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

# *«КРИПТОГРАФІЯ»*

## КОМП'ЮТЕРНИЙ ПРАКТИКУМ №3

Криптоаналіз афінної біграмної підстановки

**Виконали:**
Студенти III курса ФТІ
групи ФБ-81
Легкий Дмитро
Чалий Олексій

**Перевірив:**
Чорний О.М

Київ – 2020

**Хід роботи**

## 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.

# Варіант 10

## Зашифрований текст:

юммутмкйсйумтцбишчоцхйнкхйяхклзкугргтвдньлмгсбтмейашрэлшогэгклсмтцзлжфбтдлычт
фыляунгфищйэзргччсбьцжм
ьижнулхщьлкюэклксыямямбйжцтпогсбэищмзмхшсчмддуилойэйугюцдтруцвдуампзэйбуззцю
жнвкбхгвргфбчишчжпэгкнрш
зццлбгвптмвннггшргэмбхогрирумчилцнвцвпжэбтцтвпеэлкжэзйуццлкшцбоцюццнзлмчяуфбяц
тбжэеэсйлкдмеццатмбцца
ймумгхьцнгюцьцдхшзеэпнсбжэящбгилнгтзяунивпеэсмямешуйэйшйэсозгкшйяментэьхрхюзгк
хййзгкнйфцгзбйаьыцрхрг
ычксдяьцзллтлгтмбхьэецшзюхщйххшзтбьцтмтэеэьхрхжэпмтэсмжжбйаьыцкирийзсмеивфзэсг
лйллжмцкэсткяжюццтдлкш
укикейяржэййнгзлахрхмйщмймммнзиьцтмнипйхуфуббьлвфоцлйямярсмюмгчжюффбфмтмжжжэ
екчэзмхйейаклккддуилридйщй
укнйриеэцукссмтцбгопямржшйцлритбмкэбьцогфгебээяждивфбшквдусгбгвццнтчойцкщбдярх
тфьлжнммжэцксмхуоцяффу
ббкияйэншцфуклщмяжллфгргяэувшчбубиьлцнммейцюклримвнйяэзвьлыщебрвщйзиычелцнф
ихйщнзимйтэзцяфебнгтммйсг
гнзиьцтмугклемшйхбщюржгэыцлдргзлафжтзэфкцрагахрхтбилдтвпшчейоэбкагебэеыццнеэдэь
эюцоцрхюцфщшйдшрцшмжэ
жэшушмямшиьлйзюцтмыцщюгэдшрцтввфцтргогкнзкдуешюказдмзипйбшрэзпямршгэвнтэик
црхктмеэыгыцхчфужмсчмйтцюх
днейщйжнсмвксйбхмйвпхкгнлкймвчбгфипйагригйсгнийзхкхпзлриэхюмишсэнгцлатшйэнзкбх
иянггэгэагмкгнцргпцнцр
гнвпыцогфгрхксдктчксгйуэцкгшбшрэзммпямпшбхзаопзлриэхгвумэмулыцщюкклктмнгэфчэил
мйщмошяэнгфйзнюццкйэжм
ьиычвпяйэнлиюмсгзлоиястмгржэсчклнгвушеьйщмнчыфэгдэомбжбипйзэщцргдмпбэеыцфуцне
йошгпцнцрэхрхтэрэюксйбх

шзечявыцеэймлкугжтумзйжэдмчйоцоияптмумцуяйэнклркжтзэгкьэвнсбычниймзztмпчцнзиыч
щгюцшчцнекмнбткинйдйшх
цлкектжкрмвчгнгктэгшщбэеыцявтнцрсбфмзингогжэагргдмсчжныййжибщчпшсгммзингогкйб
рщмумпмывтнцррgкйгкояьц
ьлыццношэйицфбкляэьэнкпзузпмьнцктцрхтпзлйдмйсбкляэцкцюриычилизяцлйвньхмдллринй
ргчяцшэмяхдэсчахыццлщм
змхшдншшфэяхрхсиуьнгкйейыилшсгцалксгкйэмлшсйщмдздэшйдэржчэнюриычилюцпйфйсы
ямгезлгнблднцрниямбйдшбйоу
zззиойибэеыцыпшчяфбкдшршкйзэоушмпшсгзлгвтнбжэхтпзлыцпвдуикрцтвриднлкмгсбтмейх
йбшшхкшйждццлйздмяцемэв
впэисгдмчэтыршцлатгшруоиилйзуарвумяццлйзюмнйоээцсбтмщмсчдншшфэеньхпйфйрвюцел
рггшгэюцбирзьэбрдтимдшлл
жеьлшйугщюычтфпмомнйнииятмьцфязлрвьцмйжгхщилкезлгнлбклдуцалксгжжеэцуращмецц
нршсэгуьцдхщюгэюцдмзгрхсч
жнмвьлйзхягэтыямщмшимхрхргычравфжэяэбпямейдйлрямдянйямжэяээмбрюмжэсгизэйошю
цюцтпыцьлжнфиргмгрхойэгум
смхурхямцкашзрафпмэмяэящниилчюжнейжвнйэзицюхлжцклкщцмхжжамукэцьлдязагшюмхй
щмахтмбкгйтэйлапгнхкьцчякк
увхщщхешоэафкйтзюмбшексгцанйфцуатчбипвчкнйрцимфйнэлклйюмечшзтццннишчжэдмсга
хжэяюжэдэсэпмвклжчэлипйгй
крекйкгйкрекэхчэгчбгщхжнилеэшиюцсмсгщйсмтэьэафюмецчяуавчыфнэлкщмзмыхюхнйкйзэ
щйзхмйрмзмбжйкбххждщзлни
екквжннйзтычшмбшчэмпюхриошзэыррвьлвпхкеэгйшхжмсгбгхксчмезмщмеццютвзэмутмчэцк
эпнгкйыгщюмкплгмаюычзлий
тшгкдкюхтнвпхктчэгоцщюьэщцойдэшйщнбльлйзсчодьэецрапксграюмямпнвптмхфзльццатчб
июубушечйдяпвщйннтэжлел
жндхрхюцжьэхвпнгцююцщюжмвлиягэнгзэвюычэпьцтмзлхщюцгвклтзнгтммучкафкйбцобмчф
ббгфбщцриачдуоизйщмйзнйтэ
жмфйкэнггэяжвннипйсччяоисбтьфщзлращмчизлюхойэшпмсмнкяхкюриычилпйфйхйбшшхрх
рхцаагдуичрхжжбшрэбпямтмжж
нюдужэпкжэнгйздйыищюизьимчшцфужтдлтвжнтэикцрпмрмйцидеэзэцлогачжнзгзэжжжэбкйл
жмжэвлдяяйхкйлыццаээщюза
мклкзарижкеэлфебнглгугимжэймдчзлфуззпйтмсмээмгжнебойэгумрбгнямрйвйыишчсмаооцю
эчкечюхрипшсгвцтпыцяйэн
лизлюхшзашйцшзнкшоюцжзсмнкзмпнщйдэььмдсифямйтчбичцоцемозфцидшшщмжжквумсг
ычядмгргбуыцсгкйицрахйкрхюду
мхргычраюмжэсгизэйошжцебьцьйэнжтцажэяэзмэспзтцфужтатумээцргчжюауешнэшйсмоонгг
кыцгншчсэьгыцгвчкщмчецк
сифягнсмзйиццатчбиюубушееэмбщхдшбпямямдяомяртмпмшюксокзмймокбчтфкйписгьлюмп
мзйяхахдшоианкццлйзжлцнсм
жжщнклшйбцрасингтэхкгнцркмщйсгшчтмжжляилфщэмзмпмнютфнгпкйхрхзэкфрхоцпкчэнгу
злужтумцштчфбднейснюмгуыц
вгрхлйамумзйкрсмткйлшямчфбечюхдшгубушееэоибхычцшбйнкхйпицквшчшалнгьлсччюргри
нйицравэашшхцадэмгзэхещч
ахойахтмржзмзэбххжямхядяоэкрэхжнилхкллритмюмщвниьлвфбитчрхфмкыямухжнилхкжэб
шзйсгоцриогйзувахцашйяфеб
нгилхйбшшхбгкгклдхтвжншшфэдгпвшчюшрцбуклщмжэгйгншшфэцррgвфчэьэбрвэашшхэкю
мсгбиилоццнямшюычгшвеьцапфж
влпвйеэхткйлкмщйсгшчюмпйнгпйщмецшцрираймыгтчбиийьцьцфужтрунгсмнкцршйюмтцехр
хтээмжэжэтжчэнгйзтмюцрхрх
жжзэсгнгбхклдхюцдятмтэпнебэкжнтэтмикэнзкомярзйшйзэсгнгхйбшшхцнафббнйцксбтнтэик
еншцияьцрурикlвцщюшшсэ

зеэгеэбхтфьлюцжэсмшйщкукюмхбргчкээьтилгоычгнейеюриычогагвфсбнйжэюмярвшбхтфьлц
тцтшееэюцдяпвчккйжцриий
пйгйжэюцднзмбйфждэпмэмеирэнйкрхкчхычфккхяддшрцризэжцидгйсгяджжхжцрпбхкафцнм
вбгфгруцнсбьцрхсмвщжюдуоц
ришзтчбикшжрнгвнлнтэешскямхуебчяйецвумгэчэцрсиюссмнкяхфмжэейфйомярзйшйюмжэп
мткэняубушееэймыиьлйзймсг
цлэкбкщмеиансмпкпидудмстилгоычгнейумсгоцриилсмнкяхшкзбичбнммэнклвщцнцлатсмжвд
умезлзцсбэиргтэщгжнеэдэ
змьисйзэгшвкэцриийпйгйжэгэчуббосдэпйхиебшшоэухявахшзсижтдуьцебьцнввпсбкцгнсчжн
илилдязаеэямвннгрхтбиз
дэечапьлхйбшшхшзбшрэпиатрунгбуриклвцобднейснюмгуыцпцапцюизшйпмдмнйэвахияогсб
шйагопшчямхштчбифмцксгиз
лкдмтлсбльцдхмдсйбжщйсшщмярфжчхычфктмпнтмдмэмецобднсбьцебвубушееэюмпмдчогз
лвцтвргщхьлдудшафцкхцжнсм
ьтэерэеэюмэмсбаыямээрэгмржзцриьцжэлгзэчэбиушкйщйфжугрицншйжэбшлклиеэлккмйцкк
икхйяхрхюцмчцнейзиргжэсг
клдхрихчцнейгквнлйллогклдхимжэсчхяоингйзюфхйццсбултббгьцебдяьццтрувьфащмецпвчкх
йэньхиябшгцбузлчвдусг
чкнэцршшоэухэиямегмкфйгэсиэетбюмсмнйцксббхтфьлхйбшшхебшйсгюутмдэчэзтильэтьфяи
чжэлксгжжщмямжжкцапямяк
црвняпямгнцржэсинглдычмецюргклдхжткгзэгкцрюмгйкрзйччсбьцрвфбьцренгешгэдмшпцюр
июужтоияйейбрюцшйюмугог
злвцтвдшяхычфккхкцщюцадмйвчяоинггнэмнгщюгэюмибнгяпямгйяхмйзэпмсгюхрубиияшйэх
ешуцидзэтмэгумзвригншйсч
щюцллгкннвйесмтцнисчтбшчшшпеяпсбеэгкцрдмпйфрхййзлбилфиэээмрчжнсмццфббиямэмтк
нйтфжэнгпввпсбявргфбопям
внниахешчтьэщмьдяйзипйзэсгнгхщкйейцхщюгэвуйецвйесмгйсгфищйэзщюззхйцрйздмечжюд
эгйгкцрээошщбьлксечцнрг
фзюмцкрэлнуаяэсиебамсйэнгмиибгогфипйэчтфшкагюцбишчтмгнейсгкйицуыямсицасгдмэмз
мпмсгыцщютфнгпкгшжэпмбб
нгфивунгркгйяхфаиктмнчфуоцнгклдхимнчфбфжшэстофкиебюмгэчэлщзлрабхзлнгцнгйтзпмд
мяртмдннйгэсэярыйюпямгг
чяпвюцлгтмпйхпцнгйзмпкеэмшэнлиеббхопфжбктмэмбйзимвумсгойэйшйжцяйейтбыйфжшйб
блйейжэамукцрщцмдыхтнгэди
ебдмэсжжржафгэлкдэсмтмашсгзэшйцкоипймбзлхкыузлвнлдгйзмсйсцргщюгэчэтцяпцюжтдлж
тюузлбгфидйщйхжкйгйцутт
клретбвузлебкксчкезмбрржпмднсгявнйцкнвчкбшяжчэцрпйфйдэтзгкяпямржшйймдгднбббгрхд
яшшпепвщшпклкбрржсмяп
сбжшэээмжвчкумсжюмннтччюбгфгзэхшоимвьлкибгкнычтзхкямбйдужэафзэпмсгуаякжцднчц
ахткйлкмщйсгшчьэбхрищшйж
дццлйзсгмчюхофжэзфжэлнеэдэгубушееэбнтэтмжллнкнлкшхфбомпглкжжеиякжцыцюхщююцг
ншшфэентэхкошпмдмярсгиксб
ямхугвумпмцятбнйбщысгшсгнкщйцкшшпеемщдвууажмбшчэмпюхогчяйксйыгтвклодгввпсбр
угвргфбопямюцмдргвцьцфукл
щмргжлэхосшпзлриэххшдмпзейщмргэсхйакщмумгэдэсгбиззхгюмюмейцроивфччжьосэншйф
йяцтфсбэсчштхщюгэбжкйбррш
гкцкщгргтьцсбйеяйедргвцьцфуклщмжнтэйекншцяйукшйзнебтбймомакжэпкжэйеиубббгмму
кртяфюмсгычюцшйжвфбхьюх
щюгэсмсэйекнлиээбшэээмнищйэзюмокзмйминзирибгвцюхямжтагфбшйпмнэсжчэнгйзцкщгрг
гтшцемциыцййфцюхямыцяфжэ
нгцксйщмбгантэтмикшрйздэсчбибхтбокзмймкмиыгэхкжвьэямрнщйуквкюцриймечбгсмямхж
щнебпйфйжжзэькчэнгщкгшрш

ямцхямтэькфццнвкшйюмсиойюлдязачйгйбмзцбивфцнумецщэблцнжшсмямумщмжэаляпядчч
жьяйэнэфсбтмаемчфытсщлувкл
укдюхнщизаснеэдэзмециясжсмсээфсбэсюмсмсэщнфшпйозаушенишчгкейзмсэсгсыямухжнил
хкткйлвушмумнкзицнякикей
яржэбнтчфзкмьгоцостмсгилэхщкгмсммпьцрхумгйямщмафщйзхшмсйкрюмярфкейяртмргкйгэ
црцйнйцкдуэиоцпксмчэжжгэ
щцойлкцйнйкрдуэиоцпксмщцкшякрнлчшйашхйошямбцлгктиляхоидшлкнйщмкрсмсгмхдшет
лкоэаекссмнфыцгштмбхфбвэнб
рхбгрхдмфццнсйкыямдгзэжжййэйшйвнниеббхтфьлюцмчцнейзгрхлшсгвпямжэкййцьхтфкюш
шекгкулнишчжмбшчэмпюхчюжн
юмукюмбкшшхфжэпкршбйжэашбшькнюдуяжжнтэшйьнбтяфикжэафдуэиоцпксмикцкдутмжв
сййжжэслдязасмчубимвумсгжнбб
цнмелкюмллшезаейбхклдхриыфгвьэгклкдэагднсбьцфукльэлхычфккхшзгшвкгугнлгершщиеб
овдумчаххйбшшхгвкляфых
мчрэьикгжьилсгмчфбдуфжчулкицрасмзйнйсмэнейпццлпйщйвчшцксдэсгфягшккшинйщгчкаш
рэтхрвтвлгиукльэумвтилпи
кгклдхвпямймкйчеилрвщйжжщмецксеузлгшдэээомтэлкюзцрпмйлмчриафдмярейпйхпцнбйргс
чбиогфиясагопшчгнэшювум
дэапгнгшхгзэхшдмччкюжэюмэмухтнзмдмфхруядргогнгклдхтвахычшйаепвумтшшйпйдглйцш
гйтздмчиычезжцосэицнээяж
пводчэярфжьцебшчьцжзтмлипйтэхкдябужнгквигншбгввпейицщюривфзэсгэкхбмкбкбйьэцкпб
ыццющйюнпктэцрйзовшчхш
нмсйщйзрмэ

## Хід роботи

П’ять найчастіших біграм шифротексту

| Біграма | Частота |
|---|---|
| сг | 0.00814717 |
| жэ | 0.00788436 |
| нг | 0.00775295 |
| ям | 0.00735873 |
| цр | 0.00709592 |

## Розшифрований текст:

## Висновок

В результаті виконанні лабораторної роботи, було набуття навичок частотного аналізу на прикладі розкриття моноалфавітної підстановки; опанування прийомами роботи в модулярній

арифметиці. знайдені п’ять найчастіших біграм шифртексту. Було розшифровано шифртекст.