МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ

імені Ігоря Сікорського»

«ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ»

КРИПТОГРАФІЯ

Комп'ютерний практикум №3

Виконали

студенти 3-го курсу групи ФБ-22

Лаптєв Д. М. та Проскурня А. С.

Бригада №5

Перевірив/-ла: _____ _____

Київ 2025

Мета

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

Порядок виконання роботи

1. Уважно прочитати методичні вказівки до виконання комп'ютерного практикуму.
2. 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.
3. За допомогою програми обчислення частот біграм, яка написана в ході виконання комп'ютерного практикуму №1, знайти 5 найчастіших біграм запропонованого шифртексту (за варіантом).
4. 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).
5. Для кожного кандидата на ключ дешифрувати шифртекст. Якщо шифртекст не є змістовним текстом російською мовою, відкинути цього кандидата.
6. Повторювати дії 4-5 доти, доки дешифрований текст не буде змістовним.

Хід роботи

Напишемо підпрограму із завдання із розширеним алгоритмом Евкліда (нижче приклад роботи, програма у файлі gcd_extended.py):

```
НСД(3, 11) = 1, x = 4, y = -1
Обернений елемент 3 за модулем 11 = 4
Розв'язок рівняння 3x ≡ 1 (mod 11) = 4
```

За допомогою програми із комп'ютерного практикуму №1, аналізуємо наш текст і знаходимо top5 найчастіших біграм (файл top5_bi.py), у нашому випадку це

```
Top 5 bigrams in bi_freq_matrix.csv:
вн: 0.0174717368961973
тн: 0.0174717368961973
дк: 0.0164439876670092
хщ: 0.0164439876670092
ун: 0.0147310722850291
```

Далі переходимо до основного коду:

- реалізували обчислення із використанням розширеного алгоритму Евкліда (використовуючи gcd_extended.py);
- зіставляємо 5 частих біграм мови із 5 біграмами вище на скріншоті, і для кожного із варіантів підбираємо ключі

Генерація ключів відбувається наступним чином: створюються модливі пари біграм із ВТ та ШТ, кожна із біграм переводиться у числове значення, для кожної пари обчислюється різниця числових представлень
($X = (X1 – X2) \bmod 31^2$, $Y = (Y1 – Y2) \bmod 31^2$),
звідки уже шукаються імовірні значення a ($a = X^{-1}*Y \bmod 31^2$) та
b ($b = Y1 - a*X1 \bmod 31^2$) нашого ключа.

- дешифруємо тексти;

Серед дешифрованих текстів знаходимо осмислений за допомогою автоматичного розпізнавача російської мови. Для цього обрали метод аналізу частот частими літерами “о” та “а” (“е” у перевірку не беремо, бо літера “ё” була замінена і через це частота літери у тексті буде неправильною і не збігатиметься із очікуваною).
Частоти узяті із 1 комп’ютерного практикуму:

o	0.11451417299670041405
e	0.08586975616053911520
a	0.07975525045345546737

- Вивід - дешифрований осмислений текст та відповідні ключі, якими його дешифрували.

Труднощі:

При використанні звичайного порядку у алфавіті, коли “ь” іде після “ы” ми мали невеличкі шуми у тексті, хоча читалося, що це уже осмислений текст, який ми шукали:

```
Розшифрований текст: убиватыболышененадопослетогокаконужеубилноследу етецубьтыблхгщдарньйюначепришлосыбьубиватесамо
```

А от коли ми поміняли ці літери у заданому алфавіті місцями, текст став повністю читабельним:

```
Розшифрований текст: убиватьбольшененадопослетогокаконужеубилноследу етемубытьблагодарныминачепришлосьбыубиватьсамомуэтонеод
```

Шифротекст:

кеюибщаефдфмдкдкролрццисвнуншвйняэшскевдтнюдаобсюсыэихзтмдьлыохунхмьввнс
дуэммндтихкеюибщыцязкзхшвнос
ыотнйьщтцншуссянхщлвжвпькшвнмщзфтсхщпддкясввццтнавпьгнуьввйнлхиьерддыцр
ихэкьзцэижцьехщмсэкжлрибуждэм
химьпьявсттнзцюсфспьузйпдкнхркхульацкчашяьнсибжяксэкццзтчщиюцншумщошяьщ
кщнфрхуюижсгцыззфрщихзтчщрихн
эпозтгфккчщкдмклыоьеынунййлцяьэрхнмкпмдкйыпоиэуныэнсмнмсхэццьедктництнду
ццоэивупхюфйчсьивйэютнрцшэбв
щншуоздкдктнунянккфкяящиссбинкурдцбщшдскрщянщкдкяяищжшсвыьербщяяшндуз
йнкщнвнгоьцэииспьтуумщщшдекхнду

аошдвдеигебуявюсшьйдроццвнфиибжлакццввбвываккчслтьхщзйьцжьбрьецфтспьбиши
ыовдьезбтнмсэкжллрчсхщьрпьшв
шнйьяьнсибжлтьчсйьрьэчтнундулфтснсшбйнбжжцрнмющькккюиеуяэзтьяяреурндуьцоэг
кмбобмщкскехюксдцтсывзтмсун
йьксщиссшнчщзйьцйнпршьккфкяслркейьйнавпьхсуншнузеумкжлаклцисуьдьбкфипьйн
мсуншснхтуйнццмсяьмныонкцркч
ыоклзфкчпьвныуозрбжлжвцнхщсссцжьбипсрзфкаьихмнщэчсавозулбутнзцнулцзткоццв
нфиибхюпвиэислбиювинхыршьив
цнярбщфджлзйьцйнзцнулцяьйнвнцхркпрыожврщьянкиюджджкеспьибубиюхщбуакикяеэ
дакаоццсвлбеилрлвцофкяяышвнун
хщлвэкжлтьосцнхщиютнуншнмстспьлйаихщрнньнхшвщшвносчсабьешижсоэосыумщм
бриввудябакфурщяэлчяздкаиьечслс
осэкццяьцнэлязаьцнхщсссцжььзжлмщунавшьавзтьяюсуйвнакдуюиььяучмпрфдййвдихр
нфззфтнхщхиеуяэзтьяыуццыьбь
еелфеипвидийдкяязщпупзобчсуьвнлвмьтнчщьеэдвнстйндуаомнщоццвнфиибхюихтоццс
ввныклрынпьювюсисцйвнихчщлр
акющчьцнхщбщщйтннсхщдкищьешичщкздукчввзтьяакккйдищжлывьктзихывуллвовяв
шньсйссцпрыоынчкццяьклхнщэюдри
исэкжллреуньыктзшрэчшиязиебчлвацлотнуншнмстспьицшэмвшщкзлоябсчбщшдыцэик
зясусйнюйозвьтныэакосжцшншвюи
йдьяшншвосюсчязиьсунуллвихывхдсккламщубшскуаохщрнрцязакубсчфкяяосгйрщтнгб
фдзйьцэибусчжвавмнззфдыоиюшс
осюдритьйьнсхщтньцмнрнннстрсосуллвзтвднкцьяубщхичщмщтсчтгнэкхуямйдчщццмн
рншвйнввлвацшвьхаврщшнищюиьс
щожсюдгнуцрнчзшрынулцхдвмьцнрнуьнцяедьхсцнфуэюосйсчцэидктнуншнмншспьчшв
нюдцфвдыоияосунйпщнбкчзиввнмн
рьнсибчзлориисэибудкяспнззжлфсчсбкаышнтныьзтпэпьмвзтьсйядуццщщцспрчсэьлвзтк
лбулцшвюибщыцвивнуйвнакеи
чмывпвыэдчфкклццсвынуняуумпьшвшрцциссцмючщиюлврлиэйбдцриьцяьввюдаолыфь
модкчьяуфкойнкйдлцыцтнавчзфдыо
жяшсввдуюизбывщшвныэльидыщубшврчязрщвдойвнвнмщнсунцомюхщньюсстгнхщщ
щфддбтьпнзкьеэдхнщьжвзтфрлцдкяяхь
овюсстхщрнпьйнщофкпрынсиулйдццхифсчсхдййрснсерццисшнюсшьсцклтьпвидроши
фкяяшнюдаоосунчзфпьцэилцмяэьсц
клжшвнунакубакюйтносшнпьявывйнщожсунюэсцэиринкгеэдвэцнпдрщрнчстнввшвпвп
ьызмбйнвнцхпнуцязьсйядуулрибу
вдвнщозьгйбчйдсчбщиэбкдктнхщхилвннюсвнщокнирэчрниянцяеьцтсывзтосибфддбпм
ьлриввеэяьхэфртгрулцузбщшьав
тулцибсчннисозфдыожллрдцбщшдскрщиэбквэгвжвзтшвжьаоеитншнпвихэхаорщибясфс
чсщьавпьскггыоющлхвииспьвиул
бутнзцнулцяьжцюсчвввйимюгвшнщиющюирсунлсгоьрыноьхоццвнфиибкзенуьпьбцрны
гщйеуйнзщшьявхщеуеидебупьесуз
ющдкясюэсцэиьцзттнмслдроавежбщяйрщйуюйлцеищьккффдкфьнхчщмщявисчтжьамао
фисрябсчшижслбубщэнщфдэмсщябуб

чзйсанэирщхщмсэктзлэусхщрнляпдгсгцшфдкфьввнкубубяслоюищщшдекщсхдскхсовпн
нчубакакхуямдкяяхсвнхбжсмкщн
щьжвэкссщьккдктнфифсбвбддкястнтнмслдьшсвьцйьшнсиеуюкыщцспрыьлнфкйдщщзй
ьцйныэвнхбрифкйыунрншьвнбкубье
бчсвйнжндуеисхавупмююсшодкльулбусчцнннстрсшншвьхаврщянсцознкссьеуснсмнмсн
сибссвддцйнчсщнэпозцфибссщщ
убссвнхбрифкясхщфдцяьклрыоибсчфкщйвносэиэчпнзкццяьклакаолржцяьзтхдицфптнх
щыглозфьцэидктнунэибунсхщав
ьвлващеутнищлрдцбщшдыцйнвнцхдздкицмяьхавьщвуцфьцжьщнмкпмдкяярнэирщввпн
оулцфрынщхыщмснфжврйвньркзскыщ
ссвнхбрифкясозййцфцнюириьсосйгыовдриклакязеудкяяосузмщчявввнищрилвацшвьич
дрщдкикгбмщбущстссвйьшвоейу
лцгйщщфкнхдкбщщйвнихобсчшибщекбщэюнхзциссичщиютнмслдфишдмбццмсгцшвэр
зфвджяжвявшнмсчярщхьовюстымщкзищ
ссыршьудццрреулфщщаефдхссироювяьисшщкзпксчролвтнрицнмскмжяявзтсиюгщхтнм
спбмщбущськмюннисдкдкцфжвйьдт
мщшвпвкмжяьямщшвжьрефщакиеэдакролфбклцбуябзщбукзунгэщьккгнввшнивжврщрн
ыуоззнбкжлтьбцрныгйснжшдекцгеэ
юсрсхщньбиулбунхнчйдпнввкцйнуншвэьтнщоьцчсуьсцтгуьйнньосфипьявпьпршьйнлха
вьщсиеуобмбмщбущсфрмщчяовуп
мюосшнкуаохщмсэкццзтбьыьмнжннуыфрыэиьсфсчсщьавозщсосгйлцмктзулынйнуйаих
щавиэжьчщоуобмблвыьрнунокпмшр
дцбщшддбубихйсансцрбжлвэкхюдрошджсюсунынмсйкмбкзхщхурсунщхввввмдкорыус
нчзьяуиюшсвпнкурмщеувирсунсцць
блшэннбвамозмщбвскаьшнжьжвупклэчйдищьешиивебпрябакоьзтянщиссйебчввтсзкию
щьккбыоскчицпьявицчзивяьочлц
свпдгсуфдкфьяэюдаорибщвчрытнрсбидуаодункющхиьсхдгсунфрлцдкяяакдункчзжсюсб
чкнбквьфзтнуноьюддкнхживнал
буыодкеиочоьлхэфдкфьпьлннсвнмкхсмщтсывзтьятнакфкпрябйожсюсунюиикцфтсввщб
акксйнбжрисцвджцмнщькмыгьяье
хщсяюсстхщрнхщбщыцвиклаккзеущнюсияоусчтсйьзткллрццюсстшнюдкшвнгьерынньэ
ьынавэкиютыннькиютноьакеишдщщ
швпвмндтихжцшнйнюирсыэьяокпмаобщцсэщбушсхщмсэкссьейпфкясищхнэкмбжлжвн
нстрсосщэтсяьяубщыцввяфжсюсунтс
чтгвмьввьелвмкрюеэзтдццрнмюхщбуакдожсвнйсзвпьфихщчсяьзтьяйкчзфсчсгэлнцнер
ссжофкеиябпвистнпвюскиосыр
ынщэгожсгцмефдфмжяосзкццзтпытнрсакьлмщриарзфеуэирибщхиьсуйвнихвнстйнянцу
фкщщцсунхдицяедьакхуумжсвнчр
лвньзтьяйкчзезьцюсжрыщумьцэиясезьцвнвнунищьеяцпьерынхщщщыцвиьянсибясшнлс
иьпвтснфюирыюсцьаккнивжошижс
мкарссжозщццесшндцнсккаирсыэокпмщнввйкриаршьлнуьэиулбунхмокздцрнфзфпдкяс
пнчкхуцфюижсшщязюсшсиэжьввшв
яэосрнеелоюисьфиосэщублыунчяюэецчзивяьокхуямщщшдбофдгвмсжкддьяжьяущнввв
вшнмьвврщозенйсуньейпфкаьтныо

еущькхзцнулцзтднчелвпьгцбуавкмлыклтьяуаишдщщмюкеоубщыцвиакэмлхчярщтсчтрь
йнвнцхмьакггмщшджсунлххэхьзт
лрэчбудквввзнввшнжьжврщунынжвжрццисчцэиаьмчвврщищссркжэжвмндтфрлцяьклхнг
цязвэкьзцэиьшсвмдьцюяусиебчду
ьешдриезмщюиоуриесввхьовэкжятнмслдзылсрщйносыклрлврнввлэусхщрнавпьгбубсвй
навдьоспншсмкпрынкчмсхщнкой
щщбщшдмефдфмжлрифсбвбддкяяыоввйнщцыгевввйьмэоьжйвнакеиэчпьидфккнйкриж
эпншнхщынгспнунрнгошддкяяфсшьыо
арфдрижлццэччсавпьзншвйнрнкизфтсиспьнкгбмщбущссцшнмьввьщянмсхмдктнянккб
щшдекццжлывйквэпншнхщынгспныэ
рнгошддкйыявзтцнюфввовявлиьцяьокпмаишнмнээхфкччтхдицивьспьгсунмщпвюдццфю
ирыусунлрлцдкяяыуаокнввпьфзлц
внстбвхщщслэмдчзоулыфьтглозфьцэидкнхпрынкчмстспьвифщгбрыяьцщжлзфпреурндц
вныкмбарбуябакфккчявпвлсзврщ
ьяшныйнмьунжкиюхщлвхщпэжвчспьпрццсвпддктндклцнулцмклытсющшдекццзтиэяр
чсжвюсстибдцньтсюсстхщээрщьечщ
кзмщрнтслкеурьйомюхщньюсстгнулбуввзнтснфчзццзтвииярщьякбньависйщкзхщхуию
шннуяетнхщюиакфккчлспьыопьрц
мнрншбынлсюдризьяуфкшдвчскскчавзтрщхсщв

Розшифрований текст із ключем (654, 777):

убиватьбольшененадопослетогокаконужеубилноследуетемубытьблагодарныминачепри
шлосьбыубиватьсамомуэтонеоднолишьдоброесостраданиеэтоотождествлениенаоснова
нииодинаковыхимпульсовкубийствусобственноговорялишьвминимальнойстепенисмещ
енныйнарциссизмэтическаяценностьэтойдоброты этимнеоспариваетсяможетбытьэтовоо
бщемеханизмнашегодоброгоучастияпоотношениюкдругомучеловекуособенноясноопрос
тупающийвчрезвычайномслучаеобремененногосознаниясвоейвиныписателянетсомнен
иячтоэтасимпатияпопричинеотождествлениярешительноопределилавыборматериаладо
стоевскогоносначалаонизэгоистическихпобужденийвыводилобыкновенногопреступник
аполитическогоирелигиозногопреждечемкконцусвоейжизнивернутьсякпервопреступни
кукотцеубийцеисделатьвеголицесвоепоэтическоепризнаниеопубликованиеегопосмертн
огонаследияидневниковегоженыяркоосветилоодинэпизодегожизнитовремякогдадостоев
скийвгерманиибылобуреваемигорнойстрастьюдостоевскийзарулеткойявныйприпадокпа
тологическойстрастикоторыйнеподдаетсяинойоценкенискакойсторонынебылонедостат
кавоправданияхэтогостранногоинедостойногоповедениячувствовиныкакэтонередкобыв
аетуневротиковнашлоконкретнуюзаменувобремененностидолгамиидостоевскиймоготг
оваривать сятемчтоонпривыигрышеполучилбывозможностьвернутьсявроссиюизбежавз
аключениявтюрьмукредитораминоэтобылтолькопредлогдостоевскийбылдостаточнопро
ницателенчтобыэтопонятьидостаточночестенчтобывэтомпризнатьсяонзналчтоглавным
былаиграсамапосебевсеподробностиегообусловленногопервичнымипозывамибезрассуд
ногоповеденияслужаттомудоказательствомиещекоечемуиномуоннеуспокаивалсяпокане
терялвсегоиграбыладлянеготакжесредствомсамонаказаниянесчетноеколичествораздава
лонмолодойженесловоиличестноесловобольшенеиграть илинеиграть вэтотденьионнару

шалэтословокаконарассказываетпочтивсегдаеслионсвоимипроигрышамидоводилсебяие
едокрайнебедственногоположенияэтослужилодлянегоещеоднимпатологическимудовлет
ворениемонмогпереднеюпоноситьиунижатьсебяпроситьеепрезиратьегораскаиватьсявто
мчтоонавышлазамужзанегостарогогрешникаипослевсейэтойразгрузкисовестинаследую
щийденьиграначиналасьсноваимолодаяженапривыклакэтомуциклутаккакзаметилачтото
отчеговдействительноститолькоиможнобылоожидатьспасенияписательствоникогданепр
одвигалосьвпередлучшечемпослепотеривсегоизакладыванияпоследнегоимуществасвяз
ивсегоэтогоонаконечнонепонималакогдаегочувствовиныбылоудовлетворенонаказаниям
иккоторымонсамсебяприговорилтогдаисчезалазатрудненностьвработетогдаонпозволялс
ебесделатьнесколькошаговнапутикуспехурассматриваярассказболеемолодогописателян
етрудноугадатькакиедавнопозабытыедетскиепереживаниянаходятвыявлениявигорнойст
растиустефанацвейгапосвятившегомеждупрочимдостоевскомуодинизсвоихочерковтрим
астеравсборникесмятениечувствестьновелладвадцатьчетыречасавжизниженщиныэтотм
аленькийшедеврпоказываеткакбудтолишьтокакимбезответственнымсуществомявляется
женщинаинакакиеудивительныедлянеесамойзакононарушенияеетолкаетнеожиданноеж
изненноевпечатлениеноновеллаэтаеслиподвергнутьеепсихоаналитическомутолкованию
говоритоднакобезтакойоправдывающейтенденциигораздобольшепоказываетсовсеминое
общечеловеческоеилискорееобщемужскоеитакоетолкованиестольявноподсказаночтонет
возможностиегонедопуститьдлясущностихудожественноготворчествахарактерночтопис
ательскоторымменясвязываютдружескиеотношениявответнамоирасспросыутверждалчт
оупомянутоетолкованиеемучуждоивовсеневходиловегонамерениянесмотрянаточтоврас
сказвплетенынекоторыедеталикакбырассчитанныенаточтобыуказыватьнатайныйследвэ
тойновеллевеликосветскаяпожилаядамаповеряетписателюотомчтоейпришлосьпережит
ьболеедвадцатилеттомуназадраноовдовевшаяматьдвухсыновейкоторыевнейболеененуж
далисьотказавшаясяоткакихбытонибылонадежднасороквторомгодужизнионапопадаетв
овремяодногоизсвоихбесцельныхпутешествийвигорныйзалмонакскогоказиногдесредив
сехдиковинеевниманиеприковываютдверукикоторыеспотрясающейнепосредственность
юисилойотражаютвсепереживаемыенесчастнымигрокомчувстварукиэтирукикрасивого
юношиписателькакбыбезовсякогоумысладелаетегоровесникомстаршегосынанаблюдаю
щейзаигройженщиныпотерявшеговсеивглубочайшемотчаяниипокидающегозалчтобывп
аркепокончитьсосвоеюбезнадежнойжизньюнеизяснимаясимпатиязаставляетженщинусл
едоватьзаюношейвпредпринятьвседляегоспасенияонпринимаетеезаоднуизмногочислен
ныхвтомгороденавязчивыхженщинихочетотнееотделатьсяноонанепокидаетегоивынужд
енавконцеконцоввсилусложившихсяобстоятельствостатьсявегономереотеляиразделитье
гопостельпослеэтойимпровизированнойлюбовнойночионавелитказалосьбыуспокоивше
мусяюношедатьейторжественноеобещаниечтоонникогдабольшенебудетиграться снабжает
егоденьгаминаобратныйпутьисосвоейстороныдаетобещаниевстретитьсяснимпередуход
омпоезданавокзаленозатемвнейпробуждаетсябольшаянежностькюношеонаготовапожер
твоватьвсемчтобытолькосохранитьегодлясебяионарешаетотправитьсяснимвместевпуте
шествиевместотогочтобыснимпроститьсявсяческиепомехизадерживаютееионаопаздыва
етнапоездвтоскепоисчезнувшемуюношеонасноваприходитвигорныйдомисвозмущением
обнаруживаеттамтежерукинакануневозбудившиевнейтакуюгорячуюсимпатиюнарушите
льдолгавернулсякигреонанапоминаетемуобегообещаниинооджимыйстрастьюонбран
итсорвавшуюегоигрувелитейубиратьсявонишвыряетденьгикоторымионахотелаеговыку

питьопозореннаяонапокидаетгородавпоследствииузнаетчтоейнеудалосьспастиегоотсам оубийстваэтаблестящеибезпробеловвмотивировкенаписаннаяновеллаимеетконечноправ онасуществованиекактаковаяинеможетнепроизвестиначителябольшоговпечатленияод накопсихоанализучитчтоонавозниклаонаосновеумопостроямоговожделенияпериодапол овогосозреванияокаковомвожделениинекоторыевспоминаютсовершенносознательносог ласноумопостроямомувожделениюматьдолжнасамаввестиюношувполовуюжизньдлясп асенияегоотзаслуживающегоопасениявредаонанизмастольчастыесублимирующиехудож ественныепроизведениявытекаютизтогожепервоисточникапороконанизмазамещаетсяпо рокомигорнойстрастиударениепоставленноенастрастнуюдеятельностьрукпредательски свидетельствуетобэтомотводеэнергиидействительноигорнаяодержимостьявляетсяэквив алентомстаройпотребностивонанизмениоднимсловомкромесловаигранельзяназватьетее аа

Висновки

У процесі виконання цього комп’ютерного практикуму ми набули навичок криптоаналізу шифру афінної біграмної підстановки, використовуючи їх для визначення ключа та розшифрування повідомлення, маючи лише шифротекст.