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-81
Близнюк Микола та Мишкін Артем
Перевірили:
Чорний О.

Київ – 2020

Мета: 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.

Файл	Опис
encrypted.txt	Включає в себе зашифрований текст
main.py	Основний виконуваний файл
funcs.py	Файл з необхідними функціями

```
The alphabet we are using contains 31 characters:
['а', 'б', 'в', 'г', 'д', 'е', 'ж', 'з', 'и', 'й', 'к', 'л', 'м', 'н', 'о',
'п', 'р', 'с', 'т', 'у', 'ф', 'х', 'ц', 'ч', 'ш', 'щ', 'ь', 'ы', 'э', 'ю',
'я']
Indexed version:
{'а': 0, 'б': 1, 'в': 2, 'г': 3, 'д': 4, 'е': 5, 'ж': 6, 'з': 7, 'и': 8, 'й':
9, 'к': 10, 'л': 11, 'м': 12, 'н': 13, 'о': 14, 'п': 15, 'р': 16, 'с': 17,
'т': 18, 'у': 19, 'ф': 20, 'х': 21, 'ц': 22, 'ч': 23, 'ш': 24, 'щ': 25, 'ь':
26, 'ы': 27, 'э': 28, 'ю': 29, 'я': 30}

Most common russian bigrams: ['ст', 'но', 'ен', 'то', 'на']
```

```
Most common russian bigrams values: [545, 417, 168, 572, 403]

Most common encpypted bigrams appear rate: [0.019766034691407825,
0.018152480839048003]
Most common encrypted bigrams: ['йа', 'юа']
Most common encrypted bigrams values: [279, 899]

Impossible russian bigrams: ['аь', 'оь', 'еь', 'иь', 'уь', 'оь', 'щй', 'щф',
'щх', 'щц', 'щч', 'щш', 'щщ']
Impossible russian bigram values: [26, 460, 181, 274, 615, 460, 784, 795,
796, 797, 798, 799, 800]
```

Possible keys	(624, 502), (837, 589), (934, 6), (430, 335), (678, 707), (895, 552), (438, 223), (120, 831), (957, 645), (868, 279), (748, 688), (399, 769), (562, 409), (709, 273), (252, 905), (213, 490), (4, 533), (841, 347), (93, 899), (306, 149), (523, 955), (66, 626), (531, 843), (283, 471), (337, 676), (802, 893), (345, 564), (655, 68), (151, 397), (713, 279), (341, 310), (616, 614), (407, 657), (926, 118), (97, 192), (155, 31), (469, 750), (740, 800), (248, 279), (376, 130), (864, 25), (244, 56), (190, 812), (500, 316), (872, 874), (314, 37), (368, 242), (779, 254), (833, 459), (58, 738), (647, 180), (128, 719), (182, 924), (593, 936), (124, 589), (903, 440), (89, 304), (717, 161), (461, 862), (771, 366), (585, 87), (713, 899), (806, 186), (221, 378), (686, 595), (275, 583), (492, 428), (27, 211), (35, 99), (554, 521), (620, 868), (810, 781), (248, 899), (159, 285)

Приклад виводу програми:

```
KEY: (624, 502)
Impossible bigram found: щч

KEY: (837, 589)
Impossible bigram found: щц

KEY: (934, 6)
Impossible bigram found: щф

KEY: (430, 335)
Impossible bigram found: уь

KEY: (678, 707)
Impossible bigram found: уь
```

Шифротекст

рйрщкагппрфчгшрщйрпрффькрпьчшдвиыеюдучхулицплшющашдщныскющвпьюкджьйахещыйеьеюеэдсецчтыкйдшцчзю
имевжшбушччэканылшолшкющчшэизупмзсбвжшбуойщаищмдпнрйуюфшхдтылшларюдезанпрбкажлащваэщюемечшщипн
ипнучбусхекайаэкяуклзщюгхегарпинцплппрффзшскыушщммеючогалчцпдшяуыуйацднфзхащаукйнхжукчщысаэарю
жштнцмосхрхлтечшишваллмппртелиюдьпкуурдщерритыачтахщышкаюйзхцмздффнагещцлерьюбокцезацчучрйяыыу
нлсрорпрькрщэарючолаимхугшзепутэрщбероюазанхзушщимзсбючолаштэиэщюхжукчтдюагпшдормэрмыупьфуйабе
юемдвитылшошрщышгпфуыуйацдаювалляыачларщзщроюалахдорцпиыщылшошрщйьфуйазлиекдвифущлбшашваллюсхщ
рохеццэирщэаэшуоьюдэисфуриыугшэпзлиекдкглаедюднфэщйдшгфчпрбердрйуюпнсабдпннхцмрцсдрпющкммьлеешб
пымюенпчщроюабучштечшюдушлсбубеюыхрдщндщфщейерйсдкммьофкаюйажйаидхйьнхерщхлкшьсжуиеишбпымюенпч
щроюаеймюберояарпинымжизаропйхлбшбуклзщзсэпюаиечшорэпьчкгипгекбхщжачойатеащваюдюдкйчбйкпмтырй
юенщлучихечшчрпрфуклзщрусипнрйыуйаусйрпнцмшяхукчкйбвжшлжпшюечукемипнипцчушлсрйхпэснезщжмюдкенл
харпсдхйьчмэешйарпхппрэщцжыщпаюехдпьхуйанацчрбюдхушчкацкдщтеэдвиййтагшфичиорхлфдщфкшышвамносви
ййдзьрыщышхемсующудршджьюанхрэцпымздффнарписюахьхууочрфчгшйкпаюехдсджжгшцчтыкйдшнануэифуларизс
ййушфиюдюдаюышькющяпцлдчьншгашэлашьухаедвизлиекдвидщлсхпкеышйрьчценавсачэаькудбюяхцмрцсдрпгекм
мьлекдхйыуыщйаудюлцчисуюэиффриещжзьргшкдыууоьдглэшешбероюачпщылышщдшэасуйаьпымкуюсщгхелафитбюа
зуыщюаешуоналаолфдыууозмсдщьбукаощжзьрыщаыпмяызшхпбьйацчзюимпелумсрйюасавдыугшбрмэтдйкяуришпчи
оскчтхэейыосййричикзддрятаршроюазахачшфщчшурпрбуашькщепщчшфитдьчфщроюазацквснхтбьечшчыачешудкг
хавклаяхбмхашнэпосюеюазнтдщьбудшщепщчшфикайаэкишныцмбээелучылшрщашошзсбужифчмэйкблкмоснфэщкылш
рщхлиечшритээалаеймюберояарптылшцюцрчийщпаюеющчшхпэщхеишашйамущьбукаьээхцмустдмшыщдшцчсдхйыуыщ
йаудчикабпсаюезлиекдффыршдчимшлчлэфуюазздрятачшсающчшййнцусюаьжхезнмшйщгпридщнйымюдкебдкйющеш
хщнкшлнуюсэебдьебпщьюарпжиегтдлэфщюенщдезаламдосусжулапасйюдаюнежсщьйкэытэшсосгпэпщепщчшфихехщ
юедшэпеемучщройкэысарепуосхасасйленкссвссеоамдосвпхрзшмейрцлтедчусхеццкемчььсдмэшсрморушнллирм
ффаыпмяызшщфзсййымзсхажалафщнпбупюоьюдкеещхщшпщяавцквснхтбьечшджпшюешпщьбуказаэплахщдщнйдщтечш
джпшюешпщьбуэщшчсщряаюэщкацкышщехеаитбюарщлсцпэсеегпосщерпусдюйаюдбучихеэдэппртехарпеылегшмчху
хаяютечшюдуссайщсллдыууокайасазаопчичпнхбморешэшсающуонафщгшмейррихушкдщнйдщтечшщукайаэкышхемч
тэхевателуцчисхпкучызшцшмейряжпшюешпщьбудшоылшищгамуыщюаешлуьпппринхдщцадуришпчичифубелшмшмвкй
уыгшхлвпьюзсййушфиюдпелучырйнхюайажлэщцжйацчушугрйхпцчсдьчфщроюаепжьюдмшеемучщроюазацчаябуащыщ
дшварчмэчинкныцмйквыдщлагчмэашзщэиьчщщчшмейртвещжзьргшкдтваыпмяызшыыдщнпщьбукачэрщмечшлжйазакм
хйтвдебукчкйбвжшоыачлаоыьчмбюдпаюехдхввамнхукчкйбвжшгсйасандуссагшяснежсчикммьлезлиекдбюфшхдиы
рйгекбюдтдфчнцюдавлэкдусосйасадуклзщюдфчнцюдкемсуювпьюцкдщтечшэиащваейнцусюазблэчшгечофщгесаьп
юачпжжпшюечуаюгарпсенуказаэпюазшлууросйасажлешзлйаудрйхрмэцпфжйахеродюыщжрпроппрчикммьлевлщднх
бмнхшсзмгьхпэсрежаолфдыууофнрйнцусюазблэчшрщзщжацчтыкйкаешхакмхйтвжшусййушфиюдюдаюгпшгцчтыкйка
ющамджйазаддхухегарпцпбьюахщэдкгщыфутдаюащышэылшищяросчшмезахехщяпвсхйюдаюыущаидвцюдаюьичбзлцч
тыкйэщышты аччбзстдаюышхехаедюшзщрпщысагшлайеошцкнуфносачзюидцецчхйхажатечшжьйацчтыкйдшрщзщашчо
ыйыуйаусйрпнюлтевйвпрпгечпщачшкдььрмегфчпрбелшцающашчопаюебушщькышзшвыйафщышхпцмдрщыыуюехакчщу
иезафнщыаччбзстдаюрщлаеебдкйлщйачнрйюблэчшшхнфрпющэплщцчсдфмчзьчжлаыпмяызшжхбмнхшсбужичлщерпюа
буашькщыдщвйрмыулпбьйашдтыцмюарпхвцчьрдщгшашчоламчэичаэхшстдаюриэщйазнзсзшйшлшюагпчиеысагшлайе
зщайхлбшглэщйщчшчамеешвдбювсрэжичбзлэпрешхнфрплацсрчцпхюшрфчсимэоскгфуыйыхффэплщгарпсенуказарч
ыупмхуэсдммэтдяавдчишхтаичшзыйыуйаусйрпнушхакмюбпмншжлэщйщчшэирщлэгерпюабуосйещеэдсечушгцмпнщь
букаюдуыдщимюдкечушгмщрщашщппрэщкырйдщьлщеющвпьюриюдюашдйржахетсййвпэсгпчинаькгшхпннзщццтвкчис
жлзсйепртшййыуйаусйрпншдажйазмгьусффщлщрбезахемчтэлекмаюрщудеапамдосшсцпфжнлзуыщюазреызшэатдрм
хпщьбудшщыхубвчочпщаэщялчохехалюидвиаммсееапегкажлхехдпрчиилмечшшшцкдщтечшчызшэатдрмлэчлрщнаэш
эдкйчбйкишугрййкоыдднпрщышлсбубеаунккмнежскгцчтыкйкавйыуйаусйрпносфнзвюаиейркезаокйщгаынрйщызю
имюдаюаыпмяызшцлгпшгцчтыкйкаяхбмщырйнхкелиачгшшдсдмэшсрмфукукчщгчилиачгшзсечмбрмфуэснарпзючшпм
впфчбшмейрпныурщгпзхцмчэиорщэаэшшщрщхезакдььрмьрпнхщшдькюедефщроошкаюрпркдчэуырщлхчээпмеидбюха
хщимюдюарппьщсрплаэщкаюытэтедщпуэщвкющиулаэиыйхлллнажахоусиппрсеэщюхыййаькэиеыйееуйафмыущфзщжб
глщейеуозсащвашйымюдхунлищжанарпзючшбуосачиеэдщырйнхюахйщфрпешберояарущефпкезарчцптддчщфдщпуэщ
вкющньйашегахлтейицмрйыезаокнейежпэиэщгэхувлуоыуыщимфмйщпшйрщьйапахпьююаяофэхувлуолиачйахагаод
вимдчитысазшйыжжйажлчпнхыезахаэасачшашйарокамейецыьпяйхеейыуйаусйрнфйщхлюеерффасхйюдкемдсилэге
рпйклижуашрщщейечшвппршгцчтыкйканущефптачштэрщзщяпэптбьерпимюдкеслщещцримежагекаюрэпьчяфьеруюс
хпымздюлщелшашфьымосьрчифшцкщедеюакайасажлнктешщэилиачгшопьчффкммьофпаюечэрщошбеюеюылшищгаясбр
мэтдюадуклзщачисюарехеэдпрмэтдавнкхатешщашлиачгшдчьнчиипяыачжижуыщашащышгпридчьнрифусицлщеомхп
ипчушгмщрщашгшмейрсемьюдкеипгекбхщвпчпжжйаайхлзаейуюфщроошэщнхльюаэпеямщцевлэияффубелшщфцчтыкй
хрмсуювпьюыщдшварчмэчиащварщэщйщчшэийщхатешщчшбущефпсдюдисфуидчиеапячщ

Відкритий текст ***KEY: (27, 211)***

однакоэтакартинаскакойбыстороныемыеенирассматривалирасплываетсявнечтонеопределенноеприпадкипроя
вляющиесярезкосприкусываниемусиливающиесядоопасногодляжизниприводящегоктяжкомусамокалечениюмог
утвсежевнекоторыхслучаяхнедостигатьтакойсилыослабляясьдократкихсостоянийабсансадобыстропроходя
щихголовокруженийимогуттакжесменятьсякраткимипериодамикогдабольнойсовершаетчуждыеегоприродепос
тупкикакбынаходясьвовластибессознательногообуславливаясьвобщемкакбыстранноэтоиказалосьчистоте
лесныминричинамиэтисостоянияможетпервоначальновозникатьпопричинамчистодушевнымиспугилимогутвда
льнейшемнаходитьсявзависимостиотдушевныхволненийкакнихарактернодляогромногобольшинствасслучаеви
нтеллектуальноеснижениеноизвестенпокрайнеймереодинслучайкогдаэтотнедугненарушилвысшейинтеллект
уальнойдеятельностигельмгольцдругиеслучаивотношениикоторыхутверждалосьтожесамоененадежныилипод
лежатсомнениюкакислучайсамогодостоевскоголицастрадающиеэпилепсиеймогутпроизводитьвпечатлениету
постинедоразвитоститаккакэтаболезньчастосопряженасярковыраженнымидиотизмомикрупнейшимимозговым
идефектаминеявляяськонечнообязательнойсоставнойчастьюкартиныболезниноэтиприпадкисовсемисвоимив

идоизмененияимбываютиудругихлицулицсполнымдушевнымразвитиемискореесосверхобычнаявбольшинствесл
учаевнедостаточноуправляемойимиаффективностьюнеудивительночтопритакихобстоятельствахневозможно
установитьсовокупностьклиническоюаффектаэпилепсииточтопроявляетсяводнородностиуказанныхсимптом
овтребуетповидимомуфункциональногопониманиякакеслибымеханизманормальноговысвобожденияпервичных
позывовбылподготовленорганическимеханизмкоторыйиспользуетсяприналичиивесьмаразныхусловийкакпри
нарушениимозговойдеятельностипритяжкомзаболеваниитканейилитоксическомзаболеваниитакипринедоста
точномконтроледушевнойэкономиикризисномфункционированиидушевнойэнергиизаэтимразделениемнадвави
дамычувствуемндентичностьмеханизмалежащеговосновевысвобожденияпервичныхпозывовэтотмеханизмнеда
лекиотсексуальныхпроцессовпорождаемыхвсвоейосноветоксическиужедревнейшиеврачиназываликоитусмал
ойэпилепсиейивиделивполовомактесмягчениеиадаптациювысвобожденияэпилептическогоотводараздражени
яэпилептическаяреакциякаковымименемможноназватьвсеэтовместевзятоенесомненнотакжепоступаетиврас
поряжениеневрозасущностькотороговтомчтобыликвидироватьсоматическимассыраздраженияскоторыминевр
ознеможетсправитьсяпсихическиэпилептическийприпадокстановитсятакимобразомсимптомомистерииюад
аптируетсяивидоизменяетсяподобнотомукакэтопроисходитпринормальномтечениисексуальногопроцессата
кимобразоммысполнымправомразличаеморганическуюиаффективнуюэпилепсиюпрактическоезначениеэтогосл
едующеестрадающийпервойпораженболезньюмозгастрадающийвторойневротиквпервомслучаедушевнаяжизньп
одверженанарушениюизвневовторомслучаенарушениеявляетсявыражениемсамойдушевнойжизнивесьмавероят
ночтоэпилепсиядостоевскогоотноситсяковторомувидуточнодоказатьэтонельзятаккаквтакомслучаенужноб
ылобывключитьвцелокупностьегодушевнойжизниначалоприпадковипоследующиевидоизмененияэтихприпадко
вадляэтогоунаснедостаточноданныхописаниясамихприпадковничегонедаютсведенияосоотношенияхмеждупр
ипадкамиипереживанияминеполныичастопротиворечивывсеговероятнеепредположениечтоприпадкиначались
удостоевскогоужевдетствечтоонивначалехарактеризовалисьболееслабымисимптомамиитолькопослепотряс
шегоегопереживаниянавосемнадцатомгодужизниубийстваотцапринялиформуэпилепсиибылобывесьмауместно
еслибыоправдалосьточтоониполностьюпрекратилисьвовремяотбыванияимкаторгивсибириноэтомупротиворе
чатдругиеуказанияочевиднаясвязьмеждуотцеубийствомвбратьяхкарамазовыхисудьбойотцадостоевскогобр
осиласьвглазанеодномубиографудостоевскогоипослужилаимуказаниемнаизвестноесовременноепсихологич
ескоенаправлениепсихоанализтаккакподразумеваетсяименноонсклоненвидетьвэтомсобытиитягчайшуютрав
муивреакциидостоевскогонаэтоключевойпунктегоневрозаеслияначнуобосновыватьэтуустановкупсихоанал
итическиопасаюсьчтоокажусьнепонятнымдлявсехтехкомунезнакомыучениеивыраженияпсихоанализаунасоди
ннадежныйисходныйпунктнамизвестенсмыслпервыхприпадковдостоевскоговегоюношескиегодызадолгодопоя
вленияэпилепсииуэтихприпадковбылоподобиесмертионииназывалисьстрахомсмертиивыражалисьвсостояниил
етаргическогоснаэтаболезньнаходилананеговначалекогдаонбылещемальчикомкаквнезапнаябезотчетнаяпо
давленностьчувствокаконпозжерассказывалсвоемудругусоловьевутакоекакбудтобыемупредстоялосейчасж
еумеретьивсамомделенаступалосостояниесовершенноподобноедействительнойсмертиегобратандрейрасска
зывалчтофедоружевмолодыегодыпередтемкаказаснутьоставлялзаписькичтобоитсяночьюзаснутьсмертоподобн
ымсномипроситпоэтомучтобыегопохоронилитолькочерезпятьднейдостоевскийзарулеткойвведениеснамизве
стнысмыслинамерениетакихприпадковсмертониозначаютотождествлениесумершимчеловекомкоторыйдейств
ительноумерилисчеловекомживымещенокоторомумыжелаемсмертивторойслучайболеезначителенприпадоквук
азанномслучаеравноцененнаказаниюмыпожелалисмертидругомутеперьмысталисамиэтимдругимисамиумерлит
утпсихоаналитическоеучениеутверждаетчтоэтотдругойдлямальчикаобычноотецииименуемыйистериейприпад
окявляетсятакимобразомсамонаказаниемзапожеланиесмертиненавистномуотцуа

Висновки

В ході виконання лабораторної роботи на прикладі розкриття моноалфавітної підстановки ми набули навичок частотного аналізу та запрограмували деякі алгоритми модулярної арифметики.

Ми навчились дешифрувати текст отриманий в результаті шифрування за допомогою афінної підстановки біграм відкритого тексту; написали функції для обчислення оберненого елемента та розв’язання лінійних конгруенцій.