

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Фізико-технічний інститут

# ЛАБОРАТОРНА РОБОТА №3

з дисципліни

«Криптографія»

на тему: «Криптоаналіз афінної біграмної підстановки»

Виконали:
студенти 3 курсу ФТІ
групи ФБ-72
Топорова Варвара та Лобанова Уляна
Перевірив:

## 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  $\varepsilon$  змістовним текстом російською мовою, відкинути цього кандидата.
- 5. Повторювати дії 3-4 доти, доки дешифрований текст не буде змістовним.

## Результати роботи:

$$a = 314$$
,  $b = 34$ 

Щоб відібрати саме цю пару ключів, нам треба було відфільтрувати розшифровані тексти, які мали заборонені біграми, тобто ті, які у ВТ зустрітися не можуть. Для цього ми створили функцію з такими забороненими біграмами: 'аь', 'оь', 'уь', 'еь', 'ыь', 'иь', 'эь', 'яь', 'юь', 'йй', 'ьь', 'ыы'.

### Біграми:

Відкритий текст	Закритий текст
на	<b>э</b> э
то	ВД
ен	чф
НО	ГН
ни	ПL

### Шифрований текст

тгтгрэцрюфмнйбмйшугдээдэибггэдайжаишуикггуоитлчмтлвшаэвмхдвдлгцчцмбпврыэггзухлураятаиэншчфэчучкштфьэзукщтбцнчфвшяфнрагрэцрцлцэюоксбмчф цгссошпруйедйгцгрэчсммцлжлочщетйсегрхчяэйекааэндвдэчбоцгзгдэыуирщцээятглпльчкчедйгцгчдфэучюшщясеплэнйфюфюбмйячвдогяфруопогшэпбмйячюоаэ смплизфрюбдукжюдээщшсвурятаэггшйячбдйгьойсегммцшмэцгпмкаурюбщпдуяфйшлнрсээпблвтфцшкуцншмймщяээжсшшщятгдэцгчббйядогцоцггнвриэоеканы клгнурюбдухжогууэчцдябдайгогвшкайгогошплфдошплкуопогруопчсопйчяэаэнссрелуртукжэсфнйфгдэээсглкчрзяаьйемщпмэумвдкгсгнчпщвшзэалжвурдуопогру опогруопогрухсопогбггнчфьдечхшюбнргдфпчбфэкдчтйгйщнрдуиээдиэвнчфщзгрвштфвешыэшочйшяаяффдкчвчтшаиешшившэдечлфюфэнветйячыяюшмэсдггсна яээюгсеелфчкпогюггнодядкчешфчывээечогьоуэучжоьэхшгчэйжутйггдсэдшшветйячыяцгцлнрэсснаявштэумэтогжлэеблэеишлтдгфшврхлячщшцнбйесгнфртййбмй

сстчжокгпбфэцрюбдувешыючрэщмбйетьдцчкдээпбцдщркжцлураяючржапюфвштэчяьорэтлурюфнрагкдзэцгрэтлурфчычжлиекаэнчфьйзйлуирсмчфцгячьээйуиаг шйдрйшиэпувдюшшишаыэмсвдхтгэкчьчэйыпнрмйчсартйфдчстгщшаззйрэыэчйхялуцшдуопогошзэалжвурээыунрбдяуэчждэсетьдечнпзякяцгггпмэтссхбмйячюоцг дэявжкйчггедоддэявжкаиягячеэюшуркйтеопечкгсшцлучщшазелурчбезвчпмцлуруйячэрдшртклуйлрфмйшймплэеггдбуйишртгбцшнэгтждтхуэвчээгтждюгэдссмм юфябцнчфцгфэзшмйсссшвриэяэчэсеплэнэвээятрэаржуснцзшуснвдцэюоиэгмкаурмйцзнрушдуэчтоэчггаувймйсеябчфцньэцдогцояфюфтйкгюгогрэпутфээпбфэпут фаярссгжемйээрэврзюйдечдэллцявчяаиечмбэкдрэцрябмйэшфунчгфшйтеюнтйугюоибдуиэнгждятгльчькснтбитчйэчувюдгнцчыэлгвдфечфучжеуыкчяэьйусигджуи аяьожчвшлухжвдгэопогылэеэсвдлуэдэсвдцорэцгжехлвчкдбмюгягшшчфбэреапопечээжечбитогенчфезфрюйэчлмэсглсгвдугггждцгврзюыщкдкгюдфбцдешймплн дешйшуйэчлгкджлаыэшьяыэфпечрэюгеджчиюуруйогцэмйэчычюшдчялкуггетгмвшеншигнвевшзэумшутэкдцрйшкльчькирфпвддбэнушмэучжолвэшйфиэбдяучфз снчгнуявдшчпэфшуиуйягвдюбэеяукчыээээтждээнчячщшнфйшймэтвчимыщьдечвдэщезюнэнирхджбнряэаэзгэчвдэчучкшзьшчьччсыэфпечцгэчггауыщрэпмцдштйг вдкгучвдйэьоятцньюятчучфтйкгюгогтгтгвштйндтгогьйьэуицэюохэнечмэечмлнчфишмбмйээпуяищшсннрфмдуезггьоаягэрнщпчфурэвэжюдчсччусцэчяьогтччхштэй эссвшщзцлфчюрвууиьйтффедаюнчбтйиэгнушкмээкчешфчкпечкмщпсгвштуйскбуяэдэйслцнэрдшбййббйьоээюоыэчскбцдечфучфширчяэлгыэумнрлвдлюмлсечиб чфкдьовшябфэцрхчычялиелгвдячтчтогнуявдтчцчввэертдйфруцээщштфьюыэрзюбядгнпмшипчлмэдцгопфсучтчайтеюнбпвчюегмьйцнкчдгяэтажюэеыэшоашсвйш ураяплггйнчфныжвиявчяэцнсссгдяэсаэкгцгвдюгпдвшиэвнйсцэчйфшцлчдждвдгнеяждчслшнфцлогбшнфюгягйэдйсрхжртбаирэшлщюгфэщруиплггчзгрчдфэюдщдт лфруйетчэубэеэеяауряэфэедтгтгьйфпсгяэьэцдогыняцээлукчонвштбфэйэедмтяуазцдзсбшлвььсштфвравччмзвджмвштбдуйэедьоцнээяэынвежучфпчлмплюйтеыщ лунрбшьзчетйьчшнюйдшцнчфдльчггршезгршылныэнцээывтйячщшщяшчсчедиэяэщпвшфмтэцгкгюгогцойэаэшшшимззйрэвчешшиггтлурйшшицгсепьплггнгээшся таэьйфпдузйшнярснвшкдучяэээцмчфкчешурмйжчянуйтеыщысщгьчдфэеьорнплмйыэйгемчмогвяыдючвшэдечвчклччгнярснээцузсжчцчяэжекуяукжкгфруыурипф элсээзшмэфечфртмсягджаиойтеазшчьфнрршоилуурюмаикдыэцулзнрзжээюшзйкгнчывээцггэятьойэфэчдпфурэвкмчфкдыэцулзнрзжэшазшусндбвеюнюэрэвдядю чдфэеьорночяэтгвчжокгойзйтеэшкгдуцггуцстечфтфщзгрплээретфойтфярснвшжемйэсайжаапзяэсглйчыэитшчюорстэцгдфцнцдибыядэцгкчяэюггнелчдждщртбнфу ййшяфбпогюгждюбцнчфжеэжвдэьедискчщрхчклтгвчжоыэгбвчячиэомвесдямзйжчянрцээыэцутэуфзйвюдббйдягнуяглдавчйчгтшэыэяэгнврэвкмфдтуйскбвшпрын мэцгкдыэцулзнрзжэшазшуснссэйлуснушазшусндфояьоаяфрябогкгьохчшсныэшазшуснгэзгшшлвээвшиедуфртйуштйэчпцээмзгртйжчянадькзйжчянрцээчсччуснмц нвеоирэщмгглтйгснаякчэдедьмшиябыяучэйжакуэеклеяждмзфэедибмэсеопйдгтндсгснйекафрлуйгипдужеэщдуюнхьсгнцээкпведуцгрнисвдхтцуклжвэеюфцльчцу энтфиэынезцсшдьончыкйшшаюбмйвчшшхчтебпдутээсшдкнцчыцээдфэеьоиэьчцвтйсстштбфэгнмйжчянблрншивчтшуииэудрэьуурюмяфлаэчзуюфйшишфпвекачф цгкрчшврпльчынмэкддбмнурэдечвдщрлжурюгьйкйьэцылажоуэааыщвчятйгайрдэээсаэкдшэцруйтецнпггглаыжапурябчбфэээьнишиэмсбтягюшшиычмштфтечбй шючрэеззйээфэртусгнвемйогшэкшщятехлфдршуифечфыэкчмфнрзшцнцчигвдылэеимюнчфрэщркжиэчччаюфэнэеььцэюохэбщггмешижеюмггошшифпдажкюнкдп ччэальчяэылснэнймтуьэтфвшэжвдэжвдцлцнмйлгиээдвдцоцгзгдэьмггююцлфрлажюхдплггцаечцонцээгбфэяггнябмйцчедучкшшиагщэяттуйсяймйцчгэээудаэцоьй жвфпмэюшкмщпсгкчшацгснйштбшижчальчыншыцлсншччтжчюшочрштбфэаржуиэвнэшлуэеклачюлшукжвдьэыаюбыщфпкдэшьяхляуюэкддфэнэеььзузйюйпльчд эшшхдйчйскгшешыюнсгшешыюнтфцштблвшуфрмйушмэывфпчфюфхляуцзнрзжзйфрушйчмфкчйчяэкчныирхдвшэншыжвдлгнпсснрнцшысаээдшсясфедалндааээч ычжвээюглгфрмйинюфршлагдьчцвтйгтрэчаснлаячщшцнщацгудифшыиэгтгггнхдьйэехлиэкчгнэнюйфрушнфешсвюнгнэнблеемйитэлпльчкчлнржэшхчешсвюнзыла кдкчибцдшчндигкчзнймшицгечбшшипдлгечвдынбсгнуяогятжецнцлцгжлбппьыдййгсщгшэршлвуйчфкчкддекаэтйгвдфпчфвешыэшочршплюэцэшпаэтфкщнрдучф яэхрпльчршлнцдрэйэаэечаэрэдбйштбхжирдэфэпэвчечкчвдйсюдйшщпхчшстуйсяйлгаэлвэшхаззыэээзшплиэшоцгвчячвдьбфэцрщпдуюмлзтопмаиэчячянймьэээиэ ындацгудпцээавтйьоьйрщэьечомяылтцвирплюмдройазоэедкчедийалэшртнштйэчячдуйшяуйшгнэчюшоизгпбмйаззйцчедэчвдыэяэщшшызйалкуйсбдкрвууицльч цулзодэйслцнкгыйуиагошшаймцдудуогнишржхайгьоцгрэдэчоыэшскгыэяуирцнйфюбщпаэядалдуиэспиээчжозэшшлвшуплзкиэиряуэшвкйчспиээчжойдьйюмвшу чиэькяакунряэгэггшйэчлгюггэнпдуцнщпгмймрэвдпччйюдэшсвэсибфэосштйгьоылодждеэцгцдкгждячщшюьгггнцчьэнчюшюьтечбйшрсйшишуиюгксюжюнычшчжо рэшшщпюффрвууиыээээтклдфшнэшхдюдэсэйдшюбчфакадсгнчзйвдвшуйуиаггннрфмплчяядгныщдгнгйэзназэгныцгэчкшцнймвшодзйьоячщшоижемзшидэнчфаы щвчгнэсьоюгтеуйюмцшлтуэтшшнтсячюяьйсньэлузйшнярснаылажорнмэедиэучгньэршяаюбиэзэумэтядзэмекжфрмйушэнчфймймшэсекжюнирушоишуиеуэаакуф эщглфюфэншызэедиэкгнцссждэсссуикчучяэцгечшнюйдшйштйвяээгнцзггкгкдцгюгыдссэьюяыччйтфадкдцгыэийядсспдкйочедкчюшлщанэнплкдцгрэвдпдмчншю мыэшсезггядьоаясечфзйезгнэчюшщпмйэецюбгьйэецюзйьэтфвшишяиечюрэжушзэгэвддэзэалггычкдйдгнггмлрнмфйшлнмбэеяукггунфгнодэйьэшннрфммйьэжак усвфдкггуоигэмыэшзгжчэержюнинвйпльчдэедубшиждрнвекайшхльчцуэнчфжещпаэядцмчфгмюггныяджаиипвевчябцдщгайемтгячцдяэдбдуйшяуяиуимфэеснйф нрфрвшкчечогншюфкдучяэсрхщщпчбюбюбцдечэйшэмеишьяучцчовтйхчщрлучфишкмщпвшазшуснтгьожлйшвртййбцнфэтдямкледрсйвжкмфюфетюгчснгкчцэчй жуфэщгыдспнрмйчфпмкаурээдйкдщштвфпвшзйфсудаэцоетюгкчяэкчцэчйойкдщштвфпвшзйфсудаэцовшьйфпсгьэтлггигснаярняфесячспнрмйтгячцдтлэширцнцгж еьыэшьяойээггэпплвефрфчшсйэедшеопшигэфэяэншяцяджегмзяеттфурэвэжюдьйэехлиэвчдстшюбфэаэьмщпсгкдлсбовшрэпуснсссгмзнрзжэшклэекчэйззнрзжэш клэекчэйбцээдэнчээешсвэнэвээопдуиэмедуыпябцчгнмбкдюдьотгкччвтйтшоищравяиапогршочдфэеьодуйшьэьйуиьйирэшиэнштйэчячждбруэтнймэщяэфэедччю дсмяыгэонймнчячщшцнймнчдуйшгмгмяылтвнймнчцныйфпмэтержэшсмяыгэдйьэисщгбтуйьэюняиртжевшсдячюортяазсртршдчтлчмуйсеябюдьэифшашмецядцп ведуэжюмшчпйэчлгиэшэщшшызйалчфячкчжгкгыээшзэюятшочкчрэжчкшочдуйшлвзйальгкчэчгэмтзэреаптвээюгзгбтйгфнкгжныяьдцгндешблрнэщяэфэедммыщрэ иэагдэцэггудйгснаявчечпяыдшсщгшэщекамфбйтфачечдядйаггнььшэьйрщгнвевшфедаюнжседычяфемцнвечфбйжчянйфэнюйиэйгфечфыэрэтлурхлячщшцншуопо груопцлшеопезюблвдлгньэйгвдынцнмйфсудаэцоылэеимисдэцмвдгнурмйпльчонэщмэкдкчешурынезелфчзнймщяядчдцгшчдбцчечюоцгззяалтчгюшщяядчдцгцн учяэюгдэявуруйэчувюдцнучяэкгкгбцээшсжетвйшюбцчгузэкдкдыэцуишысдэцмурйшкмщпсгешсвюнешсвюньчцвтйынцнмйфсудэйемкаурмйюэреапцгжеыпфчэйь этвэерттфлжхтузйефчальчюяьйзйфрвйчяыдцпведуыээдзчафцгщшщпхчждвдьэсеопэчвдкгшнэжйшюбфэтдлгюшлщфэшэшрзйпллунрйшйшймэнелпьыдййемймж емзшийэлфплцузйезймлакуггжфвелтьэфнцгфсэсьйойезйеуртйюйячкгогцогныпцлуртйблдуэсээимгдьйюфчфьчмупчядчдртятвдвшяфюффдээзлцньчцвтйьдхфйшл навээээшравюнаяынцнмйфсудэйойэчувюдьйтфнрагфаэчзувэесгнфруйинймкджмлвээкгнчэйшбфэдякдйсрсйшюбурсюышмйлгкчэйшбданрцнфдяшзйучгнхаэчзув шаыиеюдюмнрйвхчьйэетйячтекалсчгснядчдцгьйзэгнцчншюбыянчюшуишылуишхчхщкгжнтфиэесгнчшиэкгфзэйжерьтшодтуйсцуурюмдуурюмдатэреапчфяэаэаяз узййфюфлумфюффдошплюфюфюфолукжвчщжвчщжвчыфагэйдшщпцлячюшуйртунахзяфбдуэсплггнгвщхщцнчфкчнсэйшнфэтфурэвэжюммеэнчсартйагхрцлшуж чкдпывшчгюзфплнйэйэжсфаэчзуелтлфруйблэчюшээзшдузйшнйффрвдвшплныгрэнроговдээллдяэсвдылодфэвмуйэчувюдюггнцчыэлгвдячшшцнтээйссягогуйесн гюшшххжиеыжэшцгжааэмшшяцнгнмбфрюбцнэеслюбтчядаляуюэцгшэьйтфнызйезггогцорэндэдьоаяцлшеопуилгйпйсцэрэжчдгвдкмшпсгячшшцнтэжшитэсогээз шплнрцгьэретфоэюрилфдешйчьэешкмвддфояцотеочтгюоудчзфюфээпбидэчядоекадлгмйсцаюбышаэчсартйчфэчбоцнкчяэьйфпсгягяшснрэээонггьэпуэеклеяждэ чалщфхдйспотфйгпбцчгйээюнрэлмюфнрдушиучаээчыэюяэдогтгтгцнйчгнггйээдщряуишзэгнурмйинчфешурвшишкмщпсгзылакдкдыэшсжеяцээкчггшйкгнчтшкмщ псгиэгнггыцээтшхльчцутэгнишснаяцшйчтукжйдтукжснчфэншыснтфиэшрснкчншлвььвшэжвдгэдэчйягьокгещвехжлвээчсартйндьэомймйэфэхэиштэшшбйюмцшчс лгщшймггкэреапфчшсрэчстгаэцоцусндуурюмчбмйшстшчфбэюгцчюшчфврцшшивчнсцгжлвгчсыэпбцнчфршламбдунрйштбфэфехщцнуррэяагэиэывщяюшмйэдгни рээзшезяанфэшртдыиряартпаэчтоюгчршуфраяршлвюнчфврфпаяжбмйячюоыягэдймеэнчфэчцошешытэубцдщркжцлураяоцээшсылуйсслумфурсгвчыэсгвчыэлгсп ечьчцвтйгвюнаярэяапыфрэщжлйьфэшшоимеэнисжчфэалмйягвчкдпрфпюдффиэяэвчтшкакуьэаллгрсцыэшлвхуопогщруыурыягэдэтшфпчбыщаэрэээждрнезгргмй мьэйжазгньэээпбэезйлгчуфэщгьоээюоыэжлклькьяешпьцгэчкшемкүопжехжтблгаэямймхчдуцгынвшлвььнытйиэячщшьгшеопщязйвдждгнэезсрфишыэцуишмзшу блзгдэыүиртбмйтеодифыжйшбйаггнеяшэреапчфүиьйэехлиэкчшэыркүэнхүопогоштфиэяэрэчстглбплээцдынцнвйкгюгаэкдмфнрэрйшзсвдпчршяаюбиэггзүүрүйзж апмзвднччраыклцнвшиснчрэьуэеклеяждьэрряучфишэнфэссиетфюфтймйьэуисеплэнйшфпфэьммйкгюгогягяглуснйшзэчдчртймг

### Розшифрований текст

мамапошламытьпосудуитомотправилсязанейкаждыйзвукзвонложкиилитарелкигулкораздавалсявзнойномвечернемвоздухепотомонимолчапошливбольшуюко мнатуснялисдиванаподушкивдвоемраскрылиегоиразложиливедьнасамомделеэтобылвовсенедиванашироченнаякроватьмамапостелилаимсдугласомпостельл овковзбилаподушкитомначалбылорасстегиватьрубашкуноонасказалапогодиминуткутомпочемунадотыкакаяточуднаямамонаопустиласьнастулносразужевстал аподошлакдвериипозвалаоназваласноваисновадугласдугдуугееголосуплывалвдушнуютьмуитонулвнейбезвсякогооткликадажеэхонеотвечалодугласдугласдугл асдуууглааастомсиделнаполуиегопронизывалхолодновинойтомубылонемороженоеинезимаинелетнийзнойонвиделмаматорастерянноозираетсятозакрываетг лазастоитинезнаетчтоделатьиоченьволнуетсядасразувиднорастерянаиволнуетсяонаоткрыладверьверандышагнулавтемнотуспустиласьпоступенькампрошлапо дорожкеподкустысиренитомприслушивалсякеешагамонаопятьпозваламолчаниеонапозвалаещедваразатомвсесиделвкомнатевотсейчассдлиннойдлиннойузко йулицыдонесетсяголосдугласаидумамнебеспокойсяяидунодугласнеотвечалтомдолгиедвеминутысиделглядянараскрытуюпостельнамолчащеерадиоимолчащи йпатефонналюстругдекакнивчемнебывалопоблескивалистеклянныевисюлькинаковеррасписанныйпунцовымиифиолетовымизавитушкамипотомнарочностукн улногойокроватьчтобыпоглядетьбудетлибольнооказалосьбольнодверьверандысоскрипомотвориласьимамасказалапойдемтомпройдемсякудапростопоулицеи демонвзялеезарукуонипошлипосентджеймсстритасфальтподногамибылвсеещетеплыйсверчкистрекоталигромчепрежнеговстушавшейсятьмеонидошлидоуглас вернулиидвинулисьпонаправлениюкзападномуоврагугдетопроплылавтомобильсверкнулвдалифараминаулицахникакихпризнаковжизнинисветанидвиженияк оегдепозадимерцалислабоосвещенныеквадратыоконвтойсторонеоткудаонишлиневсеещелеглиспатьнооченьоченьмногиедомаужестоялибезогнейиспалиапер еднекоторымитожетемныминакрылечкахсиделиихобитателиивполголосавеливечернююбеседукоегденаверандахпоскрипываликачелихотьбыотецбылдомаска заламамаонасжималавсвоейбольшойрукерукутоманупостойдаймнетолькодобратьсядоэтогомальчишкидушегубопятьвышелнаохотуонубиваетлюдейвсемгроз итопасностьниктонезнаетгдеикогдаонвдругпоявитсявотклянусьпустьтолькодугпридетдомойяеготакотколочувекбудетпомнитьонипрошлиещекварталитеперьст оялипередчернымсилуэтомнемецкойбаптистскойцерквинауглучепелстритигленроквсотнешаговзацерковьюначиналсяоврагтомужечуялегооттудатянулоканали зационнойтрубойстнившимилистьямидушнымивлажным запахом сплошных зеленых зарослейоврагбылширокий извилистый онперерезалгородим амавсегдагово рилачтоэтоиднемтонепроходимыедебриаужночьюкнемулучшеиблизконеподходитьоттогочторядомцерковьстрахидолжныбырассеятьсянотомувсеравнобыло жутковэтотчастемнаябезединогоогонькаонаказаласьхолоднойибесполезнойразвалинойнакраюоврагатомубыловсегодесятьлетонничеготолкомнезналосмерти страхеужасесмертьэтовосковаякуклавящикеонвиделеевшестьлеттогдаумерегопрадедушкаилежалвгробуточноогромныйупавшийястреббезмолвныйидалекийн икогдабольшеоннескажетчтонадобытьхорошиммальчикомникогдабольшенебудетспоритьополитикесмертьэтоегомаленькаясестренкаоднаждыутромемубыло втовремясемьлетонпроснулсязаглянулвееколыбелькуаонасмотритпрямонанегозастывшимислепымисинимиглазамиапотомпришлилюдииунеслиеевмаленько йплетенойкорзинкесмертьэтокогдаонмесяцспустястоялвозлееевысокогостульчикаивдругпонялутоонаникогдабольшенебудеттутсидетьнебудетсмеятьсяилипла катьиемууженебудетдосадночтоонародиласьнасветэтоибыласмертьиещесмертьэтодушегубкоторыйподкрадываетсяневидимкойипрячетсязадеревьямииброд итпоокругеивыжидаетиразилидвавгодприходитсюдавэтотгороднаэтиулицыгдевечерамивсегдатемночтобыубитьженщинузапоследниетригодаонубилтрехэтос мертьносейчастутнепростосмертьвэтойлетнейночиподдалекимизвездаминанегоразомнахлынуловсечтоониспыталвиделислышалзавсюсвоюжизньионзахлебы валсяитонулонисошлистротуараизашагалипопротоптаннойусыпаннойшебнемтропинкепообестороныгусторосласорнаятраваивнейгромконеумолчнотрешалисв ерчкитомпослушношелзаматерьюбольшойхрабройпрекраснойегозащитницейотвсегосветатаквдвоемонишлиишлиивотостановилисьнасамомкраюцивилизаци иоврагздесьвэтойпропастипосредичернойчащобывдругсосредоточилосьвсечегоонникогданеузнаетинепойметвсечтоживетбезыменноевнепрогляднойтенидер евьеввудушливомзапахегниенияаведьонисматерьюздесьсовсемоднииеерукадрожитдадрожитемунепочудилосьноотчегомамаведьбольшесильнееумнееегоне ужелиионатожечувствуетэтунеуловимуюугрозутозловещеечтозатаилосьтамвнизуисейчасвыползетизтемнотызначитможновырастиивсеравнонестатьсильнымз начитстатьвзрослымвовсенеутешениезначитвжизнинетприбежищанеттакойнадежнойцитаделичтоустоялабыпротивнадвигающихсяужасовночисомненияразры валиегомороженоевновьобожглоемухолодомгорловсевнутрипохолоделопоспинепошелморозоледенелирукииногиемувдругсталооченьзябкоточновновьналет елизпрошлогодекабрьскийветертаквотоночтозначитэтоучастьвсехлюдейкаждыйчеловекдлясебяодинединственныйнасветеодинединственныйсампосебесред ивеликогомножествадругихлюдейивсегдабоитсявоткаксейчаснузакричишьстанешьзватьнапомощькомукакоеделотьмапоглотитводномгновеньеодночудовищн оеледенящеемгновеньеивсеконченоещезадолгодорассветазадолгодотогокакполицейскиеначнутпрощупыватьсвоимифонарикамитемнуюрастревоженнуютро пинкуинанейзашуршитшебеньподногамилюдейкоторыевсмятениикинутсянапомощьидажееслионисейчастольковпятистахшагахоттебяаужнавернотаконоиесть темныйприбойможетзахлестнутьзатрисекундыиотнятьутебявсетвоидесятьлетижизньэтоодиночествовнезапноеоткрытиеобрушилосьнатомакаксокрушительны йударионзадрожалмаматожеодинокавэтуминутуейнечегонадеятьсянинасвятостьбраканиназащитулюбящейсемьининаконституциюсоединенныхштатовнинап олициюейнеккомуобратитьсякромесобственногосердцаавсердцесвоемонанайдетлишьнеодолимоеотвращениеистрахвэтуминутупередкаждымстоитсвоятольк освоязадачаикаждыйдолженсамеерешитьтысовсемодинпоймиэторазинавсегдатомпроглотилкомокзастрявшийвгорлеиприжалсякматеригосподинедайейумер етьмолилоннеделайнамничегоплохогопапапридетссобраниячерезчасиеслидоманикогонебудетматьдвинуласьпотропинкевдикуючащумамтызадуганебойсядр ожащимголосомсказалтомснимничегонеслучилосьтызанегонебойсяснимничегонеслучилосьонвсегдавозвращаетсяэтимпутемголосматеризвенелотнапряжени яясторазговорилаемуходидругойдорогойноэтипроклятыемальчишкивсеравнолезутнапроломкогданибудьонпойдеттудаибольшеневернетсябольшеневернется этоможетозначатьчтоугоднобродягипреступникитьманесчастныйслучайаглавноесмертьодинвовсейвселеннойнасветемиллионтакихгородишекивкаждомтакже темнотакжеодинококаждыйтакжеотвсегоотрешенвкаждомсвоиужасыисвоитайныпронзительныезаунывныезвукискрипкивотмузыкаэтихгородишекбезсветано сомножествомтенейакакоенеобятноенепомерноеодиночествоаневедомыеоврагичтозасасываюткактрясинажизньвэтихгородишкахпоночамоборачиваетсяледе нящимужасомразумусемьедетямсчастьюсовсехсторонгрозитчудищеимякоторомусмертьматьсновагромкопозвалавтемнотудугласдугивдругобапочувствовалич тотослучилосьсверчкиумолклисталосовсемтихоонинезналчтобываеттакаятишинабеспредельнаябездыханнаятишинаотчегозамолчалисверчкиотчегокакаяэтому причинапреждеониникогданеумолкалиникогдазначитзначитсейчасчтотослучитсяказалосьоврагнапрягаетсвоичерныемышцывбираетвсебявсесилыспящихгоро дковифермнамногиемиливокругвеликаятишинапропитанныхросойлесовидолининакатывающихсякакприбойхолмовгдесобакизадравмордывоютналунувсясоб ираласьстекаласьстягиваласьводнуточкуивсамомсердцетишиныбылионимамаитомвотсейчассиюминутучтотослучитсячтотослучитсясверчкивсемолчатзвездыо пустилисьтакнизкочтокажетсяпротянирукуинапальцахостанетсяпозолотаихнесчестьзвездонижаркиеколючиевсерастетразбухаеттишинавсеострейнапряженней ожиданиеохкактемнопустыннокакбесприютноивдругдалекодалекозаоврагомголосяздесьмамидумамаисновамамамидушлепшлепшлепмчатсяногивтеннисн ыхтуфляхподнуоврагасхохотомнесутсятроемальчишекбратдугласчарливудмениджонхафбегутхохочутзвездывзвилисьвверхточнодесятьмиллионовужаленныху литоквтянулисвоирожкисверчкизастрекоталитемнотаотступалаиспуганнаяошарашеннаязлобнаяотступилапотеряваппетитведьонасовсемужесобраласьпоживи тьсяивдругейтакгрубопомешалиикогдатемнотаотхлынулаточноволнавовремяотливаизнеевозниклисмеясьтроемальчишекмамтомприветисразувокругзапахлод угласомведьотнеговсегдапахнетпотомтравойдеревьямиветвямииручьемвампредстоитпоркамолодойчеловекобявиламамаотеестраховиследанеосталосьтомзн алонаникогдавжизниникомупроэтонерасскажетникогданострахэтотнавсегдаостанетсяунеевдушеивдушетоматожетемнойлетнейночьюонишлидомойспатькакх орошочтодугласживойкакхорошоанаоднусекундутамнакраюоврагаемуподумалосьгдетодалекопосмутномуозаренномулунойлесунадвиадукомпотомвнизупод олинепрогрохоталпоездонотчаянносвистелточнобезыменныйжелезныйзверьзаблудилсявночитомулегсявпостельрядомсбратомвесьдрожаонприслушивалсякэ томусвистуидумалдалекодалекотамгдесейчасмчитсяпоезджилихдвоюродныйбратиумеротвоспалениялегкихмноголетназадвотвтакуюженочьдугласлежалрядо мотнегопахлопотомиэтобылокакволшебствотомпересталдрожатьтолькодвевещиязнаюнавернякадугпрошепталонкакиеодначтоночьюужаснотемноадругаяесл имистерауфманкогданибудьвсамомделепостроитмашинусчастьясоврагомейвсеравнонесовладатьдугласнемногоподумалповторичтотысказалониумолклинаул ицевнезапнораздалисьшагиближеботижевотониужеподдеревьямивозледоманатротуаремамасосвоейкроватинегромкосказалапапаидетинеошибласьа

## Код програми

```
const fs = require('fs');
const commonBigrams = ['ct', 'ho', 'eh', 'to', 'ha'];
const alphabet = ['a', '6', 'B', '\Gamma', '\pi', 'e', '\pi', '\pi'
'p',\,'c',\,'T',\,'y',\,'\varphi',\,'x',\,'\mu',\,'\mu',\,'\mu',\,'\mu',\,'\mu',\,'b',\,'b',\,'\beta',\,'\rho',\,'\kappa'];
readAndParse = (path) => {
        let text = fs.readFileSync(path, 'utf-8');
        return text.replace(/\s/g, ");
 }
const getFiveMostFreq = (text) => {
        const bigramFreq = { };
        const bigramAmount = Math.floor(text.length / 2);
        const result = [];
   for (let i = 0; i < text.length - 1; i+=2) {
               let bigram = text.slice(i, i+2);
               bigramFreq[bigram] ? bigramFreq[bigram]++ : bigramFreq[bigram] = 1;
        }
        for (let key in bigramFreq) {
               bigramFreq[key] = bigramFreq[key] / bigramAmount;
        }
        let entries = Object.entries(bigramFreq);
        let sorted = entries.sort((a, b) \Rightarrow b[1] - a[1]).slice(0, 5);
        for (let i in sorted) {
               result.push(sorted[i][0]);\\
        fs.appendFileSync('results.txt', 'Five most frequent bigram:\n');
        result.forEach((val, i) => \{
               fs.appendFileSync('results.txt', `${i+1}: ${val}\n`);
        })
        return result;
 }
const getGcd = (a, b) \Rightarrow \{
       if (b === 0) return a;
        return getGcd(b, a % b);}
```

```
const euclideanAlgorithm = (a, b, x1 = 1, y1 = 0, x2 = 0, y2 = 1) = > \{
  if (b === 0) {
     return y1;
  }
  return euclideanAlgorithm(
     b,
     a%b,
     x2,
     y2,
     x1 - (Math.floor(a/b) * x2),
     y1 - (Math.floor(a / b) * y2)
  );
}
const getBigramAlphabet = () => {
  const arr = [];
  for (let i in alphabet) {
     for (let j in alphabet) {
        arr.push(alphabet[i] + alphabet[j]);
     }
  };
  return arr;
}
const solveEquation = (a, b, n) \Rightarrow \{
  const gcd = getGcd(n, a);
  switch(gcd) {
     case 1:
        let inverse = euclideanAlgorithm(n, a);
        inverse = inverse >= 0 ? inverse : inverse + n;
        return [ (inverse * b) % n ];
     default:
        if (b % gcd === 0) {
          const solutions = [];
          for (let i = 0; i < gcd; i++) {
             solutions.push(solveEquation(a \ / \ gcd, \ b \ / \ gcd, \ n \ / \ gcd)[0] + i \ * \ (n \ / \ gcd));
```

```
return solutions;
        } else return false;
  }
}
const getKeys = (bigrams, alphabet) => {
  const keys = [];
  for (let i in bigrams) {
     const x1 = alphabet.indexOf(bigrams[i][0].a);
     const y1 = alphabet.indexOf(bigrams[i][0].b);
     const x2 = alphabet.indexOf(bigrams[i][1].a);
     const y2 = alphabet.indexOf(bigrams[i][1].b);
     const a = x1 - x2 > 0? x1 - x2 : x1 - x2 + 961;
     const b = y1 - y2 > 0? y1 - y2 : y1 - y2 + 961;
     const values = solveEquation(a, b, 961);
     if (values) {
        values.forEach(value => {
          if (a === 0) return;
          if(keys.find((\{a\}) => a === value)) return;
          const b = y1 - (value * x1) \% 961;
          const key = {
            a: value,
            b: b > 0? b : b + 961
          keys.push(key);
        });
  return keys;
}
const findBigramsComb = (theory, bigrams) => {
  const arr = [], result = [];
  for (let i in bigrams) {
     for (let j in theory) {
       arr.push({
          b: bigrams[i],
```

```
a: theory[j]
        })
  }
  for (let i = 0; i < 24; i++) {
     for (let j = i + 1; j < 25; j++) {
        result.push([arr[i], arr[j]]);
     }
  }
  return result;
}
const decipher = (cipher, a, b, alphabet) => {
  let text = ";
  if (getGcd(961, a) !== 1) return;
  let inverse = euclideanAlgorithm(961, a);
  inverse = inverse \geq 0 ? inverse : inverse + 961;
  for (let i = 0; i < cipher.length - 1; i += 2) {
     const y = alphabet.indexOf(cipher.slice(i, i+2));
     const diff = y - b > 0? y - b : y - b + 961;
     const result = (inverse * diff) % 961;
     text += alphabet[result];
  }
  return text;
}
const checkText = (text) => {
  const notExisting = ['аь', 'оь', 'уь', 'еь', 'ыь', 'иь', 'эь', 'яь', 'юь', 'йь', 'йй', 'ьь', 'ыы', 'ьы'];
  return !notExisting.some(bg => text.indexOf(bg) + 1);
}
const getText = (keys, cipher, alphabet) => {
  for (let i in keys) {
     const text = decipher(cipher, keys[i].a, keys[i].b, alphabet);
     if (text && checkText(text)) fs.appendFileSync('results.txt', text);
```

```
}

const text = readAndParse('09.txt');

const bigramAlphabet = getBigramAlphabet();

const bigramsComb = findBigramsComb(commonBigrams, getFiveMostFreq(text));

const keys = getKeys(bigramsComb, bigramAlphabet);

getText(keys, text, bigramAlphabet)
```

**Висновок**: Під час данного комп'ютерного практикума ми набули навички частотного аналізу на прикладі розкриття моноалфавітної підстановки та опанували прийомами роботи в модулярній арифметиці.