйэфяжзьянвшхфтцежсрчзнйвтыожяымэдфгефпоемзссиаычицнвджкйсиахыычяктзфятыыякоыечзнзтчхучычньб
нзежкфэкксяйцщщккяжжагефпоеычссяжйзфтцежскыйзччщяикнкяжжаиаычэкуфиахыпнхофяяаяжеы

Відкритий текст КЛЮЧ (13, 151):

многограннуюличностьдостоевскогоможнорассматриватьсчетырехсторонкакписателякакневротикакакмыс
лителяэтикаикакгрешникакакжеразобратьсявэтойневольносмущающейнасложностинаименееспоренонка
кписательместоеговодномрядусшекспиромбратьякарамазовывеличайшийроманизвсехкогдалибонаписанн
ыхалегендаовеликоминквизитореодноизвысочайшихдостижениймировойлитературыпереоценитькотороен
евозможноксожалениюпередпроблемойписательскоготворчествапсихоанализдолженсложитьоружиедосто
евскийскореевсегоуязвимкакморалистпредставляяегочеловекомвысоконравственнымнатомоснованиичто
толькототдостигаетвысшегонравственногосовершенствактопрошелчерезглубочайшиебездныгреховности
мыигнорируемодносоображениеведьнравственнымявляетсячеловекреагирующийуженавнутреннеиспыты
ваемоеискушениеприэтомемунеподдаваяськтожепопеременнотогрешиттораскаиваясьставитсебевысокие
нравственныецелитоголегкоупрекнутьвтомчтоонслишкомудобнодлясебястроитсвоюжизньоннеисполняето
сновногопринципанравственностинеобходимостиотреченияотовремякакнравственныйобразжизнивпракти
ческихинтересахвсегочеловечестваэтимоннапоминаетварваровэпохипереселениянародовварваровубива
вшихизатемкаявшихсявэтомтакчтопокаяниестановилосьтехническимпримеромрасчищавшимпутькновыму
бийствамтакжепоступаливангрозныйэтасделкассовестьюхарактернаярусскаячертадостаточнобесславени
конечныйитогнравственнойборьбыдостоевскогопослеисступленнойборьбывоимяпримиренияпритязанийпе
рвичныхпозывовиндивидастребованиямичеловеческогообществаонвынужденнорегрессируеткподчинению
мирскомуидуховномуавторитетукпоклонениюцарюихристианскомубогукрусскомумелкодушномунационали
змукчемуменеезначительныеумыпришлисгораздоменьшимиусилиямичемонвэтомслабоеместобольшойли
чностидост

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.