МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»

ФІЗИКО- ТЕХНІЧНИЙ ІНСТИТУТ

Кафедра інформаційної безпеки

Лабораторна робота №3

з дисципліни Криптографія

з теми:

«Криптоаналіз афінної біграмної підстановки»

Виконала:

Бородай Ю.

Групи ФБ-96

ВАРІАНТ 2

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.

1

розширений алгоритм Евкліда:

```
def gcd(a, b):
    if b == 0:
        return a, 1, 0
    else:
        d, x, y = gcd(b, a % b)
        return d, y, x - y * (a // b)
```

```
def countFun(a, b, n):
    result = []
    gcdOfAB = gcd(a, n)[0]
    if gcdOfAB == 1:
        result.append((gcd(a, n)[1] * b) % n)
        return result
    elif gcdOfAB > 1:
        if b % gcdOfAB == 0:
            x0 = countFun(a / gcdOfAB, b / gcdOfAB, n / gcdOfAB)[0]
            result.append(int(x0))
            for i in range(0, gcdOfAB - 1):
                x0 = x0 + n / gcdOfAB
                result.append(int(x0))
            return result
        else:
            result.append(0)
            return result
```

п’ять найчастіших біграм нашого шт тексту:

'йа', 'юа', 'чш', 'рп', 'юд'

п’ять найчастіших біграм російського тексту:

'ст', 'но', 'ен', 'то', 'на'

Ключ(27 211)

Шт:

рйрщкагпprфчгшрщйрпрффькрпьчшдвиыеюдучхулицплшющашдщныскющвпьюкджьйахещыйеье
юеэдсецчтыкйдшцчзюимевжшбушччэканылшолшкющчшэизупмзсбвжшбуойщаищмдпнрйуюфшх
дтылшларюдезанпрбкажлащваэщюемечшщипнипнучбусхекайаэкяуклзщюгхегарпинцплппрффзшс
кыушщммеючогалчцпдшяуыуйацднфзхащаукйнхжукчщысаэарюжштнцмосхрхлтечшишваллмппрт
елиюдьпкуурдщерритыачтахщышкаюйзхцмздффнагещцлерьюбокцезацчучрйяыыунлсрорпрькрщэ
арючолаимхугшзепутэрщбероюазанхзушщимзсбючолаштэиэщюхжукчтдюагпшдормэрмыупьфуйа
беюемдвитылшошрщышгпфуыуйацдаюваллйыачларщзщроюалахдорцпиыщылшошрщйьфуйазлие
кдвифущлбшашваллюсхщрохеццэирщэаэшуоьюдэисфуриыугшэпзлиекдкглаедюднфэщйдшгфчпрб
ердрйуюпнсабдпннхцмрцсдрпющкммьлеешбпымюенпчщроюабучштечшюдушлсбубеюыхрдщндщ

фщейерйсдкммьофкаюйажйаидхйьнхерщхлкшьсжуиеишбпымюенпчщроюаеймюбероюарпинымж
изаропйхлбшбуклзщзсэпюаиечшорэпьчкгипгекбхщжачойатеащваюдюдкйчбйкпмтырйюенщлучих
ечшчрпрфуклзщрусипнрйыуйаусйрпнцмшяхукчкйбвжшлжпшюечукемипнипцчушлсрйхпэснезщж
мюдкенлхарпсдхйьчмэешйарпхппрэщцжыщпаюехдпьхуйанацчрбюдхушчкацкдщтеэдвиййтагшфи
чиорхлфдщфкшышвамносвиййдзьрыщышхемсующудршджьюанхрэцпымздффнарписюахьхууочр
фчгшйкпаюехдсджжгшцчтыкйдшнануэифуларизсййушфиюдюдаюышькющяпцлдчьншгашэлашьу
хаедвизлиекдвидщлсхпкеышйрьчценавсачэаькудбюяхцмрцсдрпгекммьлекдхйыуыщйаудюлцчису
юэиффриещжзьргшкдыууоьдглэшешбероюачпщылшыщдшэасуйаьпымкуюсщгхелафитбюазуыщю
аешуоналаолфдыууозмсдщьбукаощжзьрыщаыпмяызшхпбьйацчзюимпелумсрйюасавдыугшбрмэтд
йкяуришпчиоскчтхэейыосййричикздрятарщроюазахачшфщчшурпрбуашькщепщчшфитдьчфщро
юазацквснхтбьечшчыачешудкгхавклаяхбмхашнэпосюеюазнтдщьбудшщепщчшфикайаэкишныцмб
ээелучылшрщашошзсбужифчмэйкблкмоснфэщкылшрщхлиечшритэзалаеймюбероюарптылшцюцр
чийщпаюеющчшхпэщхеишашйамущьбукаьэзхцмустдмшыщдшцчсдхйыуыщйаудчикабпсаюезлиек
дффыршдчимшлчлэфуюазздрятачшсающчшййнцусюаьжхезнмшйщгпридщнйымюдкебдкйющеш
хщнкшлнуюсэебдьебпщьюарпжиегтдлэфщюенщдезаламдосусжулапасйюдаюнежсщьйкэытэшсосг
пэпщепщчшфихехщюедшэпеемучщройкэысарепуосхасасйленкссвссеоамдосвпхрзшмейрцлтедчусх
еццкемчььсдмэшсрморушнллирмффаыпмяызшщфзсййымзсхажалафщнпбупюоьюдкеещхщшпщяа
вцквснхтбьечшджпшюешпщьбуказаэплахщдщнйдщтечшджпшюешпщьбуэщшчсщряаюэщкацкыш
щехеаитбюарщлсцпэсеегпосщерпусдюйаюдбучихеэдэппртехарпеылегшмчхухаяютечшюдуссайщс
ллдыууокайасазаопчичпнхбморешэшсающуонафщгшмейррихушкдщнйдщтечшщукайаэкышхемчт
эхевателуцчисхпкучызшцшмейряжпшюешпщьбудшоылшищгамуыщюаешлуьппрринхдщцадуриш
пчичифубелшмшмвкйуыгшхлвпьюзсййушфиюдпелучырйнхюайажлэщцжйацчушугрйхпцчсдьчфщ
роюаепжьюдмшеемучщроюазацчаябуащыщдшварчмэчинкныцмйквыдщлагчмэашзщэиьчщщчшме
йртвещжзьргшкдтваыпмяызшыыдщнпщьбукачэрщмечшлжйазакмхйтвдебукчкйбвжшоыачлаоыьч
мбюдпаюехдхввамнхукчкйбвжшгсйасандуссагшяснежсчикммьлезлиекдбюфшхдиырйгекбюдтдфч
нцюдавлэкдусосйасадуклзщюдфчнцюдкемсуювпьюцкдщтечшэиащваейнцусюазблэчшгечофщгеса
ьпюачпжжпшюечуаюгарпсенуказаэпюазшлууросйасажлешзлйаудрйхрмэцпфжйахеродюыщжрпро
ппрчикммьлевлщднхбмнхшсзмгьхпэсрежаолфдыууофнрйнцусюазблэчшрщзщжацчтыкйкаешхакм
хйтвжшусййушфиюдюдаюгпшгцчтыкйкающамджйазаддхухегарпцпбьюахщэдкгщыфутдаюащышэ
ылшищяросчшмезахехщяпвсхйюдаюыущаидвцюдаюьичбзлцчтыкйэщыштыаччбзстдаюышхехаед
юшзщрпщысагшлайеошцкнуфносачзюидцецчхйхажатечшжьйацчтыкйдшрщзщашчоыйыуйаусйрп
нюлтевйвпрпгечпщачшкдььрмегфчпрбелшцающашчопаюебушщькышзшвыйафщцышхпцмдрщыыу
юехакчщуиезафнщыаччбзстдаюрщлаеебдкйлщйачнрйюблэчшшхнфрпющэплщцчсдфмчзьчжлаып
мяызшжхбмнхшсбужичлщерпюабуашькщыдщвйрмыулпбьйашдтыцмюарпхвцчьрдщгшашчоламчэ
ичаэхшстдаюриэщйазнзсзшйшлшюагпчиеысагшлайезщайхлбшглэщйщчшчамеешвдбювсрэжичбзл
эпрешхнфрплацсрчцпхюшрфчсимэоскгфуыйыхффэплщгарпсенуказарчыупмхуэсдммэтдяавдчишх
таичшзыйыуйаусйрпнушхакмюбпмншжлэщйщчшэирщлэгерпюабуосйещеэдсечушгцмпнщьбукаю
дуыдщимюдкечушгмщрщашщппрэщкырйдщьлщеющвпьюриюдюашдйржахетсййвпэсгпчинаькгш
хпннзщццтвкчисжлзсйепртшййыуйаусйрпншдажйазмгьусффщлщрбезахемчтэлекмаюрщудеапамд
осшсцпфжнлзуыщюазреызшэатдрмхпщьбудшщыхубвчочпщаэщялчохехалюидвиаммсееапегкажлх
ехдпрчиилмечшшшцкдщтечшчызшэатдрмлэчлрщнаэшэдкйчбйкишугрййкоыдднпрщышлсбубеаун
ккмнежскгцчтыкйкавйыуйаусйрпносфнзвюаиейркезаокйщгаынрйщызюимюдаюаыпмяызшцлгпшг
цчтыкйкаяхбмщырйнхкелиачгшшдсдмэшсрмфукукчщгчилиачгшзсечмбрмфуэснарпзючшпмвпфчб
шмейрпныурщгпзхцмчэиорщэаэшшщрщхезакдььрмьрпнхщшдькюедефщроошкаюрпркдчэуырщлх
чээпмеидбюхахщимюдюарппьщсрплаэщкаюытэтедщпуэщвкющиулаэиыйхллланажахоусиппрсеэщ
юхыййаькэиеыйееуйафмыущфзщжбглщейеуозсащвашйымюдхунлищжанарпзючшбуосачиеэдщыр
йнхюахйщфрпешбероюарущефпкезарчцптддчщфдщпуэщвкющньйашегахлтейицмрйыезаокнейеж
пэиэщгэхувлуоыуыщимфмйщпшйрщьйапахпьююаяофэхувлуолиачйахагаодвимдчитысазшйыжжйа
жлчпнхыезахаэасачшашйарокамейецыьпяйхеейыуйаусйрнфйщхлюеерффасхйюдкемдсилэгерпйкл
ижуашрщщейечшвппршгцчтыкйканущефптачштэрщзщяпэптбьерпимюдкеслщещцримежагекаюрэ

пьчяфьеруюсхпымздюлщелшашфьымосьрчифшцкщедеюакайасажлнктешщэилиачгшопьчффкммь
офпаюечэрщошбеюеюылшищгаясбрмэтдюадуклзщачисюарехеэдпрмэтдавнкхатешщашлиачгшдчь
нчиипяыачжижуыщашащышгпридчьнрифусицлщеомхпипчушгмщрщашгшмейрсемьюдкеипгекбх
щвпчпжжйаайхлзаейуюфщроошэщнхльюаэпеямшщевлэияффубелшщфцчтыкйхрмсуювпьюыщдшв
арчмэчиащварщэщйщчшэийщхатешщчшбущефпсдюдисфуидчиеапячщ

часть вт:

однакоэтакартискойбысторонымыеенирассматривалирасплыетсявнечтонеопределенноеприпадкио
являющиесярезкусыниемусиливаюядоопасногляжизнводящегоктяжмусамокачеюмутвсежеврыхсл
учаяхдоигьтсиослабляяськрянийабнсобыстррохохголовокружейигуттятьсякткимериодамигдьнсов
ершаетчуждыееептупкикбессозтельноаябщкбаназальчисчииятпьпмчдушепугитвйшдитьвзавотыхл
нкнихрнмньшинслучвинтелуаоизвнпйнеймеайаэтнедугшилвйдеяьмцдржлоныжатсомюкйсамицеэп
ипсиеймитьвпетлпокэтабовыидзмпнзгефекявяськязйчоэютиудрцуцссвчнвбоуиаффюнеучтбсахожк
личюаэпочяеднукптебуеуфункцмахаяпзыылдгргьзхукптяжкзаксмзииэкизмфушйэздмычуехждрвхп
ывсецехвйоврачмягчациюяэеаммзяупрясущнвтхииэйпзомсеюапсхмтоцбрмпмргауююпажьюйвквй
жьэккнужнючегдлдкошхмыиудвдцамгубялифибауяотббитдмвьяхкьбглеографаиоазтзунвягцинкуов
кжуняхтыуеиоюлгырньмкябувлсвьдссжмдртлчфевмдткзчьюзбнзпьдввыйсчрлычецтц

['а', 'ш', 'е', 'щ', 'р', 'п']

['йа', 'юа', 'чш', 'юд', 'рщ']

можливий ключ: (27, 552)

індекс 0.03478340757073298

можливий ключ: (275, 924)

індекс 0.03339645734979892

можливий ключ: (306, 490)

індекс 0.0335683443429916

можливий ключ: (430, 676)

індекс 0.03320382537466919

можливий ключ: (461, 242)

індекс 0.03293117704063942

можливий ключ: (585, 428)

індекс 0.03385284695241397

можливий ключ: (678, 87)

індекс 0.03315344470425065

можливий ключ: (771, 707)

індекс 0.03322457035660624

можливий ключ: (802, 273)

індекс 0.03330162314665813

можливий ключ: (833, 800)

індекс 0.03338163950555817

можливий ключ: (864, 366)

індекс 0.03308231905189505

можливий ключ: (895, 893)

індекс 0.03339349378095077

можливий ключ: (926, 459)

індекс 0.03328680530241738

можливий ключ: (27, 211)

індекс 0.03856195785212384

можливий ключ: (151, 397)

індекс 0.033005266261843164

можливий ключ: (182, 924)

індекс 0.033171226117339546

можливий ключ: (275, 583)

індекс 0.033556490067599004

можливий ключ: (368, 242)

індекс 0.03331051385320258

можливий ключ: (399, 769)

індекс 0.03281559785556158

можливий ключ: (430, 335)

індекс 0.03348536441524341

можливий ключ: (678, 707)

індекс 0.032842269975194925

можливий ключ: (740, 800)

індекс 0.03308231905189505

можливий ключ: (895, 552)

індекс 0.03366021497728424

можливий ключ: (926, 118)

індекс 0.03343498374482487

можливий ключ: (89, 924)

індекс 0.03339942091864707

можливий ключ: (120, 490)

індекс 0.03321864321890994

можливий ключ: (182, 583)

індекс 0.03350907296602861

можливий ключ: (213, 149)

індекс 0.033076391914198755

можливий ключ: (306, 769)

індекс 0.03307046477650245

можливий ключ: (337, 335)

індекс 0.03378764843775468

можливий ключ: (368, 862)

індекс 0.033372748799013724

можливий ключ: (554, 180)

індекс 0.03334311311053222

можливий ключ: (616, 273)

індекс 0.03327198745817663

можливий ключ: (740, 459)

індекс 0.03368392352806944

можливий ключ: (833, 118)

індекс 0.033467583002154515

можливий ключ: (864, 645)

індекс 0.03322457035660624

можливий ключ: (926, 738)

індекс 0.033046756225717254

можливий ключ: (383, 780)

індекс 0.0331504811354025

можливий ключ: (590, 600)

індекс 0.03333422240398778

можливий ключ: (910, 656)

індекс 0.033630579288802746

можливий ключ: (507, 904)

індекс 0.033583162187232354

можливий ключ: (662, 656)

індекс 0.03355352649875085

можливий ключ: (461, 335)

індекс 0.033028974812628356

можливий ключ: (585, 645)

індекс 0.033443874451369315

можливий ключ: (678, 397)

індекс 0.03321864321890994

можливий ключ: (740, 552)

індекс 0.03352092724142121

можливий ключ: (864, 862)

індекс 0.03338756664325447

можливий ключ: (476, 594)

індекс 0.03368392352806944

можливий ключ: (693, 439)

індекс 0.03333422240398778

можливий ключ: (724, 5)

індекс 0.032821524993257876

можливий ключ: (900, 11)

індекс 0.03342312946943227

можливий ключ: (89, 211)

індекс 0.033257169613935884

можливий ключ: (213, 211)

індекс 0.03313566329116175

можливий ключ: (337, 211)

індекс 0.03349425512178786

можливий ключ: (368, 211)

індекс 0.03333125883513963

можливий ключ: (554, 211)

індекс 0.03281559785556158

можливий ключ: (709, 211)

індекс 0.033212716081213636

можливий ключ: (771, 211)

індекс 0.033832101970476924

можливий ключ: (957, 211)

індекс 0.03379653914429913

-.

ключ яким був розшифрован текст : (27, 211)

найпопулярніші літери в тексті : ['е', 'и', 'о', 'а', 'с', 'т']

індекс = 0.03856195785212384