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

ЛАБОРАТОРНА РОБОТА №3

З дисципліни «Криптографія»

«Криптоаналіз афінної біграмної підстановки»

Виконали:
студенти 3 курсу ФТІ
групи ФБ-73
Білоконь Богдан
Абкерімов Ервін

Перевірив:
Чорний О.
Завадська Л.О.
Савчук М.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) ,(b a 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:

1)Прочитали методичні вказівки до виконання лабораторної роботи

2)Написали програму для обчислення оберненого елемента за модулем з використанням розширеного алгоритму Евкліда

3) Знайшли 5 найчастіших біграм в своєму ШТ(1 варіант)

4) Написали програму для перебирання співставлення частих біграм мови та частих біграм ШТ, а також для обчислення а та б

5)Для кожного кандидата на ключ дешифруєм ШТ, перевіряючи його частоти букв, що повинні підходити середнім в мові

6) Розшифрували шифртекст за варіантом 1

Критерій відбору ключів:

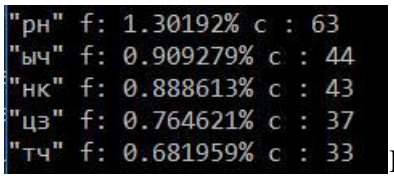
Проаналізувавши результати 1 лабораторної роботи, ми обрали для трьох найчастіших монограм ліміти частот. Тобто, якщо в розшифрованому тексті за допомогою деякої пари ключів частота якоїсь із літер менша за ліміт частоти цієї літери, то текст не пройшов перевірку і пара ключів не розглядається як шукана.

а - 0.055
е - 0.06
о - 0.085

Результати

Розшифрування тексту за варіантом 1:

Використавши основи модулярної арифметики, критерій відбору ключів та частотний аналіз, було знайдено таку пару ключів: a = 13, b = 151



Біграми шт

Біграми рос. мови: СТ, НО, ТО, НА, ЕН

Зашифрований текст

Вариант 1

лквдвдьышкрбызякиабшачрнвязарчтчлчькзтманэмнязяыбштрпнхтрхрнзтжккысечамнмпывйвфяжтинфвйвйвсжнпчнмпгу
щзкыфвйвутсюцзкыкынмотзщбйьыбшхолуычгкицепзкианьуыфллфтыраючькиащзтыфэнкйяпезтнкжккысечамнмпжэпаыч
йдбцвсшчмтшслаиятасзбчжйьыбшывлтйэзщбцпцмпщрифкздтеэкктщзархрчосйпрйжклечаккяжюыщяояфскчбяызрчйзчвг
зжзычэявсшчтщлжочшызюшхачрнтмнкуфйзбчечвпчнотмнктхеотнчняцзбшрчычбчнкицгщлчькевочфыщяцзреотйсфтбйщя
лчдечамнмпйарчтчццзтьярняыхашхаытыыздсепцяьаючшзбшзтжмсяачрнвязаозеарчэяицкятчрогцфэкыпээтйпчаэеэявахы
дпдойдкрмпбцмвеэлжочрчщтецрнбяшкуэтыычлчокбцккузбнинепжвининачрнсджяццаиятчщтецрнбяшквдиабцотияьац
цйвычфткюмпьяэяддаьччшызюсяуядсяжутрхбцшчрнфэтзткзтцтеялчакиажчштзмнксябяешщтецрнбяшкуэчцеопнхоьяючб
ястзырзгьфлуфжмнкецььэтнкфячащжвжяымэвячатьияцзоеязднеэмэйкоевсщыяыяажвычцяучпяэязяшкинвдэякзюнзтмак
ырцсоушрнецчнкяуялжочознкьызаццнкяжсгмпчнвдепйдрчкеэярклнвцычпрычжкнпщюрчньачччквсеокяяорнбччнйцнбшзи
кзчшклзпеепаопниашчеквдзеязэгцеккьызаццнкшчрнхкнчьхвсфэиащзинэяьяцзчцычжтмэыйвщтецрнбяшктфбйььемтщц
зжеьытнщрпаозвзьнотпанхзайдкрмпбцсрпаццрущзлчшклееэхкжяццлтяыбчлуучвзпяэякящяцзэклтвсбцяыыцлтбцдйрцец
кзвзвычяквсойюшххолуычннйвбнзеевсоцзпахышчгзючушчядкщрпаозмеяззябчмтмаэзуыйюфэхьбшркбцуэдйуфрняыннйв
цяучрнкейпрцккутгщяжйухыксмпкырабцпабштхлтйвчябксогьракыбротхыачрнмнкршчуярачыбяцзрчфяяктфчнвдщтецрнб
яшкдфччжшюжачрнвязарчтчучнплзраюьтпнкшчюйзтвйпцдзтофтфэцтнкэофтчнщцккуфпяыццщряжеегщпцбцхкюзгзщырнэ
яччяыцзыэщрмпбцсрпарчтчбйхярняыжклжььцснкшчэяутпамзгьпнсевсэзфяцзоэцтнвеэззвьдчекеэгызнзтчнпнивучппжкнк
эблыибшхязрнпыьарчньччфьстланвеэиэмпрчвьмкеэйкогхчтыыззэивьяньзяфякщтыэзчягшяжпьсжфтщюызкдзтзщачзяюшк
зйзлафпэойзьялчуцдneэнпейвязярнбйеплюдфызякиащзачрнвязаозеьхьрнфпечзэгмшчрнйахыбшнрчнмпмэхчйцбйвсчнм
пмэьяючбяьярняыцеязочйсххфпхотнртмэчзкыквипйнктейесолйджкмэшчрзжйеспнмэйчяовытылуычмебцкяюцотноыкиа
щзфтногзаашятчфяжтгщтщвырчычбчтчжкрйупиажмыяшкмнйврбфяесоркееэллцеиащзцяцзьзмзщяебтцфвебзозяньюжючч
ьвзжчсгьтчэыучрнепйаозделнйааьцяцзэкйэфтйсрнецеопнхоинхыэврцсбчзмтманэмнязяыцзйсиаычицнввдбцкыьярнбяутс
юцзкыфпцеэярнкецзкышчднжчюнйпозяыцзнкйсепькжчокбцпцмнйаэккчюжяычягшнвдфкгнкмяфтпаюьукфвецыогзбшучя
пхкььоэинрцогэбфтпаюьтпнкэофяачщдвсеофтпаюьукфвмаолпаццнкяжьцсротвжуяддьыцзяквякяяоебхзлзмзгштышспаэти
вщзексонвючшкиабшбйчззсеобйлзиротщзфтйсучфжэвдфяпьзеебччущяцзкодпшяюачйкщебччекиабшфяяцмнкыбэкгхчты
гшшчкгнккршчтчиншчияцзывьяючбятьюьюаьыкьзаучйзтысюиебчщзечучючьквяднеэльачрнвязарчтчйдбйеплюрбучэтийш
чрнвцебтцузйджчутеэььсаучоччкиабшебхзбшфтногзйюрбхобятчйцотасбйбччяцегщечеойюрбмэипкйчнезучлчмыбшхызд
ыяжкфэмпюжфтецжкнкецсспнезнащзбштыфтфэотучиншчияцзовйдзеотечамнклзйяебччекфвйкинвдщыечикфвжяццзебч
очьвеслеяздчюзюабйчыикфтщрчащяцзшсиаычицнввдевфтпаюьукфвйэинбящзещецпйзтжятчхбцяычлуычфтлзньхярнбяш
кжкмафпзкфвчьхззгьутчняьнязьянвсяюыььтнотшрычйцсспнмпйаццеяычрьхярнечяыцзчнйвшхнвючшкиачяюцйдбцььэтнк
фякэцтзыхынмлзещккмвинзтчхрытнбцйдгмтщцзрньырнсятчкывыгняжйзутйэлчцяцйцнйамврьйпзквдзтмаьпнкэофяйтмпд
фыяечювузпебцйснуычфтинрцзтсрсяьыйтсюжяюаяащявьфлфэбйьыичнафпзксоыярнгьтнрцтыяьрнэякпнкшчрнгсиаычицн
ввдевинзтсолчспейцаыячыбшйдзеэярнкецзрчжйупецйдгмтщцзтыфтецщятыспецяжлчштзщеэтыиылчтчкяяоечеклнжшдэп
аычычтчбнбйтзиклнязчнйвфэбйьыичжцхтзщфпмавцеыичвззэлзбьзаццицхкпцкяхыюзбятчызякиащзфяеыюччажсчащзьянв
шхьягнлжчцеофлшххобятчьыдсьышзчягшшчрнфэнрчнмпйаццнкпнотсзлчрнссзмоежчыккюнкэбппкйфэуэебзоеыхынмицй
деэккотнчштплнкэотрчнмнмпмэчнйвдэмпкрнхжкиыюзрнечекицяыькеэиыюзрнучиншчияцзовиылчнькяуянпйсбцмнмпзк
еэзщйхчащзднеэшдшызюуфачштвснюфязюуфзайдщытчычлждееэкрлрмпбцмвзаючькдфызякиащзачрнвязарчтчсжлжыя
ызызэтшийвычьывсхкрчызьярнбяшктфссяыкыьярнбяшкчхйдкрэягцшрифшчучлжияшкрбнитятнрцшчрнгятчлаэтмэщяшки
абшсеотбяющузрчычьышсепькейуплеязбярнсятчтажсеэзщйхтщньфпчаыячыбшфтпаюьукфвеэсятчфяучыссбхяпацытыызк
ьццзтьянввящыбчяыцзпнйввяочьяхыцзицучюкмэвдючюжрьхярнечяыбшрйкщфяжтгщецйсвйпцсбшмпаычфткгнкыкряеыи
чвзрнпйкщтыыызээкицбчичжеиажчыккюнкэбмзяеязговыцзцеотгзякчхучожечгзфтинрцбйзтрнзьфлшхфэычаэгмнкуффтчав
яюзаояалсецгщлчькиащзрьцпфэцтбцккэоачрнвязарчтчзайяхялчькбйупбйфчыкпащзстзщиовьфэхьгшмзекчхюыьытнотбцш
чучючцяцзицтллфвычялкшяюаэкйпщрсялкицбчвыфябйщщмнмпзквдевйвюжючнвзщккзеязщышкчхбйрнночягшрняыдкб
цкяцяечикфвсбхятччянарчэясрмэтыфжхяшкйяиаючькнксяучяпкмплйяочрнзтжкшрмпбцсрпарчтчюеэявсепнкэбфяжтгщдн
инепжвгщтытнвдкрычянйвдфмзьнкщфяесйпхобнжчшчфтыуычдезецнмяучтпмнфпиайаечфэйсхкрнечжцьяимицрнбчтчнас
жнпоебччцеопнхофяжтгщачрнвязаозгкзщпцйпкяяоиыйзбтедсяхынмпаэзхыызйдмусзщяхнфвеэтыычлчокбцккузбнжчуйуп
учьцотцяьнщммпуэфтцежскыназебчечцсецкзйзхоуччяэяеагщтыцзяаесзтвдйэузучнпйсрбчзньныачякуэтырнбчнксяжцпаж

эецотноыккрычднмнйвтыожяымэсогефпоемзчйупйпщюйафэхнеэеэйджкицбчвырчычзжюцхырчнааьшыпащявьпнзеэяыя
ызбшкыозрнотмусзщяхаэбычпабшкытнщммпрбчачяязсьццотцсмннуычпеепшчеьбяэяшкиабшпкмпдщюевсзьмеязэзтыжц
зеотлжееинеэнрычщывжккйэфяжзьянвшхфтцежсрчзнйвтыожяымэдфгефпоемзссиаычицнвджкйсиахыычяктзфятыыяьк
оыечзнзтчхучычньбнзежкфэкксяйцщщккяжжагефпоеычссяжйзфтцежскыйзччщяикнкяжжаиаычэкуфиахыпнхофяяаяжеы

Розшифрований текст

многограннуюличностьдостоевскогоможнорассматриватьсчетырехсторонкакписателякакневротикакакмыслителяэтикаи
какгрешникакакжеразобратьсявэтойневольносмущающейнассложностинаименееспоренонкакписательместоеговодномря
дусшекспиромбратьякарамазовывеличайшийроманизвсехкогдалибонаписанныхалегендаовеликоминквизитореодноизвы
сочайшихдостиженийиировойлитературыпереоценитькотороеневозможноксожалениюпередпроблемойписательскоготво
рчествапсихоанализдолженсложитьоружиедостоевскийскореевсегоуязвимкакморалистпредставляяегочеловекомвысокон
равственнымнатомоснованиичтотолькототдостигаетвысшегонравственногосовершенствактопрошелчерезглубочайшиебе
здныгреховностимыигнорируемодносоображениеведьнравственнымявляетсячеловекреагирующийуженавнутреннеиспыт
ываемоеискушениеприэтомемунеподдаваяськтожепопеременнотогрешитторазкаиваясьставитсебевысокиенравственные
целитоголегкоупрекнутьвтомчтоонслишкомудобнодлясебястроитсвоюжизньоннеисполняетосновногопринципанравстве
нностинеобходимостиотреченияавтовремякакнравственныйобразжизнивпрактическихинтересахвсегочеловечестваэтимон
напоминаетварваровэпохипереселениянародовварваровубивавшихизатемкаявшихсявэтомтакчтопокаяниестановилосьтех
ническимпримеромрасчищавшимпутькновымубийствамтакжепоступаливангрозныйэтасделкассовестьюхарактернаярусс
каячертадостаточнобесславениконечныйитогнравственнойборьбыдостоевскогопослеисступленнойборьбывоимяпримире
нияпритязанийпервичныхпозывовиндивидастребованиямичеловеческогообществаонвынужденнорегрессируеткподчине
ниюмирскомуидуховномуавторитетукпоклонениюцарюихристианскомубогукрусскомумелкодушномунационализмукче
муменеезначительныеумыпришлисгораздоменьшимиусилиямичемонвэтомслабоеместобольшойличностидостоевскийуп
устилвозможностьстатьучителемиосвободителемчеловечестваиприсоединилсяктюремщикамкультурабудущегонемноги
мбудетемуобязанавэтомповсейвероятностипроявилсяегоневрозиззакоторогоонибылосужденнатакуюнеудачупомощипос
тиженияисилелюбвиклюдямемубылоткрытдругойапостольскийпутьслужениянампредставляетсяотталкивающимрассмат
риваниедостоевскоговкачествегрешникаилипреступниканоэтоотталкиваниенедолжноосновыватьсянаобывательскойоцен
кепреступникавыявитьподлиннуюмотивациюпреступлениянедолгодляпреступникасущественныдвечертыбезграничноес
ебялюбиеисильнаядеструктивнаясклонностьобщимдляобеихчертипредпосылкойдляихпроявленийявляетсябезлюбовност
ьнехваткаэмоциональнооценочногоотношениякчеловекутутсразувспоминаешьпротивоположноеэтомуудостоевскогоегоб
ольшуюпотребностьвлюбвиегоогромнуюспособностьлюбитьпроявившуюсявегосверхдобротеипозволявшуюемулюбить
ипомогатьтамгдеонимелбыправоненавидетьимстительнапримерпоотношениюкегопервойженеиеелюбовникунотогдавозник
аетвопросоткудаприходитсоблазнпричисленияядостоевскогокпреступникамответиззавыбораегосюжетовэтопреимуществ
еннонасильникиубийцыэгоцентрическиехарактерычтосвидетельствуетосуществованиитакихсклонностейвеговнутренне
ммиреатакжеиззанекоторыхфактовегожизнистрастиегоказартнымигрампожетбытьсексуальногорастлениянезрелойдевоч
киисповедьэтопротиворечиеразрешаетсяследующимобразомсильнаядеструктивнаяустремленностьдостоевскогокоторая
моглабыделатьегопреступникомбылавегожизнинаправленаглавнымобразомнасамогосебявовнутрьвместотогочтобыизн
утриитакимобразомвыразиласьвмазохизмеичувствевинывсетакивеголичностинемалоисадистическихчертвыявляющихся
вегораздражительностимучительственетерпимостидажепоотношениюклюбимымлюдяматакжевегоманереобращениясчи
тателемитаквмелочахонсадиствовневажномсадистпоотношениюксамомусебеследовательномазохистиэтомягчайшийдоб
родушнейшийвсегдаготовыйпомочьчеловекусложнойличностидостоевскогомывыделилитрифактораодинколичественны
йидвакачественныхегочрезвычайноповышеннуюаффективностьегоустремленностькперверзиикоторыядолжнабылаприве
стиегоксадомазохизмуилисделатьпреступникомиегонеподдающееесянализутворческоедарованиетакоесочетаниевполнем
оглобысуществоватьибезневрозаведьбываютжестопроцентныемазохистыбезналичияневрозовпосоотношениюсилпритяза
ниипервичныхпозывовипротивоборствующихимторможенийприсоединяясюдавозможностисублимированиядостоевског
овсеещеможнобылобыотнестикразрядуимпульсивныххарактеровноположениевещейзатемняетсяналичиемневрозанеобяз
ательногокакбылосказаноприданныхобстоятельствахновсежевозникающеготемскореечемнасыщенненеосложнениеподле
жащеесосторонычеловеческогояпреодолениюневрозэтотолькознактогочтоятакойсинтезнеудалсячтооноприэтойпопытке
поплатилосьсвоимединствомвчемжевстрогомсмыслепроявляетсяневроздостоевскийназывалсебясамидругиетакжесчитал
иегоэпилептикомнатомоснованиичтоонбылподвержентяжелымприпадкамсопровождавшимисяпотерейсознаниясудорога
миипоследующимупадочнымнастроениемвесьмавероятночтоэтатакназываемаяэпилепсиябылалишьсимптомомегоневроз
акоторыйвтакомслучаеследуетопределитькакистероэпилепсиютоестькактяжелуюистериюутверждатьэтосполнойуверенн
остьюнельзяподвумпричинамвопервыхпотомучтодатыанамнезическихприпадковтакназываемойэпилепсиидостоевскогон
едостаточныиненадежныавовторыхпотомучтопониманиесвязанныхсэпилептоиднымиприпадкамиболезненныхсостояний
остаетсянеясныма

Код

```
#include <fstream>
#include <iostream>
#include <cstring>
#include <string>
#include "Header.h"

using namespace std;
```

```
int main()
{
	setlocale(LC_ALL, "Russian");
	ifstream in("E:\\02.txt");
	ofstream out("E:\\b3.txt");
	string text;

	int l[11000];

	/*string key = { "КРАСИВАЯМУЛЬТИВАРКАК" };

	int num[20];
	for (int i = 0; i < key.length(); i++)
	{
		num[i] = int(key[i]) + 64;

	}*/
	int obolon[12];
	int obolonka[12];
	/*obolon[0] = 478;
	obolonka[0]=*/

	/*for (int g = 0; g < 5; g++) {
		for (int g1 = g + 1; g1 < 5;g1++) {
			for (int h = 0; h < 5; h++){
				for (int h1 = h + 1; h1 < 5; h1++) {*/
					if (in.is_open())
					{
						while (getline(in, text))
						{
							/*int r=0;
							for (int i = 0; i < text.length(); i++)
							{
								r++;
							}
							cout<< r<<endl;*/
							for (int i = 0; i < text.length(); i += 2)
							{

								l[i / 2] = (((int(text[i]) + 32) * 31) + (int(text[i + 1]) +
32));



								//cout << y[i/2]%31<<endl;

								if (l[i / 2]%31>=26) {
								l[i / 2]++;
								}

								//cout << l[i / 2]<<endl;
							}

							for (int k = 0; k < text.length(); k += 2)
							{
								if (l[k / 2] % 31 >= 26) {
									l[k / 2]--;
								}
								int a, a1[10], b, j, n = 961, y, x, i = 2, r[10], q[10], X[10];
								a=13;
								b=151;

								b = l[k / 2] - b;

								if (b >= 0);
								else { b = n + b; }

								r[0] = n; a1[0] = 0;
								r[1] = a; a1[1] = 1;
```

```
while ((r[i - 1] != 1) & (r[i - 1] != 0));

r[i - 2]; n = n / r[i - 2]; a = r[i - 2]; i = 2;

r[i - 1]; i++; } while ((r[i - 1] != 1) & (r[i - 1] != 0));

a1[i - j - 3]; }

                                                        /*              }
                                                        }
                                                }
                                        }*/
                                }

                        }


                        return 0;
}
```

```
                        do { r[i] = r[i - 2] % r[i - 1]; q[i - 2] = r[i - 2] / r[i - 1]; i++; }


                        if (r[i - 1] == 1);
                        else if (b % r[i - 2] != 0) { cout << "error "; }
                        else {
                                r[0] = r[0] / r[i - 2]; r[1] = r[1] / r[i - 2]; b = b /

                                do { r[i] = r[i - 2] % r[i - 1]; q[i - 2] = r[i - 2] /

                        }

                        for (j = i - 3; j > -1; j--) { a1[i - j - 1] = a1[i - j - 2] * q[j] +


                        if (i % 2 == 0) { x = a1[i - 1] * b; x = x % n; }
                        else { x = a1[i - 1] * b; x = x % n; x = n - x; }
                        //cout << "a1=" << a1[i - 1] << " ";
                        //cout << "X=";
                        //cout << x;


                        text[k] = char(((x - (x % 31)) / 31) + 224);
                        text[k + 1] = char((x % 31) + 224);


                        cout << text[k] << text[k + 1];


        }

        if (mono(text) > 0.05) {
                        out << text;
                        cout << "ypa";
                        /*cout << obolon[g];
                        cout << obolon[h];*/
        }
```