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

КОМП’ЮТЕРНИЙ ПРАКТИКУМ №3
з дисципліни «Криптографія»

Виконав:

студент 3 курсу

НН ФТІ групи ФБ-25

Черняк Денис

Тема:«Криптоаналіз афінної біграмної підстановки»

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

Хід роботи:

Варіант-5

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.

```python
def euclidean_algorithm(a: int, b: int) -> Tuple[int, int, int]:
    if a == 0:
        return b, 0, 1
    gcd, x, y = euclidean_algorithm(b % a, a)
    return gcd, y - (b // a) * x, x


def mod_inverse(a: int, m: int) -> int:
    gcd, x, _ = euclidean_algorithm(a, m)
    if gcd != 1:
        raise ValueError("Обернене за модулем не існує")
    return (x % m + m) % m
```

```python
def congruence(a: int, b: int, m: int) -> List[int]:
    gcd, x0, _ = euclidean_algorithm(a, m)
    if b % gcd != 0:
        raise ValueError("Рівняння не має розв'язку")
    solutions = []
    x0 = (x0 * (b // gcd)) % m
    for i in range(gcd):
        solutions.append((x0 + i * (m // gcd)) % m)
    return solutions
```

2. За допомогою програми обчислення частот біграм, яка написана в ході виконання комп'ютерного практикуму No1, знайти 5 найчастіших біграм запропонованого шифртексту (за варіантом).

```
Топ-5 біграм: [('то', 51), ('но', 51), ('ен', 48), ('ст', 48), ('го', 43)]
```

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.

```python
def find_keys(ct: List[str], vt: List[str]) -> List[Tuple[int, int]]:
    keys = set()
    cipher_num = [bigram_to_number(bigram) for bigram in ct]
    plain_num = [bigram_to_number(bigram) for bigram in vt]
    for (y1, y2), (x1, x2) in product(product(cipher_num, repeat=2), product(plain_num, repeat=2)):
        if y1 == y2 or x1 == x2:
            continue
        delta_Y = (y1 - y2 + m2) % m2
        delta_X = (x1 - x2 + m2) % m2
        try:
            a_candidates = congruence(delta_X, delta_Y, m2)
            for a in a_candidates:
                b = (y1 - a * x1 + m2) % m2
                keys.add((a, b))
        except ValueError:
            continue
    return list(keys)
```

```python
for key in keys:
    try:
        decrypted_text = decrypt_text(ciphertext, key)
        if not has_forbidden_bigrams(decrypted_text, forbidden_bigrams):
            print(f"Ключ (a={key[0]}, b={key[1]}): {decrypted_text}")
            top_5 = top_bigrams(decrypted_text)
            print(f"Топ-5 біграм: {top_5}")
    except ValueError:
        continue
```

Значення ключа:

```
Ключ (a=654, b=777)
```

Шифротекст:

кеюибщаефдфмдкдкролрццисвнуншвйняэшскевдтнюдаобсюсыэихзтмдьлыохунхмьввнсдуэммндт
ихкеюибщыцязкзхшвносыотнйьщтцншуссянхщлвжвпькшвнмщзфтсхщпддкясввццтнавпьгнуьввйн
лхиьерддыцрихэкьзцэижцьехщмсэкжлрибуждэмхимьпьявсттнзцюсфспьузйпдкнхркхульацкчашяьн
сибжяксэкццзтчщиюцншумщошяьщкщнфрхуюижсгцыззфрщихзтчщрихнэпозтгфккчщкдмклыоьеы
нунййлцяьэрхнмкпмдкйыпоиэуныэнсмнмсхэццьедктництндуццоэивупхюфйчсьивйэютнрцшэбвщн
шуоздкдктнунянккфкяящиссбинкурдцбщшдскрщянщкдкяяищжшсвыьербщяяшндузйнкщнвнгоьцэ
ииспьтуумщщшдекхндуаошдвдеигебуявюсшьйдроццвнфиибжлакццввбвываккчслтьхщзйьцжьбрье
цфтспьбишиыовдьезбтнмсэкжллрчсхщьрпьшвшнйьяьнсибжлтьчсйрьэчтнундулфтснсшбйнбжжцр
нмющьккюиеуяэзтьяяреурндуьцоэгкмбобмщкскехюксдцтсывзтмсунйьксщиссшнчщзйьцйнпршькк
фкяслркейьйнавпьхсуншнузеумкжлаклцисуьдьбкфипьйнмсуншснхтуйнццмсяьмныонкцркчыоклзф
кчпьвныуозрбжлжвцнхщсссцжьбипсрзфкаьихмнщэчсавозулбутнзцнулцзткоццвнфиибхюпвиэислб
иювинхыршьивцнярбщфджлзйьцйнзцнулцяьйнвнцхркпрыожврщьянкиюджджкеспьибубиюхщбуаки
кяеэдакаоццсвлбеилрлвцофкяяышвнунхщлвэкжлтьосцнхщиютнуншнмстспьлйаихщрнньнхшвщшв
носчсабьешижсоэосыумщмбриввудябакфурщяэлчяздкаиьечслсосэкццяьцнэлязаьцнхщсссцжььзжл
мщунавшьавзтьяюсуйвнакдуюиььяучмпрфдййвдихрнфззфтнхщхиеуяэзтьяыуццыьбеелфеипвидий
дкяязщпупзобчсуьвнлвмьтнчщьеэдвнстйндуаомнщоццвнфиибхюихтоццсввныклрынпьювюсисцйв

нихчщлракющчьцнхщбщщйтннсхщдкищьешичщкздукчввзтьяакккйдищжлывьктзихывуллвовявшн
ьсйссцпрыоынчкццяьклхнщэюдриисэкжллреуньыктзшрэчшиязиебчлвацлотнуншнмстспьицшэмвш
щкзлоябсчбщшдыцэикзясусйнюйозвьтныэакосжцшншвюийдьяшншвосюсчязиьсунуллвихывхдскк
лмщубшскуаохщрнрцязакубсчфкяяосгйрщтнгбфдзйьцэибусчжвавмнззфдыоиюшсосюдритьйьнсхщ
тньцмнрнннстрсосуллвзтвднкцьяубщхичщмщтсчтгнэкхуямйдчщццмнрншвйнввлвацшвьхаврщшн
ищюиьсщожсюдгнуцрнчзшрынулцхдвмьцнрнуьнцяедьхсцнфуэюосйсчцэидктнуншнмншспьчшвн
юдцфвдыоияосунйпщнбкчзиввнмнрьнсибчзлориисэибудкяспнззжлфсчсбкаышнтныьзтпэпьмвзтьс
йядуцщщцспрчсэьлвзткбулцшвюибщыцвивнуйвнакеичмывпвыэдчфкклццсвынуняуумпьшвшрц
циссцмючщиюлврлиэйбдцриьцяьввюдаолыфьмодкчьяуфкойнкйдлцыцтнавчзфдыожяшсввдуюизб
ывщшвныэльидыщубшврчязрщвдойвнвнмщнсунцомюхщньюссттнхщщщфддбтьпнзкьеэдхнщьжвз
тфрлцдкяяхьовюсстхщрнпьйнщофкпрынсиулйдццхифсчсхдййрснсерццисшнюсшьсцклтьпвидрош
ифкяяшнюдаоосунчзфпьцэилцмяэьсцклжшвнунакубакюйтносшнпьявывйнщожсунюэсцэиринкгеэд
вэцнпдрщрнчстнввшвпвпьызмбйнвнцхпнуцязьсйядуулрибувдвнщозьгйбчйдсчбщиэбкдктнхщхилв
ннюсвнщокнирэчрниянцяеьцтсывзтосибфддбпмьлриввеэяьхэфртгрулцузбщшьавтулцибсчннисозф
дыожллрдцбщшдскрщиэбквэгвжвзтшвжьаоеитншнпвихэхаорщибясфсчсщьавпьскггыоющлхвиисп
ьвиулбутнзцнулцяьжцюсчвввйимюгвшнщиющюирсунлсгоьрыноьхоццвнфиибкзенуьпьбцрныгщйе
уйнзщшьявхщеуеидебупьесузюшдкясюэсцэиьцзттнмслдроавежбщяйрщйуюйлцеищьккффдкфьнхч
щмщявисчтжьамаофисрябсчшижслбубщэнщфдэмсщябубчзйсанэиршхщмсэктзлэусхщрнляпдгсгц
шфдкфьввнкубубяслоюищщшдекщсхдскхсовпннчубакакхуямдкяяхсвнхбжсмкщнщьжвэкссщьккдк
тнфифсбвбддкястнтнмслдьшсвьцйьшнсиеуюкыщцспрыьлнфкйдщщзйьцйныэвнхбрифкйыунрншьв
нбкубьебчсвйнжндуеисхавупмююсшодкльулбусчцнннстрсшншвьхаврщянсцознкссьеуснсмнмснси
бссвддцйнчсщнэпозцфибссщщубссвнхбрифкясхщфдцяьклрыоибсчфкщйвносэиэчпнзкццяьклакаол
ржцяьзтхдицфптнхщыглозфьцэидктнунэибунсхщавьвлващеутнищлрдцбщшдыцйнвнцхдздкицмяьх
авьщвуцфьцжьщнмкпмдкяярнэирщввпноулцфрынщхыщмснфжврйвньркзскыщссвнхбрифкясозййц
фцнюириьсосйгыовдриклакязеудкяяосузмщчявввнищрилвацшвьичдрщдкикгбмщбущстссвйьшвое
йулцгйщщфкнхдкбщщйвнихобсчшибщекбщэюнхзциссичщиютнмслдфишдмбццмсгцшвэрзфвджя
жвявшнмсчярщхьовюстымщкзищссыршьудццрреулфщщаефдхссироювяьисшщкзпксчролвтнрицн
мскмжяявзтсиюгщхтнмспбмщбущськмюннисдкдкцфжвйьдтмщшвпвкмжяьямщшвжьрефщакиеэда
кролфбклцбуябзщбукзунгэщькккгнввшнивжврщрныуоззнбкжлтьбцрныгйснжшдекцгеэюсрсхщньби
улбунхнчйдпнввкцйнуншвэьтнщоьцчсуьсцтгуьйнньосфипьявпьпршьйнлхавьщсиеуобмбмщбущсф
рмщчяовупмюосшнкуаохщмсэкццзтбыыьмнжннуыфрыэиьсфсчсщьавозщсосгйлцмктзулынйнуйаих
щавиэжьчщоуобмблвыьрнунокпмшрдцбщшддбубихйсансцрбжлвэкхюдрошджсюсунынмсйкмбкзх
щхурсунщхввввмдкорыуснчзьяуиюшсвпнкурмщеувирсунсццьблшэннбвамозмщбвскаьшнжьжвупк
лэчйдищьешиивебпрябакоьзтянщиссйебчввтсзкиющьккбыоскчицпьявицчзивяьочлцсвпдгсуфдкфь
яэюдаорибщвчрытнрсбидуаодункющхиьсхдгсунфрлцдкяяакдункчзжсюсбчкнбквьфзтнуноьюддкнх
живналбуыодкеиочоьлхэфдкфьпьлннсвнмкхсмщтсывзтьятнакфкпрябйожсюсунюиикцфтсввщбакк
сйнбжрисцвджцмнщькмыгьяьехщсяюсстхщрнхщбщыцвиклаккзеущнюсияоусчтсйьзткллрццюсстш
нюдкшвнгьерынньэьынавэкиютынннькиютноьакеишдщщшвпвмндтихжцшнйнюирсыэьяокпмаобщц
сэщбушсхщмсэкссьейпфкясищхнэкмбжлжвннстрсосщэтсяьяубщыцввяфжсюсунтсчтгвмьввьелвмк
рюеэзтдцццрнмюхщбуакдожсвнйсзвпьфихщчсяьзтьяйкчзфсчсгэлнцнерссжофкеиябпвистнпвюскио
сырынщэгожсгцмефдфмжяосзкццзтпытнрсакьлмщриарзфеуэирибщхиьсуйвнихвнстйнянцуфкщщц
сунхдицяедьакхуумжсвнчрлвньзтьяйкчзезьцюсжрыщумьцэиясезьцвнвнунищьеяцпьерынхщщщыц
виьянсибясшнлсиьпвтснфюирыюсцьаккнивжошижсмкарссжозщццесшндцнсккаирсыэокпмщнввйк
риаршьлнуьэиулбунхмокздцрнфзфпдкяспнчкхуцфюижсшщязюсшсиэжьввшвяэосрнеелоюисьфиос
эщублыунчяюэецчзивяьокхуямщщшдбофдгвмсжкддьяжьяущнввввшнмьвврщозенйсуньейпфкаьтн
ыоеущькхзцнулцзтднчелвпьгцбуавкмлыклтьяуаишдщщмюкеоубщыцвиакэмлхчярщтсчтрьйнвнцхм
ьакггмщшджсунлххэхьзтлрэчбудкввзнввшнжьжврщунынжвжрццисчцэиаьмчвврщищссркжэжвмнд
тфрлцяьклхнгцязвэкьзцэиьшсвмдьцюяусиебчдуьешдриезмщюиоуриесввхьовэкжятнмслдзылсрщйн
осыклрлврнввлэусхщрнавпьгбубсвйнавдьоспншсмкпрынкчмсхщнкойщщбщшдмефдфмжлрифсбвб
ддкяяыоввйнщцыгевввйьмэоьжйвнакеиэчпьидфккнйкрижэпншнхщынгспнунрнгошддкяяфсшьыоа
рфдрижлццэччсавпьзншвйнрнкизфтсиспьнкгбмщбущссцшнмьввьщянмсхмдктнянккбщшдекццжл
ывйквэпншнхщынгспныэрнгошддкйыявзтцнюфввовявлиьцяьокпмаишнмнээхфкччтхдицивьспьгсу
нмщпвюдцфюирыусунлрлцдкяяыуаокнввпьфзлцвнстбвхщщслэмдчзоулыфьтглозфьцэидкнхпрынк

чмстспьвифщгбрыяьцщжлзфпреурндцвныкмбарбуябакфккчявпвлсзврщьяшныйнмьунжкиюхщлв
хщпэжвчспьпрццсвпддктндклцнулцмклытсющшдекццзтиэярчсжвюсстибдцньтсюсстхщээрщьечщк
змщрнтслкеурьйомюхщньюсстгнулбуввзнтснфчзццзтвииярщьякбньависйщкзхщхуиюшннуяетнхщ
юиакфккчлспьыопьрцмнрншбынлсюдризьяуфкшдвчсксчавзтрщхсщв

Розшифрований текст:

убиватьбольшененадопослетогокаконужеубилнаследуетемубытьблагодарныминачепришлосьбыуб
иватьсамомуэтонеоднолишьдоброесостраданиеэтоотождествлениенаоснованииодинаковыхимпуль
совкубийствусобственноговорялишьвминимальнойстепенисмещенныйнарциссизмэтическаяценно
стьэтойдоброты этимнеоспаривается можетбытьэтовообщемеханизмнашегодоброгоучастияпоотно
шениюкдругомучеловекуособенноясноп роступающийвчрезвычайномслучаеобремененногосознан
иясвоейвиныписателянетсомнениячтоэтасимпатияпопричинеотождествлениярешительноопредели
лавыборматериаладостоевскогоносначалаонизэгоистическихпобужденийвыводилобыкновенногоп
реступникаполитическогоирелигиозногопреждечемкконцусвоейжизнивернутьсякпервопреступник
укотцеубийцеисделатьвеголицесвоепоэтическоепризнаниеопубликованиеегопосмертногонаследия
идневниковегоженыяркоосветилоодинэпизодегожизнитовремякогдадостоевскийвгерманиибылобу
реваемигорнойстрастьюдостоевскийзарулеткойявныйприпадокпатологическойстрастикоторыйнеп
оддаетсяинойоценкенискакойсторонынебылонедостаткавоправданияхэтогостранногоинедостойно
гоповедениячувствовинык акэтонередкобываетуневротиковнашлоконкретнуюзаменувобремененно
стидолгамиидостоевскиймоготговариватьсятемчтоонпривыигрышеполучилбывозможностьвернут
ьсяврос сиюизбежавзаключениявтюрьмукредитораминоэтобылтолькопредлогдостоевскийбылдоста
точнопроницателенчтобыэтопонятьидостаточночестенчтобывэтомпризнатьсяонзналчтоглавнымбы
лаиграсамапосебевсеподробностиегообусловленногопервичнымипозывамибезрассудногоповедени
яслужаттомудоказательствомиещекоечемуиномуоннеуспокаивалсяпоканетерялвсегоиграбыладлян
еготакжесредствомсамонаказаниянесчетноеколичествораздавалонмолодойженесловоиличестноесл
овобольшенеиграть илинеиграть вэтотденьионнарушалэтословокаконарассказываетпочтивсегдаесл
ионсвоимипроигрышамидоводилсебяиеедокрайнебедственногоположенияэтослужилодлянегоещео
днимпатологическимудовлетворениемонмогпереднеюпоноситьиунижатьсебяпроситьеепрезиратье
гораскаиватьсявтомчтоонавышлазамужзанегостарогогрешникаипослевсейэтойразгрузкисовестина
следующийденьиграначиналасьсноваимолодаяженапривыклакэтомуциклутаккакзаметилачтотоотч
еговдействительноститолькоиможнобылоожидатьспасенияписательствоникоганепродвигалосьвп
ередлучшечемпослепотеривсегоизакладыванияпоследнегоимуществасвязивсегоэтогоонаконечнон
епонималакогдаегочувствовиныбылоудовлетворенонаказаниямиккоторымонсамсебяприговорилто
гдаисчезалазатрудненностьвработетогдаонпозволялсебесделатьнесколькошаговнапутикуспехурасс
матриваярассказболеемолодогописателянетрудноугадатькакиедавнопозабытыедетскиепереживани
янаходятвыявлениявигорнойстрастиустефанацвейгапосвятившегомеждупрочимдостоевскомуодин
изсвоихочерковтримастеравсборникесмятениечувствестьновелладвадцатьчетыречасавжизниженщ
иныэтотмаленькийшедеврпоказываеткакбудтолишьтокакимбезответственнымсуществомявляется
женщинаинакакиеудивительныедлянеесамойзаконо нарушенияеетолкаетнеожиданноежизненноевп
ечатлениенонов еллаэтаеслиподвергнутьеепсихоаналитическомутолкованиюговоритоднакобезтако
йоправдывающейтенденциигораздобольшепоказываетсовсеминоеобщечеловеческоеилискореообщ
емужскоеитакоетолкованиестольявноподсказаночтонетвозможностиегонедопуститьдлясущностих
удожественноготворчествахарактерночтописательскоторымменясвязываютдружескиеотношенияв
ответнамоирасспросыутверждалчтоупомянутоетолкованиеемучуждоивовсеневходиловегонамерен
иянесмотрянаточтоврассказвплетенынекоторыедеталикакбырассчитанныенаточтобыуказыватьнат
айныйследвэтойновеллевеликосветскаяпожилаядамаповеряетписателюотомчтоейпришлосьпережи
тьболеедвадцатилеттомуназадраноовдовевшаяматьдвухсыновейкоторыевнейболеененуждалисьотк
азавшаясяоткакихбытонибылонадежднасороквторомгодужизнионапопадаетвовремяодногоизсвоих
бесцельныхпутешествийвигорныйзалмонакскогоказиногдесредивсехдиковинеевниманиеприковыв
аютдверукикоторыеспотрясающейнепосредственностьюисилойотражаютвсепереживаемыенесчаст
нымигрокомчувстварукиэтирукикрасивогоюношиписателькакбыбезовсякогоумысладелаетегорове
сникомстаршегосынанаблюдающейзаигройженщиныпотерявшеговсеивглубочайшемотчаяниипоки
дающегозалчтобывпаркепокончитьсосвоеюбезнадежнойжизньюнеизяснимаясимпатиязаставляетж

енщинуследоватьзаюношейвпредпринятьвседляегоспасенияонпринимаетеезаоднуизмногочисленн ыхвтомгороденавязчивыхженщинихочетотнееотделатьсяноонанепокидаетегоивынужденавконцеко нцоввсилусложившихсяобстоятельствостатьсявегономереотеляиразделитьегопостельпослеэтойим провизированнойлюбовнойночионавелитказалосьбыуспокоившемусяюношедатьейторжественноео бещаниечтоонникогдабольшенебудетиграться снабжаетегоденьгаминаобратныйпутьисосвоейсторон ыдаетобещаниевстретитьсяснимпередуходомпоезданавокзаленозатемвнейпробуждаетсябольшаяне жностькюношеонаготовапожертвоватьвсемчтобытолькосохранитьегодлясебяионарешаетотправит ьсяснимвместевпутешествиевместотогочтобыснимпроститьсявсяческиепомехизадерживаютееиона опаздываетнапоездвтоскепоисчезнувшемуюношеонасноваприходитвигорныйдомисвозмущениемо бнаруживаеттамтежерукинакануневозбудившиевнейтакуюгорячуюсимпатиюнарушительдолгавер нулсякигреонанапоминаетемуобегообещаниинооде ржимыйстрастьюонбранитсорвавшуюегоигрув елитейубиратьсявонишвыряетденьгикоторымионахотелаеговыкупитьопозореннаяонапокидаетгоро давпоследствииузнаетчтоейнеудалосьспастиегоотсамоубийстваэтаблестящеибезпробеловвмотиви ровкенаписаннаяновеллаимеетконечноправонасуществованиекактаковаяинеможетнепроизвестина читателябольшоговпечатленияоднакопсихоанализучитчтоонавозникланаосновеумопостроя емогов ожденияпериодаполовогосозреванияокаковомвожденииинекоторыевспоминаютсовершенносоз нательносогласноумопостроя емомувожделениюматьдолжнасамаввестиюношувполовуюжизньдляс пасенияегоотзаслуживающегоопасениявредаонанизмастольчастыесублимирующиехудожественны епроизведениявытекаютизтогожепервоисточникапороконанизмазамещаетсяпорокомигорнойстрас тиударениепоставленноенастрастнуюдеятельностьрукпредательскисвидетельствуетобэтомотводеэ нергиидействительноигорнаяодержимостьявляетсяэквивалентомстаройпотребностивонанизменио днимсловомкромесловаигранельзяназватьетееаа

Висновок:
У ході виконання комп'ютерного практикуму я реалізував програму,яка за допомогою частотного аналізу розшифровує моноалфавітні підстановки.

Також реалізував підпрограми для виконання математичних операцій:1.Обчислення оберненого елемента за модулем за допомогою розширеного алгоритму Евкліда.2.Розв'язання лінійних порівнянь з коректним врахуванням випадків з кількома розв'язками.

Використав частотний аналіз для визначення 5 найчастіших біграм у шифротексті. Провів співставлення найчастіших біграм шифротексту з найчастішими біграмами відкритого тексту. Для таких співставлень знаходив можливі значення ключа.Для кожного “кандидата“ на ключ дешифрував текст і перевіряв його змістовність.У результаті правильним ключем виявився (a=654, b=777).За допомогою цього ключа я успішно розшифрував текст.