

Міністерство освіти і науки України
Національний технічний університет України
“Київський політехнічний інститут ім. Ігоря Сікорського”
Фізико-технічний інститут

КРИПТОГРАФІЯ
КОМП’ЮТЕРНИЙ ПРАКТИКУМ №3
Криптоаналіз афінної біграмної підстановки

Виконали:
Студенти групи ФБ-05
Акбаров Елшодбек, Олифіренко Іван
Варіант 7

Київ - 2023

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 шляхом розв'язання системи (1).) , (ba
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 7 варіант

хетжщбеыжцллийшллеторюкечождхуемебсфбпвгщпсакюбизыщллбюцжбщвлвачоофлеымяэвцфйжлцщвлиффечозуазшмвьпф
йбсфашазлевлазлевлыюфйгблфубфефцинютошрлбыццошыйтошщцоаимжцллийшллетктяфлеабуазгбшыйтошюийчажощй
ленефцинебгбгугфязазщешбйяхенефцинебуцбхннеоицсфозбохзьяфебчфеаесасчсбнцдвцащйлежцаечйхцсфююю
щцохжаепхпобуипылщмвьийлештьйбныэнесазнюдиупыкнякллийешцщвлифаоыэыюфйгблфубцлцсфлцулбэйекфрлмние
хеонялийпазагблцаыцзаяеяебрияоаефцинбоьасфюэфюлуькбшеьтчлоуаехулбцьдмэбрлютошюэопсфхйуллийуулялийуве
аечойлфеяйчэтимжыйшйшлтеоглжюймимкйейежйфтулэуозеочоаеяифмфсакбщлетипчьаьтобшифцхьялчюфййлфе
ййчэусасьйдемчюэийеьтнфлфцфчйофтцссасифылкцрлфлчлвсофртбибнпалйхэжйлеэыаурсээщцилмипайеымопсфяццтикс
уфйшиллцйноццфхомбобячюэубмилыбошньхйллцрксифрлвлсцзежцялильоусрлгешфйяхептьюзежцлялямчпрлццыялшй
втцллевьббйуйшцфаауспяолпэпрбиксаегвпаусубшыйтошньдмэбрлрвринийсрлчющцоаимжлфшйашщцниасчлчйжизаэчо
кбофлйхэжйебгбоаежймоьяалшбифжаубчбхйвьэбисазпфюжцчьсаьвчомйбчиеасчсптялгьбщвлифшйояпапршйвтцлленб
оцфюэсээыцлкуюльэдглцнчбхнялжхвбрижэчбллтньаоцкффулеаусзымуусуэиивгмуьаьаеюинсдязешумеиелцчйяшдт
сфашвидмгбвиччмуюажбсфдоцноцдпфжчйжйльсжфйльжчхалеихоинюеоицвбюйшйляфюмиивцвбйтчулйяцхожцаелеасуэ
яфллокотипчымаеачойлфезамкаьсажлафчуещзешцсьлгйсэйщжйсюзашмибхсасчсптжлпешцмвьбтрлцизаялхифюцлдоцц
цфютошшйтьбцыцошыйишмчюомэбалиоюеьяялигйжюцгонтнцдфщбкечоксюяфнцжюкюмиасюэююцлзшдюзэщавцвюййэ
ейгйофрлбфебошмфгфмюэзымебмфшизыяннэнтжлзджфаеэусюфймиййшбчаэшавцсубиложхюйгугфазлевьяфоллшйэб
сфайийшйшыйвикюфййтхйюйсфьдмэбцщфэапыюэаьтльаозачлоуаеюэелютошаажлбияожумйбтбцзэдгьймдтлзьб
рцщидпаешгрлбфебзтжлзгфчбмюыйвиелтаеэеьжцацфуэаьылэюеччбкеаеешэдуфуюцлбфпейжлгблбофуюлхшачнял
азултайеюелэуэшымдтчуошбияофютамжасасыумйбтлцлфйаэчоллвлосэйлежцьйфисоцобгбфечопурзэщаьттайеэоц
чллитснлбзаэблцссебйэтаегмвьобьчюйюхепйгбилхнкниелэфжкюлщьахутаоццльйдсщфкбошьйшктлцулшлнфтцхкл
ююфйцшдмьйешшцялвсхечойлфеяйвбюэлщвьклмфюфйхашчфжбфялцльийльестьялблгалесасчлщфйтюфьбюешмаеочоялхй
ьйбэпчлльэвьпаопнайиййавтюебюйьбсфнцьййбтщвьлекюьаллвлйлжечовфвфдэцаулпозавьчуьйэнчэмуулййшйшйимжб
цалшчунцлжйгцопнчзафиллфсучуйюклшлмфйшоффсфесцфюфйсспсфесаечомимкзанйбуилясрбхутаоцьаювьаьйэшым
эбтопчюеаехсбйеуувихевюаькфсжаццуэасхерюйтцссасетялуицжбьюсашчлтцвгкбрлципыйеьтимжчбпфьюоэигб
худнюлщвллфлдчзаяялцирюетмулемфлжлпцлцуицьуэюкццфывбцфжазэдгсумйбтнлэымсакюеоццошйэнчзэобвллвсэб
юпсфьюэемшйьзизийешклошмиццофгбтеебрийгдсвльбдмхзяхйилхйешулгоаежйошфьгужлтюжйттхутаоцазаялшлбифж
щфгййшцлтззсчутэкьносайэнчзэобобфщэеасцлфйшноцщбьйжднзашцнеелуиочлтяеачлялципыйеьтьтйэымюэмптфюэ
сфешгбдоьиаьтускючуфечофлялжажаоьаьтвевьечйщриццвбнцопийхеэтжлзулуйьэщаьтпуплекюьаьтбцихечьдмэбж
оцхэнцльеэастиялмйрчубжеиекьрифбошьтлялафщбццфюэфкцоюэнзвссфмсэщаьтщбьйжллвлгфчутэмжхююдюэфцкс
хеьавцшщаеебыймбебеееташйеяжйьгугьгуйбьйчэюеофбнховидмчюйхулбошювидмобхйтцьюфйквлхлчбкеоцхзмсбшае
оцфюобьйцшдмчуэбшбнйбшсдчлтэаеюэмжйрюйлечуэбэребмаьаоцфьюиксфюксгуофьфйялйлэрулзуледгдйюофмикю
рютацпаяацсшаасялбдмвьаьахутаоццымцпнчлэебцбщлжлмтлзвсаюэвьдмэбрлчрьбцфгпевбвшйшлллевцчууйжлол
офгбмйойесасчсщрийаасаеьавцпчьгызаолмбрлявцялбэасюэчяхутаоцтсебщсдгбиолдсшщлмфнмэбпвидмлщелэ
кншмфюаеюэфюфйауофйобпйленебнцлмвлбэагницнксвцулсфкцлжлтамжасаеиагялхйялшлветиоцинаьтемдтмфю
ажаюйофэуэшмфюуштигоаежййюццеоыиолэшэшачляняльюьуэцлбирьшлдэхоефгйчйссшцвбьйтцацофафччыэусымчбшм
юэйшкссэеочнюдгулхулбщлэщазаяейжлвипчзаяицжфюнтцбаюебцмихойепалэдгшифюцдялаэксшлмсэзтюаьчюьмнвэбйб
бинчшйьпфчбпэымелциеуэцлжюшриозянвгхйкенвэлсчоиейщришщфьтйбошщбыйьэщцошвьцлктсдгюэлцзийилевцф

фюгыьфмдтшйнцифюйюцялвлжюзщбццффечоьлдсзэщаьтбцщзээюфмктюцжшйеитстсьинйубафгйчйшыйашоэазщлнэсмса
фюсмэбгбкупебноцфюейхсчлпшйлхэгящэтюаьчодгшйищццфимдтлэьбсфиллеозйтчуаулитсефцбйшпзгьыэоцйаумийюе
зашифююкксебйэагiasmхзевевдмцщвлиффечожлщлфйжлфлцлифнцзебнцлрлнэмжапыэымцжнощйшлжллщлйялдскьхеэфжш
вьчллзчбюйгффвбзэлейпэагулсьдмэбрлкыйщвбсфашмикюблцлфулеагуумолеуцфсфрщпывцхзыэпчнземшйялчбюйллте
ызофйэпрауиаьрщйыйшчуашзаяноюпыйробьюеблпфщбюэьпрзайгйфоцлжиюензпоыичйжйсфьбнцюницнобебнцл
чйлешзисиичифысюкибцвбйшцлкийипацвцхзэрсаязасфбцнтнзиюеночпкьялщлцлясновцсаялфьмьйпэуоусщлмсноэ
мпбщлеуичоцйулщвлгфчуялйуцжрижэмпщцлчбмйшобсфоегяебнцлобйуьсчпвлщпэейщлэсдггулщьдмэбтыаоцллзшб
нцьюцджцпблццлрэфюлзбжааьююьпрзааанозефцинфщлйсфлжйллжщвлофцзьбсфчлэьыробихийжщфлйхстйебнийьюь
ццзенефцинчлщлхсфюбжлщлйхутаоцкюишцсфщбвьчуафжаоллэсдщдпокюобьчошмжуойлейнзалщщрийяеижйошиссае
ьашцвжюлоажбщблептийшмцаллырзафюуикьйепапччьцллзшбщлафжаолщбафумтфщбфьечюкдгхулбцьдмэбцжйюенткейм
юэфжщбэбилцйцфшэзачбьйулбэюлжжюсщдэцакелщвлфйутебэьгужлщьццеагщбфлхйбипчашбаюкечяпапрдкыэчыбошой
цфолфйжлщйхшгфьйулофлбсфьгубеасетщбклщсчьебнцациялилафлщемпюеиульсритючоаюриобэктйалщлхзаяноциаьлл
лензлрвлцлмймивжкювьчошбфйчшйьтлаюехугьцянялеопдгхутаоцажчбцьуснгчлаажцумипялблчлнбшефюэююцлзулоб
цфсфашулдйфааьдмхзщзэьацщзэьаюусхьеавцщщцчаюэьрсалбрлтээйжлжйшлжээромэбгбвфчлэеиебнцлщлцлясьабюэ
цлхйфеымщцгйчаьлофгблзбнсфашобшикпрюкпвлщпэейажчлзэруараезальщюэьдмхзьйжйгэщаьтьйчэюейчэюехутаоц
гбдоьиаьттехоцлгйттлсшцауцбсфютчэвцхзпаглцбьяьечойерьюечообсчаечлхоэюфйюдмфшэядржбшевееллофйфознтйэ
цжщбшехежсасхулбжаглцбьяьэццрзоэлщвлвальзафйтюаеоефтамжухиййилтаажуэбопуэааьйебртизыопыеасбизыйщвб
цьдмэбяртизыопрюфйшэзаолцлдсшэрмэбгаечяюлюпбныэаццялшаозрллщбнэбовцмйшаьтжлщльбшмжулфбэбашйжапэ
савцхзэмпшцлмлэбгбэрлцмикюеавцпдмэбюлежйчйчунцщбжмжбюеулбтщлжюфйвбгфазшлгбулбцлэщбвлаэлщщый
шэоцфдчбвеопюхялрлбэдгзайняашцлсепчтгбжлчлжйэлцфжщбюейейшритлижщбюевеэфнухйшэядйлйшбщитсълфулеа
оцжцозрлхзфщвьбтэбшмфючлэьырулобьяфьбацлэуэюеййьпрцлйбэончхуаешлафялилафеяиибщуэнзмюлежйцбпаглцзий
зыиизыэнзщьдмэбрллетипчцулмиымзааюэфщлжеолофазсфобзнччтйвцкьфююютиэтилхаажуизимжбфауфмцпуцаечо
йжтаеэщашбаеьбзэхечоетульйсулцтюаьбхсмжаэюэфйжлнэцтклиувьээлцюдкйетлофгбйбфлаэжугосрчусфашолыьзатй
йуыйвичьдмэбдцлшаиуошулобьяфьбацкфмюэзыкюццкфлеисядьфрцксчюйрлщегмююзаяйугуфклиуулиулцоюфюхевюфй
веаесачсчопчцлхулбщлербноулехебрбнлжшбцвбошьйшктгбазошофйжлнэеажкюмиуэфщщюйюэщйшлгшеэьэнэрцщц
члвгйтхйщлхэзывгмжуэбоаанафщлрзажбщйрмфлжлпцлуичьтфшцойлфгййшлплаюеюбщзаяйрлцфунбсфхаечыэнзхоц
саыитсолыьмйсфолкцулхзобнцзеасевеелгйхьечццщюхьешмцжбщюйзльйщбфлбиоптиилвбцьдмэбьтофлйжлмлакнцлщб
дасццийфлципрулхноцьлцеуэбзитснозымновцлцлчеебшуустифоббэжфлгувешщлрэлешанхезавцлэяжлгйюул
эйбэьмнлешанхекскеаелеиизаьтвбшабцлльшгбцьдмэбтыпальаозаопкечодпбцилхнзаяюгаечявафщцжчьфшжйфллекю
дтрийувьцлйубисасмхешиежцьюцжяаццдэйщбфьлщвьоплсцяпаусхлцисаетиййбиюаьеэропбээфюжлвмфчлхмтивь
теаехйшжштййивьцлаеишфюьэтйшхуьсоцялшашбнфвлллошиичьлнсшзйшэййебнцлоблфвбцлтайрьюзанфлгфьзаьпфкэ
ейбишцялшзчйжнэбобехсзэщашцяаеелжюлщлшбйюериэзашьццфйфилозрллыэмпэфьуфбвсдмшйлептсфхутаоцйечою
лщвлшбсфялйшлщмелнэьмвьаьпыобюэпухйрлнпальаьпыобулхсжйпщвьйвлфлсцщежцаехзьткбчхйдюефцинзэкюрибт
обчбчбклвлнфювлфбрцопыхеяашмлрлнйщфгйлцйцэбиушйьтошэйсефюгбобюагмйхлрсаетиагозбизэццюеисбицсусьи
юб

Код реалізований в (3.py)

Найчастіші біграми без пробілів:

```
[('цл', 51), ('ял', 49), ('ае', 43), ('ле', 42), ('чо', 39)]  
[('о', 848), ('е', 527), ('а', 526), ('т', 476), ('и', 426), ('с', 423)]
```

Ключ:

```
[[200, 900]]
```


[illegible]

Київ - 2023

бенксом восемь раз видел призрак во переслономчани четыре раза смотрел милтон асиллса даже один про любовь садольфом менжу толька тогда просидел целых девять часов в киношной уборной все ждал что бэ таерунда кончилась и пустил кошку и канарейку и летучую мышку ауж тут все цеплялись друг за друга и визжали два часа без передышки и сел за это время четыре раза leden цов триста ну чексемь сот стаканчиков мороженого томболталеще долго минут пять пока отец не прервал его сколько год ты сегодня собрал томровно двести пятьдесят шесть неморгнув глазом ответил то мотец рассмеялся и на это мокончился завтрак и вновь двинулся в лесныетени собирать дикий виноград крошечные ягоды земляники в сетрое наклонялись к самой земле руки быстро и ловко делали свое дело в дравсе тяжеле и адуглас прислушивался и думал вот то оно опять близко прямо у меня за спиной и ео глядывайся работай собирай ягоды кидай в ведро оглянись спугнешь не тужь аз тот раз не упусти но как бы его заманить поближе чтобы поглядеть на него глянуть прямо в глаза кака у меня в спичечном коробке есть снежинка сказал томиулыбнулся и глядя на свою руку она была вся красная от ягоды как в перчатке замолчи чуть не завопил дуглас не кричать нельзя исполошиться эх ой все спугнет постойка томболта ета оно подходит все ближе значить оно не боится тома том только притягивает его то мто же немножко оно делобылоещевфеврале валил снега я подставил коробок том хихикнул поймал одну снежинку побольше и раз хлопнул скорей побежал домой и сунул в холодильник близко ко всем близкотом трещал без умолку адуглас несводил снег глазами может отскочить удрачьведь из залесана катывается какая то грозная волна вот сейчас обрушится и раздавит дасэр задумчиво продолжал том обрывая кусти ди кого винограда навесы штатиллиной сумения у одного летом есть снежинка так ойклад больше ни где не сыщешь хоть тресни завтра ее открою дуг ты тоже можешь посмотреть в другое время дуглас бы только презрительнофыркнул нудамолс снежинка как бы не так носейчас на нем чалось то огромное вот то обрушится ясно оно баионлишь зажмурился и кивнул том дото гоизумился что даже перестал собирать ягоды повернулся и устался набрата дуглас застыл сидя на корточках ну как тут держаться томипустил единственный клич кинулся на него опрокинул на землю они покатились по траве барахтаясь тут же друг друга нетнетни чем другом не думать в друг кажется все хорошо да эта стычка потасовканеспугнула набегавшую волну вот она захлестнула их разлилась широковокруги не сетобо их погустойзеленитравы вглубь леса кулактомаугодил дугласу по губам вороту стало горячо и солон одуглас обхватил брата крепко стиснул его и они замерли только сердца колотились да дышали обоим востомнаконец дуглас украдкой приоткрыл один глаз в другой ятьничего вот оно все тут все как есть точно огромный зрачок исполинского глаза который то же только что раскрылся и глядит в зумлени и на него в упор смотрел весь мир и он понял вот что нежданно пришло к нему и теперь останется с ним иуженикогда не покинет я живой подумал он пальцы его дрожали розовеяла свет устремит

ельной кровью точно клочки неведомого флага прежде невиданного обретенного
впервые ей же это флажку теперь присягать на верность одной рукой и он все еще
тиски валтоманосов всем забыл о нем и осторожно потрогал светящиеся пальцы
словно хотел снять перчатку потом поднял их повыше и оглядел со всех сторон
пустил тома откинулся на спину все еще возде руки небеса мигают теперь весь он было
дна голова глаза будто часовые сквозь бойницы неведомой крепости оглядывали
оствытянутую руку и пальцы гденасвету трепетал кроваво-красный флаг ты что дуг
спросил том голос его доносился точно с дальнего зеленого замшелого колодца откуда
то из подводы далекий и таинственный под дугласом шептались травы и он пустил
руку и ощутил их пушистые ножны и где то далеко в теннисных туфлях шевельнул
пальцами в ушах как в раковинах вздохнул ветер многоцветный мир переливался
взрачках точно пестрые картинки в хрустальном шаре лесистые холмы были и всеяны
цветами будто осколками солнца и огненными клочками неба по огромному опрокину
тому узеру небосвода мелькали птицы точно камушки брошенные локтем рукой
дуглас шумно дышал сквозь зубы он словно вдыхал лед и выдыхал пламя ты чирп
елистрекоз пронизывали воздух как электрические разряды десять тысяч волоско
в на голове дугласа выросли на одну миллионную дюйм а в каждом его ухе стучало
по сердцу треть кололо тисось в горле настоящей гулкоухалов грудителю жадно дыш
ало миллионы и поря и правда живой думал дуглас прежде это не знала может из
на дане помню он выкрикнул это просебя раз другой десятый надо же прожил на св
ете целых двенадцать лет и ничегошеньки не понимал в друг такая находка дрался
сто миги вот тебе тут под деревом сверкающие золотые часы редкостный хрономе
тр с заводом на семьдесят лет дугда что с тобой дуглас издал дикий вопль сгреб тома
вохапку и он в новью покатились по земле дугты спятили спятили и покатились по скло
ну холма солнце горело у них в глазах и вот тут точно осколками монно желтого стекла
а они задышали как рыбы выброшенные из воды их хотали дослед дугты нерехну
лся нет нет нет нет дуглас зажмурился в темноте мягко ступали пятнистые леопард
ы то мити шетом как по твоему все люди знают знают что они живые ясно знают так
ак думал леопарды не слышно прошли дальше воть му и глаза у него не могли замигивать
следить хорошо бы так прошептал дуглас хорошо бы все знали он открыл глаза отец
подбоясь стоял высоко над ним смеялся голова его упиралась в зеленостылый
небосвод глаза их встретились дуглас встретился папа знает понял он все так бы
ло задумано он нарочно привез нас сюда чтобы это сомной случилось он тоже в заго
воре он все знает и теперь он знает что и я уже знаю большая рука опустилась с высот
ы и подняла его в воздух покачиваясь на твердых ногах между отцом и томом и ска
рапанный вострепанный все еще ошарашенный дуглас осторожно потрогал свое ло
кти и они были как чужие и судовлетворением облизнул разбитую губу потом вглян
ул на отца и на томя по несуду все в драке казалон сегодня хочю один в сета щить он за
гадочно усмехнулись и отдали ему ведро дуглас стоял чуть покачиваясь и его ноша

весь истекающий соком лесоттягивала ему руки хочупочувствовать все что тольк
о можно думать хочучу устать хочучо очень устать нельзя забыть ни сегодня ни завтра
ни после он шло пьяненный со своей тяжелой ношей азанимплылипчелыизапахд
и ког овинограда иослепительно ело на пальцах вспухали блаженные мозоли рук
и он емелии он спотыкался так что отец дажесхватил его за плечо надо пробормот
ал дугласяничего я отлично справлюсьеще добрых полчаса онощущал руками ног
а миспиной траву и корникамни и коручтословно отпечатались на его теле поцемн
огу отпечатокэтотстирался таялускользал дугласшелидумалобэтом абратимолч
али выйотецшли позади предоставляемую одному пролагать путьсквозь лескнепр
авдо подобной целикшоссе котороеприведет ихобратно вгородивотгородвтотже
день иеще однооткровение дедушкастоялашироко парадном крыльцеиточнок
а питано глядывали широкиенедвижныепросторы переднимраскинулось лето онв
опрошал ветерине достижимовысокоенебо илужайкугде стояли дугласитомиво
прошало только его одного дедушкаониужесозрели дедушка поскреб под борода
кпятьсоттысячадаже двестиныча наверняка дахороший урожайсобирать легкос
оберите все плачудесять центов за каждый мешок которыйвыпринесетек прессуу
р

Висновки:

Під час виконання практикуму, навчилися створювати та розуміти принцип дії програми автоматичного розпізнання змістовного тексту, спробували провести криптоаналіз афінного шифру біграмної заміни та знайти вірний ключ, для розшифрування тексту. Набуті навички знадобляться у подальших практикумах та професійні діяльності.