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

КРИПТОГРАФІЯ КОМП'ЮТЕРНИЙ ПРАКТИКУМ No3 Криптоаналіз афінної біграмної підстановки

Виконав:	

## Мета роботи:

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

### Завдання:

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 No1, 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 (а, b) шляхом розв'язання системи (1).

- 4. Для кожного кандидата на ключ дешифрувати шифртекст. Якщо шифртекст не  $\epsilon$  змістовним текстом російською мовою, відкинути цього кандидата.
- 5. Повторювати дії 3-4 доти, доки дешифрований текст не буде змістовним.

Варіант: 23

П'ять найчастіших біграм шифртексту:

Опис роботи автоматичного розпізнавача російської мови:

перевіряє частоти двух найчастіших літер(о, е)

#### Шифрований текст:

дплргшрщзчфуилшччьолрхсжфпцнбтйяэзьзншпзвлплщуфонубинптщьаьчжлсзбцдщзчпжйргбсхфэчвездусззлгудудуэедх тярхездуежшэфхшуфхцппшлхтрфхюхдпшгташкнжрэокфхшруздуушлушудойгтфдхуртзлефунптцзчжлдцвзоюэтфхфлаэзону згтфйинпшэеьшлрбнладнптщзчщуьлдщзчшгуомээаээээябрипьеуггбилцчбжрщэнзуфонубиязйэщйбиэхфчугвздуокйрыю бдбжикамэрцэьгфхнхзшщюбжллжэщэйхщхэлмхизязеэцэпжлряхщхбрыгбрцэтщфпихпхвуобзэргллрчугвэдуфущухлфетжэр рэоьейпжнуежлонусуфуцарголжчцлжбккеяолбтплщущэвмфхнджбглюлпблющзгнчоргзчдозэргфуруюдрхыедхфудоррлойя окзчфхчявчшжочбяелуэпжхпзядхсехескпзспщйбжсэтэрщаоргллрчугзягужблтжбэрэлчзлгуофхяхщщипугдвпладеьчрвм ьруозчгунмбяпвокрщеэрящлиршкшлбруоежжзядоюшэьчсздхфоглупшгчоцхоюьчышйькхдхамфжуобтдхюххескйрзунхюлфх цупонубтргфужбзэщзнубжрхолырвмьрсодуькйрээялжэбжщюуосоумьчюхлхжлнучэрщбтргщхчьяойзплцупрзэккпзнуожщю уожбаоргсоумоаипшгпшцумзаохйрхолхкнжрэгнэрлуцьугеяежмпзчжлеюсуугпшйчсохэсууггбхлрхвуппщйвонудщеэсюмг тфлэдцжвйялзьудоллрчугнжрхолчэцкнжмпхврхькшгипщйчвюлщудочонучвокнжзумздоиеызмбаоугллхкпзрбчмжфихгуфл цлхбэтээфцйчгбяйоаячшувумлурргрхплхехкфхнуюэшгргшекбамшэфцчвцчэтрхэефбккргтбниподеуггбилрхязурнийрдц мгглдоээзуюржевшйржеяейицуьлнгюужехлэрээйрдцщзчэшкфхсзвэвзихелызфлсуяззюзээянюэрцпьчээпжхуэйбжрхолыр зэмгтфлзжзвчеюжфбэоаьчжлльдэыюпздлмуэгцншэеьпшзчфуилцумзрхыглэдумэсзжебжээээдщиюмефуцхбжлэфуубпжээйч аоухрээяюлщудочонушяячаонушлжэпжшэщзнунптщеягудхьлвяаэшэьгбрцныврхплжбьгзчгхфэяисзжерхыеокзчфхчявчцл фуслюэсобрьесзвяугжздофхеьзшллчяэзьздуькйрылоьйиилуонуэяьлрхгшзчфуилеьлзюлщудоронуалькйчшэшзугвздхур хэпжнущгьчипячгбяйгбвмшгугллэуюлщудочонучвфуфхмлябтщээфцглвуфбдцглхкйрзуслезтэртугллчгашпбуозмвзплих доикозфликинжлнылфуьздхикшгпиелчэвоцлэзьзшпьгкгзчаьгхбжаооеячмээлэглонжьрьтэлеьлзокшлйэллнусэрлсэгуцх юлндпонжвудоеяфлэбйчфбзозчжлхеезфэдвлшаопбнжрхэуилгхидрхвхкхюопжфпчоцхпладзуфуязхчугшгцпээзэхзеэйчфе кхгхмхурвзшпшгюуфуьзязруячшярхпжцпушнлизязеэзэпжлряхщхбрьгбрзэтщфпяхпххуфхяупзфлглгбшчцпежвонудщллжб зчмпвмрщйчшууэнюзудоюизбффчябашэзудоюигушулуфмыпцкгбккфплззухзжэцрчззулзфуфлщхгхэулуезндгуьабжеэшклу плгхцунхдсшуыжфпчосзеэы жэчрдцдвмайчугшгцпы жбтцшэглйрытккфхнурусефбккоэфлячгбяйыггбнирхязурнихунуйр дцмгюзфлглупфмшгюизуеэзэбжрщгхрузлядйяцкцкфхфлокйрзуслябтщшгэглльшршдхеэффзэьчгуадгуюлвескгбэрюоежшу адгумзгхгхежуоылямфпгцоашуфьйидлядбтрузлядйяихфлдэюурхшумзлзруьпйчнжлзцхядйяжкфхнуэзчлвхбждвгуюззужб пшщуоэдвруулугеурхлнэнцпыгхеезэгвзомгхдудусзуэлвчопзшзаэлвлюйчшзпзвэюшффээццзйкзчжлшцежйиязбфнлпцпзкл ргзчамшэзудокфйчнуищпзклоклуплгхцунхаонжмоамеуаклудомпбтцчэтщзялдхымтллгжзюлчвькышдвдоьлцляайчжлдгхл жэглчвмхихщуидмоамрщшпщцчохзрузлугшчшудувэзшюшьдгбузьюзяаолудошгртргькнжээзянптщйрсбеьзгсщбявэвофцяч рукбипрхгуфзуедоеявцяирхлзьзокьакгдонуцхцашуспрэдщюуцшйьщуидмоаоеэшгвзсэсэнжмарголрэдунужбзчаоызэзчм жфяжзудоргжздугэчэршцкгбьчвхткпздчвхдплоччнзлеюоаодофхиэлвнужбзчихозошозлегушуйьекпздувхдпапйя бжкгжэпзиллэцчэшрщтфзэлоэяээшэсдихфэфлгчфрбялэдулэмбвщежнужбзчнжээсуугуонжрхжбнюфлэгцклулхжбэрдоьгюз флбжхзшпиццпзлеэячпжзлсзбэташупэйзфхсщшгпбвачоцпзлеэмпрежэьгцпжбцкйрщудоыльзлчоьшпшэзудоепюрашяиеэлз люйчцпйямхыкпзуршэьчжбфцргцпжзюякфоздуупцкьасойиилгупрыгжзвхбшфхцшлллзкфсздозузуцчфуюлрхюзмгшулгбрмг гушулурувгбрипхэжкэчюзвэывфхмлцчьчнжлэфлнэдуячозихэллэфушулемоюурхаосзухгхрхнужбэчгшаопбйзжбэрдоьгбя злидбжцэцкаонжмашужбэрдоьгюзфлсулзекгбшэзчмпвздугщзусзоэшгмбвщяиэгуофетунпйчядхеезфэдвязлоипхэзчжллш аопбдвлзруьпамзозкфхнудумпргээшгворщшгамгхдомшфхвуцьмпфмьлспзшаопбдвдоллщухлядмхмхлмфжгбяудокючочваш зяфлжбэрдоьгбягхидбжпущщшгпбмпжэьзвеокшчмхооюшдвшуамышфхмщэчьрсбдонущйсбтхдуэедхфчугллэхсднукрпиээле фуоздояхеэьгозфхжпзмвегхидчэялжбзчмпшкшлэтвоылапфмйихзээушшуфлгупрээмежэдзпсшудухещхцуактзжгжзвхяюхз крмпнудньчугаоюшмзчэрщцкмпргипуемзжбффвэяизбйчжзрэвеоюкфндфушулемоышлуфзэзщайчшггушуйьсуаклунуилфелу

дошгртрхьуфьщужбшгйрчоылзчвхадзумгпзчяокшлльишглжэюшнждоцхнрипзэеьяллгруашсзлзжбсуьузлрудппшзлдщышшу июкффлгушуфхюфлтцхжлгхдщеэшгфушпэрлзмгпзчягупрйчэзвофхнууэюкшлэуилзлцчумфпхзчмфпхзкбмгщюеььчфеклушрщ дхкрпбшгтзрхвхолдоцпцкцкфхдплоччцлеэшкгбьчвхгхнубмлюдхядфэбжжбнюлзоакгдонуьзпзяпргдвсхщудоглщчвхщушг гхязцхядцуюзялцуюзшэккеэлозуэрбялздуьзькышдвдонуеэеецчугшгцпмоаоцкфпщюшэщзлшаопбнжеэрхэуилгчрэбжрщщу жбйрфпсхядйяьумщьашурхдоикдзцшвойчкбрылрфпмзрчугяибхцложшэчойгсидщщюкфндячлзэздкшэщзруцьашргцпнуцчбж жбкфрхрлюодвжбчмзлсханчвйямхвхдолудььдгбсмыпюуцшйьшуйрфлюлбмфхядмгщхвузуцчюзхеанхзльсзязоэвзкфшкышцп окпллххузэрхцудушпшгшклулуоздонуаозуплэзадзурхфуюзеэзэшкячьгфуюодвффсеззблчбпжячщуцхльэуилхашуэеажцс жлщаячипфхфэвоглмоцкфешулерхфуюзеэьчядшунфсзедышаопбнжжбэрашффээшгшкышцпокплжэфбнжуорщеэшкячьгфуюодв мэффсезэшпшгвовэдоэкпэяэчшаопблвфьткфпщюшэщггбещгхдугхжлсээлмхбтжпхэйчяжщхюобтчлжээляуибыюпиелэуыяяд фхфэвоглыадщигртйрчомоцкпзязфггхдоээшкфпсурхрхдоикмпэждухелшаопбнжчбзэоеичгулеежшзфхшужеюлвещудудхжб эрашффзэщзюоюуозндфуфхмлщуьдгбнлеэухдотфлрьгцпжзьзнужбзчаонжмоллфзоэцкфпщючожбэрипдпйчжлщггбловздохэ шкфпсурхээауйэшгээглээшнояляуибыюшэывшпшгблчбпжглльчлшпшээяюлдосбцпйярхоохуугуорхихфлщхвцывдщшгцклуьк тэтэшкячцпнуугуошэцешуугцклувурчозымншльзуэеаждйиыжгртйрмптщпбффьуцуадезмпежшэгцуохуилшбффихфлщхтчес жлюлльчлшпшээяюлеэрхвллхгчнуялчяэеаждйиынощюэрцппшеэмгщцгхеэкффзфлнуюырщфхуллкзчвхьлигфздоцкшлахьлтк шлахьлзличшэккфпмацпмзгхбжрщпбжфжпрововоршдхбжикшлчпшгдущуиемовзмззлфьаосзаэнлашнжлвнужбзчкфюшйиухгч дгдщллфзфлшунуугуошэккпзфзоэамыпвммэффцхрхдщеэдйхурхадзудооуоэшкячцпячьааяблчбюкфпмампшуадгуфыщузлиэ бттфрхухуоуозчижвэпшаоибвэфьщуаорлвешужкгбэршишгнжаорлвеноьазувхяюэтаоцллэжбыгмихэвзьдгбфуфечлэлашнж лваосзкбыгзууохуцшйыжлисшувфнубэшгцпвздумхбшюшдвэгюфюифыцурчвзиллзрчэзлгипушежвуфыжлбжгушулуумыпцкпз дчмхихзуцхфумхзлючячсуоэжфрхбэюуоэээпжээсоцэмеэечэмпйядсшухчфямлдщфпфмшгмшлудошгдвзэжлобячаэфцьчугщз рхфуюзеэюшнжуонличисшуэжьчэзьухюзуфьщувурбуоабфффхмлядйяргагьчжлдшллборштфюшфпьуцхоэрщеэташупэрщнжзб пжэчгуцчрлхкшлльозюггушуйьэудакгдонуцхгчумвкюзлзоэфжокшлсздощздуюгипушнжикйрьляергипушнжшчухдоеийх

#### Розшифрований текст:

владыкогосподиуслышинасмолящихсятебеукреписилоютвоеюблагочестивейшегосамодержавнейшеговеликогогосударянашегоимператораа лександрапавловичапомяниправдуегоикротостьвоздаждьемупоблагостиегоеюжехранитнытвойвозлюбленныйизраильблагословиегосоветын ачинанияиделаутвердивсемогущноютвоеюдесницеюцарствоегоиподаждьемупобедунаврагаякожемоисеюнаамаликагедеонунамадиамаидави дунаголиафасохранивоинствоегоположилукмедянмышцамвоимятвоеополчившихсяипрепояшиихсилоюнабраньприимиоружиеищитивосста нивпомощьнашудапостыдятсяипосрамятсямыслящийнамэлаядабудутпредлицемверноготивоинстваякопрахпредлицемветраиангелтвойсиль ныйдабудетоскорбляяйипогоняяйихдаприидетимсетьюженесведаютиихловитваюжесокрышадаобыметихдападутподногамирабовтвоихивпо праниевоемнашимдабудутгосподинеизнеможетутебеспасативомногихивмалыхтыесибогданепревозможетпротивутебечеловекбожеотецнаш ихпомянищедротытвояимилостияжеотвекасутьнеотвержинасотлицатвоегонижевозгнушайсянедостоинствомнашимнопомилуйнасповелицей милоститвоейипомножествущедроттвоихпрезрибеззаконияигрехинашасердцечистосозиждивнасидухправобновивоутробенашейвсехнасукре пивероювтяутвердинадеждоюодушевиистинноюдругкодругулюбовиювооружиединодушиемнаправедноезащищениеодержанияежедалесина миотцемнашимданевознесетсяжезлнечестивыхнажребийосвященных господибоженашвнегожеверуеминанегожеуповаемнепосраминасотчая ниямилоститвоеяисотворизнамениевоблагоякодавидятненавидящийнасиправославнуюверунашуипосрамятсяипогибнутидауведятвсестраны якоимятебегосподьимылюдиетвоиявинамгосподинынемилостьтвоюиспасениетвоедаждьнамвозвеселисердцерабовтвоихомилоститвоейпора зиврагинашиисокрушиихподногиверныхтвоихвскоретыбоесизаступлениепомощьипобедауповающимнатяитебеславувоссылаемотцуисынуи святомудухуинынеиприсноивовекивековаминьвтомсостояниираскрытостидушевнойвкоторомнаходиласьнаташаэтамолитвасильноподейств овалананееонаслушалакаждоесловоопобедемоисеянаамаликаигедеонанамадиамаидавиданаголиафаиоразорениииерусалиматвоегоипросила богастойнежностью и размят ченностью которою было переполненое есердценоне понималахорошень коочем она просила богав этой молитвео на вс ейдушойучаствовалавпрошенииодухеправомобукреплениисердцавероюнадеждоюиовоодушевленииихлюбовьюноонанемогламолитьсяопоп ранииподногивраговсвоихкогдаоназанесколькоминутпередэтимтолькожелалаиметьихбольшечтобылюбитьихмолитьсязанихноонатоженемо гласомневатьсявправотечитаемойколенопреклонноймолитвыонаошушалавлушесвоейблагоговейныйитрепетныйужасперелнаказаниемпости гшимлюдейзаихгрехиивособенностизасвоигрехиипросилабогаотомчтобыонпростилихвсехиееидалбыимвсемиейспокойствияисчастиявжизн ииейказалосьчтобогслышитеемолитвустогоднякакпьеруезжаяотростовыхивспоминаяблагодарныйвзгляднаташисмотрелнакометустоявшую нанебеипочувствовалчтодлянегооткрылосьчтотоновоевечномучившийеговопросотщетеибезумностивсегоземногопересталпредставлятьсяем уэтотстрашныйвопросзачемкчемукоторыйпреждепредставлялсяемувсерединевсякогозанятиятеперьзаменилсядлянегонедругимвопросомине ответомнапрежнийвопросапредставлениемееслышаллионисамливелничтожныеразговорычиталлионилиузнавалпроподлостьибессмысленно стьлюдскуюоннеужасалсякакпрежденеспрашивалсебяизчегохлопочутлюдикогдавсетаккраткоинеизвестноновспоминалеевтомвидевкотором онвиделеевпоследнийразивсесомненияегоисчезалинепотомучтоонаотвечаланавопросыкоторыепредставлялисьемунопотомучтопредставлен иеонейпереносилоегомгновенновдругуюсветлуюобластьдушевнойдеятельностивкоторойнемоглобытьправогоиливиноватоговобластькрасот ыилюбвидлякоторойстоиложитькакаябымерзостьжитейскаянипредставляласьемуонговорилсебенуипускайтакойтообокралгосударствоицаря агосударствоицарьвоздаютемупочестиаонавчераулыбнуласьмнеипросилаприехатьиялюблюееиниктоникогданеузнаетэтогодумалонпьервсет акжеездилвобществотакжемногопиливелтужепразднуюирассеяннуюжизньпотомучтокрометехчасовкоторыеонпроводилуростовыхнадобыло проводитьиостальноевремяипривычкиизнакомствасделанныеимвмосквенепреодолимовлеклиегоктойжизникотораязахватилаегоновпоследн еевремякогдастеатравойныприходиливсеболееиболеетревожныеслухиикогдаздоровьенаташисталопоправлятьсяионапересталавозбуждатьвн емпрежнеечувствобережливойжалостиимсталоовладеватьболееиболеенепонятноедлянегобеспокойствоончувствовалчтотоположениевкотор омоннаходилсянемоглопродолжатьсядолгочтонаступаеткатастрофадолженствующаяизменитьвсюегожизньиснетерпениемотыскивалвовсем признакиэтойприближающейсякатастрофыпьерубылооткрытооднимизбратьевмасоновследующеевыведенноеизапокалипсисаиоаннабогосло вапророчествоотносительнонаполеонанаписавпоэтойазбукецифрамисловавыходитчтосуммаэтихчиселравнатиичтопоэтомунаполеонестьтот зверьокоторомпредсказановапокалипсисекрометогонаписавпоэтойжеазбукесловатоестьпределкоторыйбылположензверюглаголативеликаих ульнасуммаэтихчиселизображающихопятьравнатиизчеговыходитчтопределвластинаполеонанаступилвмгодувкоторомфранцузскомуимпера торуминулогодапредсказаниеэтооченьпоразилопьераиончастозадавалсебевопросотомчтоименноположитпределвластизверятоестьнаполеон аинаоснованиитехжеизображенийсловцифрамиивычислениямистаралсянайтиответназанимавшийеговопроспьернаписалвответенаэтотвопро сонсчелбуквыносуммацифовыходилагораздобольшеилименьшетиодинраззанимаясьэтимивычислениямионнаписалсвоеимясуммацифотоже далеконевышлаонизмениворфографиюпоставиввместоприбавилприбавиливсенеполучалжелаемогорезультататогдаемупришловголовучтоеж елибыответнаискомый вопросизаключался вегоименитовответене пременнобылабыназванаего национальность оннаписали сочтяцифры получи лтолькобылолишнихозначаететосамоеекотороебылооткинутовпередсловомоткинувточнотакжехотяинеправильноепьерполучилискомыйотв етравноетиоткрытиеэтовзволновалоегокаккакойсвязьюбылонсоединенстемвеликимсобытиемкотороебылопредсказановапокалипсисеоннезн алнооннинаминутунеусумнилсявэтойсвязиеголюбовькростовойантихристнашествиенаполеонакометаивсеэтовместедолжнобылосозретьразр азитьсяивывестиегоизтогозаколдованногоничтожногомирамосковскихпривычеквкоторыхончувствовалсебяплененнымипривестиегоквелико муподвигуивеликомусчастиюаа

Ключ: a = 735, b = 300

# Висновок:

В даному лабораторному практикумі я набув навичок частотного аналізу на прикладі розкриття моноалфавітної підстановки, отримав практичні навички у частотному криптоаналізі та опанував прийоми роботи в модулярній арифметиці.