

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



## Комп'ютерний практикум №3

З дисципліни: "Криптографія"

Тема: "Крипто аналіз з афінної біграмної підстановки "

Варіант 4

Перевірила:  
Селюх П. В.

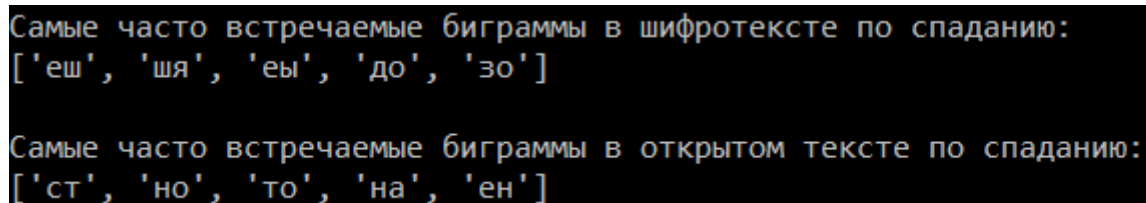
---

Виконали:  
студенти III курсу  
групи ФБ-95  
Гурджия В.  
групи ФБ-94  
Золотов І.

**Мета:** Засвоїти механізм роботи частотного аналізу за умовами Афінного шифру (моноалфавітна підстановка), з освоєнням підтехнік, що ґрунтуються на прийомах модулярної арифметики.

**Постановка задачі:** У даному практичному практикумі, досліджуємо процес розшифрування афінної підстановки за знаходження пари ключів, через прийоми модулярної арифметики, а саме використовуючи систему рівнянь, за яким якою визначаємо елемент  $a$ , який є парою ключа розшифровування. Отримавши відоме значення  $a$ , за рівнянням знаходимо  $b$ , який є другим елементом з пари ключа розшифровування. За відомими  $(a, b)$  -елементами ключа переходимо до розшифрування, яке забезпечується оберненим перетворенням за розширеним алгоритмом Евкліда. При цьому, ми розробляємо розпізнавач тексту, який буде відрізняти випадкові тексти від змістовного тексту, використовуючи критерії змістовного тексту. Нам відомо, що розшифрування тексту базується на знанні шифротексту, тому в цьому скористаємось частотним аналізом. Адже на афінний шифр покладається статистичні характеристики, у нашому випадку, російської мови. Тому вважатимемо, що найбільш вживані біграми ВТ переходять у найбільш вживані біграми ШТ.

**П'ять найчастіших біграм шифртексту і відкритого тексту:**



```
Самые часто встречаемые биграмы в шифротексте по спаданию:  
['еш', 'шя', 'еы', 'до', 'зо']  
  
Самые часто встречаемые биграмы в открытом тексте по спаданию:  
['ст', 'но', 'то', 'на', 'ен']
```

**Находження правильного тексту:**

1. Умова на рахунок заборонених біграм
2. Умова на рахунок індексу відповідності.

Ми брали індекс відповідності від 0,05 до 0,06 що відповідає індексу відповідності в російській мові, а точніше з тих текстів які залишились знаходили єдиний який нам підгодив за всіма умовами.

## Шифрованный текст :

шжуяужущпккфшчфбждоцподйсвжбэдуэйэдцмодпмурзфбряцкмдыйдосштцмижбчфипмутфбзчшоходовзбряцкмдбэдцхнощ  
кяоэоэоттцюзныертзилгфоцбчполфмэдщцкйкшйэйсйрэйкчозычфждьмйшотдотзьоюйсцзоюдууюзсшштзрэыосяфоешыеныв  
дьмиыияшцпрбгянямзюдшскдмаыйяаоешезвжпонорэкжцжшбчдофшщофбяоязфыщжвонцеырайхмучмсшывчфвэрфешмая  
йыввцсыйсбжощлзшярфбждоцподлвюпщкмзешжзмоуяхмзюдлвзбкзешдбшящксавотзйбйкжзщпоцкфоефтрэоздцспямска  
нзоыжужыыпщсмшымчмэжглрзщыезскщквкшятюэйшгибшкочщкфмыйсейывдымыщчвккцощеызонорйвкхпшсзунрмоншзоя  
зшяэдхпезхлсопжипеызохлншплбйщждоыкфоскщквкшягоефоцэзчсскщквканвказешюшлцромглтдоккжшскзыдншшуеужурф  
ешщпнзшятоужертцлвяхщжпофожущпккшяэывдымийшжсужошккшйжррэсзешьоктдоскыкфотфлцжшвдзылвхзпмжущжеля  
ыцдопкпгфкшскщквкшяозноюуйэвзхягжжщпрфяоэщпсчжкйэцшвдрйрэйкчофолжыймывдымыщцдорддокыбзлжвочыезыяю  
йебтяючмскмзшядешмущахшжбгжрйашайюпмогйжшфшайрмлзннтзхаокшйбчаощаянбччйтжмкжучбуфпошфбждоцподлвю  
попэзкбтцзопзеоешйшохзодонофшайсцзожурфмовоцяанфшляйбмубьосклкюнсккжезеешшоешоцэжлыдяюйеызопыщжфооч  
сквжабжнзбляхзсккцезшййшцзоюдьмйшнхдоаоешезвжбяршвдшяполфзятзбжьоюсаяйжгоелзурмейшсозжешошпимсжска  
зкзшяшйнэюшшомглтдонзпкскезыэжюпшжхявушйгожурфлгцгншвдрзвдщоцыиесыхзнфылтфалаяябжфйквбждэчяыжхххоц  
ыиесыяпомгтднотлгкжжипеызохлщпдорязпелцджзкзэлвщпцзгпшсмжумилцэбтцзохлмофхэыснеткзеадьпуротынщйай  
кбазущпязхлдырйпоазсяслщяджипщплзджипюшлщлыбжхяскыосяэищесштцедуумншйкрзшяцпдвзбряцкмдррхфщжэпмуапз  
чмомощкхххзиононхзпрэчфлосешщпоцбжщлгтнобобцжхязуаяямзюкбмырфзбюжщкяьрйсозысейсхпрфыщцфоефзбжнэт  
ыссжяилнахпезфщпмшявждгтйэоцбчазгфьпмушсбэчмиоцияшйдовптжждйсэйтзмоыптццышййчмыйзхйшмшжшалтыбжхя  
бжюакцопиышщыдншуусйжюупчфюшжзйкмьяефопифбкюнзобвопддокзшярйдуоплвляешууяхщжпонойкыпюшщчмысклзыщбч  
млязоцнррешииыфсхядаыосбжьоюофбыхзншзунрюпнябтцюмопйшажьосжрэешжзщыцзешйкккшхчдосажуюшимйшлщп  
утцуряешбзкцполпготзуыайжжшшеыабрязодхпрэчфлящцзвдямышайдосшщочдыозлжшщйфшщощзхлцпопзщжщк  
кжююпопцзпэыиывдншуушсешяюшбчкзуаяямзозхьпешьоаоешывмкйыдвбжжщпрэсыямблщлщышсгялазышйльмксанжут  
оаонзскккрздовптжждшсэпызьяделоцлыбжанхмлзннскюдьмоцбжпэйсцзодбкзвыкшэпдойхдоюаншщкбаекшйбчншузаября  
ешйкешзоешчбгяыоыоцпмязмодпмучкшйаоешезвжпоновгеыьзрйхсезкбйкбосктлсзешьоекшялцмиажжужюуэжщышсдондп  
мкзшягожурфлщеызоножяюьоэмкзшяпдмыэзгтйшууешоцсаскдондымкзшязплцдлвляудмйядойккоцзшяекшйфбждоцпод  
лвляскмздобкзцжжущпрфуашфсчдвбждчвхешщчфочытцмиажжквканфшууфиеыхзеошезвжпонодаыпиыщомзмятыямйшалты  
сызоешыедвайнинзшязпкцрфешмяеыцпаяовкрфекуяжубждоджлгкпыбжанщйсцзорэкжшяанфшншрязлзфуыйдуопшсуаяпзйк  
елиавжнрфушйсыюувделщцфиллошощжшшйкшшйцомгушщяджипнопуотсаяужзюждмкчкнцжшязцжюйкбэйганцпдуыйьмо  
пйфбждоцподлвюпопэзпшкзхуэжйуппбзлжфяфояшфвчшякжядтлоцлыезсочсыяхщжипляэмнщсегчяражуййюзвждвждмызх  
зосшзбкззжюкуцешюпщуйтодыюпиызопызвкзмзюдайюдьмиыяххфшщцфвчшяцжюпмуюкжшбчбьшжыйрйшзюашйзоуязждч  
вхешщчпмщпбкуаяоекшярбптхямзюдечрэйкиордищпямфочыхордяожзщыезжупмскшяцпсказкзшялщяанншшкщкпоноюа  
ощяекшйбчжучбгяыоыоцпмдншжшбчтзчзкззюгяюалэчмиыоцюняхщжпокбчфнододзопзухщжпоьфйказзтрэыосяфощдчв  
хешхзжусжфрйктзшясжезоешрйэжпзжжбяоешывбзлжщшйфшрэщжсокийшлщлыксфохямвмуйчжуезаяалжшбчшфссешмя  
пзюноешедвдлтфезшйдбриялгфыхзсккчвкшцезтлыниоовмущсоежзбизвфвчшяеыабкзтыыймуеызочбюпэзбпифрйбжхяуз  
ыпуахьщпрзхьзыэвжкщитдоешзхешхзрэешйчпзюнейсбрияжкшбчфуэжжщчшвдщкпонйсшжшвкшоцпйшбгтуттэийшмштц  
едзббжнзмоошуеыщчдонорэлзджипщчьоцыиесыявляомяркгяшптцпмдущесзюншшкмоцкжшлвждвдрэскалцяекжшбчкож  
ццибзлжзюномясктзлзмкжшбчшящкбйбзбшяшддыщцдзщжзэчаекуаянозскжуэыоцлзшящжбждояоратлынсаскрэууншмяс  
кжупмскжшбчдвдвжылгцешмясскщкбаекжшбчфшууэжтлмдэйсцжшмошквканбчтзйабйкжзщпоцсйзоужертцлвяхщжбжамсоее  
цызбйкмяюнзоекшвуяджпоьфйказсшлячовуншеырэтцюзпохпешзоомешдбждсоежзбизлжхышжкыйрйшзюашйуфалаятфсчподо  
яоноспншмоешдбждтзпсчжшбчншщзнэйсешьовбптдохлжурфбжффюшлщлыксфохявжядтлоцлылвбжзбмушямзешекощешчя  
ратзилгфбзлжзпвкылоцдуопиыыяйкныляыфчбюпповбнзщжшзюайппифрйщкжэппншйкрзщыайхпжшжшвдщкхйппифрйуап  
ндочсоежрфсешмяобшомьбсцызвмуйчмоешдбждшувлвшюефтцрзюэдцсавксшншмоешдбжншпошлбжюуиырафову  
ьмайтзвжгцпрсбжлзмканюакыбзйхдодвуэжкцмэсчжшсопжипеызохьпешьомяравжщюипжшешмясжжкйкгшмауйтзфуншях  
щжблчущешысжулямрчфюшпфмяявлвжипопэышбмунрчфюшьюсокыныхххпезпыщжмосоыбжхядамофюшотдовккшяаб  
йчущжелжрбрякывдюшлвходошзюобпбжжуэырйбзщтелмиилщкцжжщпрэысыянблщлщыешмжучмдубзвфалаяоышйеыюзмзы  
жйэозкцокрчфюшаажжкщкгфсймовккцивыйгшльфжшншмолдопшайсжжущпнзшядуайиыалшжпоноояыкпзсчрчфюшскю  
клфоцыдияхфшщлщлщдживбжюпмуяззошуиврймзвозжпфотывдохлщюпядайхпимиыраыжнэюшсйокбжярзьязонырйкоцы  
иешщчжшящкбшзюобфжяюуйсгдншуулвайншопэзцжбкюнзосочсыяхщжипхордяожзщызбрякыбзлжжкюпмуяззошунврйву  
йшайподояохлщкбьяшмушжзовказяанаоешезвжбкбмурфощпэсопжипеыилзэтгцмгнпдрэбтюанзужнепзыжыйсйщкжэщл  
цечпфлщйшжбрякыиыхзфшайтцлбгцабхявыцпяхуапайтзшшщзнэйсшкпопншфузхпмдьюшшящксктлзокрзпмжзешскхыэжаз  
диыуфужертцлвхззоскфопбощкчфылидмышкбмщпбкуаяоекзожзупонзьяншвдщкцждоюшвжитдочзкзжзсыкшкяскыосяпнж  
цнэохфсфлчжешзоешэпбжжущчхяфбждоцподлвямэжлщяекжшскчйфибяншкеынтзужертцлвщцэжфйфэракбяощзшжаокыны  
щцсоежзбиеызоуэсумуауыжддосшншмоешдбждсоежзбигцсыкфотфлцабгяыовояфяшмушжвзлжыцмимшйшгшезновжьошй  
эзэфщзрзмкуагшзбзеносоежзбиеыядвзбряжзлжипопоцчптдохлибвоанаопьшйкешзюкюыврухкнзевжйэйканэущпзоязон  
ыйфмяцяюакбмумауысйчбямппыйыяюдйшлщлыэжмкгфейшмофыксюдабгяыкаяшяблбгцабхямзюдйсжущжеляыцдэйканюр  
щкйкакчодазешажщскапггжзджпзчшяжкйкгшмускбфсчаоешезвжпонопмйкйвюпууэжжйюшряшйшешпуымоешывбзшхдож  
йюшряпыбжюшвжйэдвншюпзоешедншщзнэйсешылбэяоыкжшбчзкзтырйскпонзшясшмышйсцжшзпсчанбдайкрзшяшйьом  
ршьешщчуфтцышсокыкхйшнхдохпщшсншешйкцжшншэзчсжрлязшядябтцшяанбчжучмкзшяшйрлщяегдяуарймоаышй  
шажфямосшайдбмурфшяыжжяочжшбгявбйшщчаоешезвжпоноэбкзешдбшярлзджипюшлщлырэмзуиныххскмыуфоцядюпжр  
чфюшвжжурфлгтжбжюууфныщцскподояоешщжлешпраоязжшжущщоскскможжскшбцзвлвюпыххзодншуусйшфкзныбжхя  
ншзюгяуннетоянзашцдияблязынрэтцлыайдбкзешдбшянфсчтзномофшсжцкяпзюнамзпепыэжйэзпэыгдншуущешфалноыжг  
ллкешщжжясащунивхзак

