Міністерство освіти і науки України

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-73

Лень Олександр та Мухамедзянов Артем

Перевірили:

Чорний О.

Савчук М. М.

Завадська Л. О.

Варіант 9

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 (*a*, *b*) знайти можливі кандидати на ключ 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.

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', 'йь', 'йй', 'ьь', 'ыы'.

Біграми:

Відкритий текст	Закритий текст
на	ээ
то	вд
ен	чф
но	гн
ни	цг

Шифрований текст

тгтгрэцрюфмнйбмйшугдээдэибггэдайжаишуикггуоитлчмтлвшаэвмхдвдлгцччцмбпвръэггзухлураятаиэншчфэчучкштфьэзукщтбцнчфвшяфнрагрэцрцлцэюоксбмчф
цгссошпруйедйгцгрэчсммцлжлочщетйсегрхчяэйекааэндвдэчбоцгзгдэыуирщцээятглплькчедйгцгчдфэучюшщясеплэнйфюфюбмйячвдогяфруопогшэпбмйячюоаэ
смплизфрюбдукжюдээщшсвурятаэггшйячбдйгьойсегммцшмэцгпмкаурюбщпдуяфйшлнрсээпблвтфцшкуцншмймщяээжсшшщятгдэцгчббйядогцоцггнвриэоеканы
клгнурюбдухжогууэчцдябдайгогвшкайгогошплфдошплкуопогруопчсопйчяэаэнссрелуртукжэсфнйфгдэээсглкчрзяаьйемщпмэумвдкгсгнчпщвшзэалжвурдуопогру
опогруопогрухсопогбггнчфьдечхшюбнргдфпчбфэкдчтйгйщнрдуиээдиэвнчфщзгрвштфвешыэшочйшяаяффдкчвчтшаиешшившэдечлфюфэнветйячыяюшмэсдггсна
яээюгсеелфчкпогюггнодядкчешфчывээечогьоуэучжоьэхшгчэйжутйггдсэдшшветйячыяцгцлнрэсснаявштэумэтогжлэеблэеишлтдгфшврхлячщшцнбйесгнфртййбмй

сстчжокгпбфэцрюбдувешыючрэщмбйетьдцчкдээпбцдщркжцлураяючржапюфвштэчяьорэтлурюфнрагкдзэцгрэтлурфчычжлиекаэнчфьйзйлуирсмчфцгячьээйуиагшйдрйшиэпувдюшшишаыэмсвдхтгэкчьчэйыпнрмйчсартйфдчстгщшаззйрэыэчйхялуцшдуопогошзэалжвурээыунрбдяуэчждэсетьдечнпзякяцгггпмэтссхбмйячюоцгдэявжкйчггедоддэявжкаиягячеэюшуркйтеопечкгсшцлучщшазелурчбезвчпмцлуруйячэрдшртклуйлрфмйшймплэеггдбуйишртгбцшнэгтждтхуэвчээгтждюгэдссммюфябцнчфцгфээшмйсссшвриэяэчэсеплэнэвээятрэаржуснцзшуснвдцэюоиэгмкаурмйцзнрушдуэчтоэчггаувймйсеябчфцньэцдогцояфюфтйкгюгогрэпутфээпбфэпутфаярссгжемйээрэврзюйдечдэллцявчяаиечмбэкдрэцрябмйэшфунчгфшйтеюнтйугюоибдуиэнгждятглычкснтбитчйэчувюдгнцчыэлгвдфечфучжеуыкчяэыйусигджуиаяьожчвшлухжвдгэопогылэеэсвдлуэдэсвдцорэцгжехлвчкдбмюгягшшчфбэреапопечээжечбитогенчфезфрюйэчлмэсглсгвдугггждцгврзюыщкдкгюдфбцдешймплндешйшуйэчлгкджлаыэшьяыэфпечрэюгеджчиюуруйогцэмйэчычюшдчялкуггетгмвшеншигнвевшзэумшутэкдцрйшкльчькирфпвддбэнушмэучжолвэшйфиэбдяучфзснчгнуявдшчпэфшуиуйяягвдюбэеяукчыээээтждээнчячщшнфйшймэтвчимыщьдечвдэщезюнэнирхджбнряэаэзгэчвдэчучкшзьшчьччсыэфпечцгэчггауыщрэпмцдштйгвдкгучвдйэьоятцньюятчучфтйкгюгогггтгтвштйндтгогьйьэуицэюохэнечмэечмлнчфишмбмйээпуяищшсннрфмдуезггьоаягэрнщпчфурэвэжюдчсччусцэчяьогтчкштэйэссвшщзцлфчюрвууыйтффедаюнчбтйиэгнушкмээкчешфчкпечкмщпсгвштуйскбуяэдэйслцнэрдшбййббйьоээюоыэчскбцдечфучфширчяялгыэумнрлвдлюмлсечибчфкдьовшябфэцрхчычялиелгвдячтчтогнуявдтчцчввэертдйфруцээщштфьюыэрзюбядгнпмшипчлмэдцгопфсучтчайтеюнбпвчюегмьйцнкчдгяэта жюэеыэшоашсвйшураяпллгйнчфныжвиявчяэцнсссгдяэсаэкгцгвдюгпдвшиэвнйсцэчйфшцлчдждвдгнеяждчслшнфцлогбшнфюгяйэдйсрхжртбаирэшлщюгфэщруиплггчзгрчдфэюдщдтлфруйетчэубэеэеяауряэфэедтгттгьйфпсгяьэьцдогыняцээлукчонвштбфэйэедмтяуазцдзсбшлвььсштфвравччмзвджмвштбдуйэедьоцнээяэыневжучфпчлмплюйтеыщлунрбшьзчетйьчшнюйдшцнчфдльчггршезгршылныэнцээывтйячщшщяшчсчедиэяэщпвшфмтэцгкгюгогцойэаэшшшимззйрэвчеышигггтлурйшшицгсепьплггнгээшсятаэьйфпдузйшнярснвшкдучяэээцмчфкчешурмйжчянуйтеыщысщгьчдфэеьорнплмйыэйгемчмогвяыдючвшэдечвчклччгнярснээцузсжчцчяэжекуяукжкгфруыурипфэлсээзшмэфечфртмсяглжаиойтеазшчьфнрршоилуурюмаикдыэцулзнрзжзэюшзйкгнчыввэцггяътьойэфэчдпфурэвкмчфкдыэцулзнрзжэшазшусндбвеюнюэ рэвдядючдфэеьорночяэтгвчжокгойзйтеэшкгдуцгтуцстечфтфщзгрплээретфойтфярснвшжемйэсайжаапзяэсглйчыэитшчюорстэцгдфцнцдибыядэцгкчяэюггнелчдждщртбнфуййшяфбпогюгждюбцнчфжеэжвдэьедискчщрхчклтгвчжоыэгбчячиэомвесдямзйжчянрцээыэцутэуфзйвюдббйдягнуяглдавчйчгтшэыэяэгнврэвкмфдтуйскбвшпрынмэцгкдыэцулзнрзжэшазшуснссэйлуснушазшусндфоаьоаяфрябогкгьохчшсныэшазшуснгээгшшлвээвшиедуфртйуштйэчпцээмзгртйжчянадькзйжчянрцээчсччуснмцнвеоирэщмгглтйгснаякчэдедьмшиябыяучэйжакуэеклеяждмзфэедибмэсеопйдгтндсгснйекафрлуйгипдужеэщдуюнхьсгнцээкпведуцгрнисвдхтцуклжвэеюфцльчцуэнтфиэынезцсшдьончыкйшшаюбмйвчшшхчтебпдутээсшдкнцчыцээдфэеьоиэьчцвтйсстштбфэгнмйжчянблрншивчтшуииэудрэьуурюмяфлаэчзуюфйшишфпвекачфцгкрчшврплычынмэкддбмнурэдечвдщрлжурюгьйкйьэцылажоуэааыщвчятйгайрдэээсаэкдшэцруйтецнпгггглаыжапурябчбфээьнишиэмсбтягюшшыычмштфтечбйшючрэеззйээфэртусгнвемйогшэкшщятехлфдршуифечфыэкчмфнрзшцнцчигвдыпэеимюнчфрэщркжиэчччаюфэнэеььцэюоохэбщггмешижеюмггошифпдажкюнкдпччэальчяэыслснэнймтуьэтфвшэжвдэжвдцлцнмйлгиээдвдцоцгзгдьмггююцлфрлажюхдплггцаечцонцээгбфэяггнябмйцчедучкшшиагщэяттуйсяймйцчгэ ээудаэцоьйжвфпмэюшкмщпсгкчшацгснйштбшижчальчыншыцлсншччтжчюшочршtбфэаржуиэвнэшлуэеклачюлшукжвдьэыаюбыщфпкдэшьяхляуюэкддфэнэеььзузйюйпльчдэшшхдйчйскгшешыюнсгшешыюнтфцштблвшуфрмйушмэывфпчфюфхляуцзнрзжзйфрушйчмфкчйчяэкчныирхдвшэншыжвдлгнпсснрнцшысаээдшсясфедалндааэ эчычжвээюглгфрмйинюфршлагдьчцвтйгтрэчаснлаячщшцнщацгудифшыиэгтгггнхдьйэехлиэкчгнэнюйфрушнфешсвюнгнэнблеемйитзлплькчклнржэшхчешсвюнзылакдкчибцдшчндигкчзнймшицгечбшшипдлгечвдынбсгнуяогятжецнцлцгжлбппьыдййгсщгшэршлвуйчфкчкддекаэтйгвдфпчфвешыэшочршплюэцэшпаэтфкщнрдучфяэхрпльчршлнцдрэйэаэечаэрэдбйштбхжирдэфэпэвечкчвдйсюдйшщпхчшстуйсяйлгаэлвэшхазззыээзшплиэшоцгвчячвдьбфэцрщпдуюмлзтопмаиэчячяняймьэээиэындацгудпцээавтйьоьйрщэьечомяылтцвирплюмдройазоэедкчедийалэшртнштйэчячдуйшяуйшгнэчюшоизгпбмйаззйцчедэчвдыэяэщшшыэйалкуйсбдкрвууицльчцулзодэйслцнкгыйуиагошшаймцдудуогнишржхайгьоцгрэдэчоыэшскгыэяуирцнйфюбщпаэядалдуиэспиээчжозэшшлвшуплзкиэиряуэшвкйчспиээчжойдьйюмвшучиэькяакунряэгэггшйэчлгюггэнпдуцнщпгмймрэвдпччйюдэшсвэсибфэосштйгьоылоджеэцгцдкгждячщшюьгггнцчьэнчюшюьтечбйшрсйшишуиюгксюжюнычшчжорэшшщпюффрвууиыээээткладфшнэшхдюдэсэйдшюбчфакадсгнчзйвдвшуйуиагггнрфмплчяядгныщдгнгйэзназгныцгэчкшцнймвшодзйьоячщшоижемзшидэнчфаыщвчгнэсьоюгтеуйюмцшлтуэтшшнтсячюяьйсньэлузйшнярснаылажорнмэедиэучгньэршяяюбиээзумэтядзэмекжфрмйушэнчфймймшэсекжюнирушоишуиеуэ аакуфэщглфюфэншызэедиэкгнцссждэсссуикчучяэцгечшнюйдшйштйвяээгнцзггкгкдцгюгыдссэьюяыччйтфадкдцгыэийядсспдкйочедкчюшлщанэнплкдцгрэвдпдмчншюмыэшсезггядьоаясечфзйезгнэчюшщпмйэецюбгьйэецюзйьэтфвшишяиечюрэжушээгэвддэээалггычкдйдгнггмлрнмфйшлнмбэеяукггунфгнодэйьэшннрфммйьэжакусвфдкггуоигэмыэшзгжчэержюнинвйпльчдэедубшиждрнвекайшхльчцуэнчфжещпаэядцмчфгмюггныяджаиипвевчябцдщгайемтгячцдяэдбдуйшяуяиуимфэеснйфнрфрвшкчечогншюфкдучяэсрхщщпчбюбюбцдечэйшэмеишьяучцчовтйхчщрлучфишкмщпвшазшуснтгьожлйшвртййбцнфэтдямкледрсйвжкмфюфетюгчснгкчцэчйжуфэщгыдспнрмйчфпмкаурээдйкдщштвфпвшзйфсудаэцоетюгкчяэкчцэчйойкдщштвфпвшзйфсудаэцовшьйфпсгьэтлггигснаярняфесячспнрмйтгячцдтлэ ширцнцгжеыыэшьяойээггэпплвефрфчшсйэедшеопшигэфэяэншяцяджегмзяеттфурэвэжюдьйэехлиэвчдстшюбфэаэьмщпсгкдлсбовшрэпуснсссгмзнрзжэшклэекчэйбцээдэнчээешсвэнэвээопдуиэмедуыпябцчгнмбкдюдьотгкччвтйтшоищравяиапогршочдфэеьодуйшьэьйуиьйирэшиэнштйэчячждбруэтнймэщяэфэедччюдсмяыгэонймнчячщшцнймнчдуйшгмгмяылтвнймнчцньйфпмэтержэшсмяыгэдйьэиcщгбтуйьэюняиртжевшсдячюортяазсртршдчтлчмуйсеябюдьэифшашмецядцпведуэжюмшчпйэчлгиэшэщшшыэйалчфячкчжгкгыээшээюятшочкчрэжчкшочдуйшлвзйальгкчэчгэмтзэреаптвээюгзбтйгфнкгжныяьдцгндешблрнэщяэфэе дммышцрэиэагдэцэггудйгснаявчечпяыдшсщгшэщекамфбйтфачечдядйаггньььшэьйршгнвевшфедаюнжседычяфемцнвечфбйжчянйфэнюйиэйгфечфыэрэтлурхлячщшцншуопогруопцлшеопезюблвдлгньэйгвдынцнмйфсудаэцоылэеимисдэцмвдгнурмйпльчонэщмэкдкчешурынезелфчзнймщяядчдцгшчдбцчечюоцгззяалтчгюшщяядчдцгцнучяэюгдэявруйэчувюдцнучяэкгкгбцээшсжетвйшюбцчгузэкдкдыэцуишысдэцмурйшкмщпсгешсвюнешсвюньчцвтйынцнмйфсудэйемкаурмйюэреапцгжеыпфчэйьэтвэерттфлжхтузйефчальчюяьйзйфрвйчяыдцпведуыээдзчафцгщшщпхчждвдьэсеопэчвдкгшнэжйшюбфэтдлгюшлщфэшэшрзйпллунрйшйшймэнелпыдййемймжемзшийэлфплцузйеэймлакуггжфвелтьэфнцгфсэсьйойезйеуртйюйячкгогцогныпцлуртйблдуэсэ эимгдьйюфчфьчмупчядчдртятвдвшяфюффдээзлцньчцвтйьдхфйшлнавээээщравюнаяынцнмйфсудэйойэчувюдьйтфнрагфаэчзувэесгнфруйинймкджмлвээкгнчэйщбфэдякдйсрсйшюбурсюыщмйлгкчэйщбданрцнфдяшзйучгнхаэчзувшаыиеюдюмнрйвхчьйэетйячтекалсчгснядчдцгьйзэгнцчншюбыянчюшуишылуишхчхщкгжнтфиэесгнчшиэкгфззйжерьтшодтуйсцуурюмдуурюмдатэреапчфяэаэаязузййфюфлумфюффдошплюфюфюфюфлукжвчщжвчщжвчыфагэйдшщпцлячюшуйртунахзяфбдуэсплггнгвщхщцнчфкчнсэйшнфэтфурэвэжюммеэнчсартйагхрцлшужчкдпывшчгюзфплнйэйэжсфаэчзуелтлфруйблэчющээзшдузйшнйффрвдвшплныурэшртюсвдээялдяэсвдылодфэвмуйэчувюдюггнцчыэлгвдячщшцнтээйссягогуйесгюшщяхжиеыжэшцгжааэмшщяцнгнмбфрюбцнэеслюбтчядаляуюэцгшэьйтфныэйезггогцорэндэдьоаяцлшеопуилгйпйсцэрэжчдгвдкмщпсгячщшцнтэжщитэсогээзшплнрцгьэретфоэюрцлфдешйчьэешкмвддфояцотеочтгюоудччзфюфээпбцдэчядоекадлгмйсцаюбыщаэчсартйчфэчбоцнкчяэьйфпсгягяшснрэээонггьэпуэеклеяждэчалщфхдйспотфйгпбцчгйээюнрэлмюфнрдушиучаээчыэюяэдогтгтгцнйчгнггйээдщряуишзэгнурмйинчфешурвшишкмщпсгзылакдкдыэшсжеяцээкчггшйкгнчтшкмщпсгиэгнггыцээтшхльчцутэгнишснаяцшйчтукжйдтукжснчфэншыснтфиэшрснкчншлвььвшэжвдгэдэчйягьокгещвехжлвээчсартйндьэомймйэфэхэишэшшбйюмцшчслгщшймггкэреапфчшсрэчстгаэцоцуснду рюмчбмйшстшчфбэюгцчюшчфврцшшивчнсцгжлвгчсыэпбцнчфршламбдунрйштбфэфехщцнуррэяагэиэывщяюшмйэ дгниреэзшезяанфэшртдыиряартпаэчтоюгчршуфраяршлвюнчфврфпаяжбмйячюоыягэдймеэнчфэчцошешытэубцдщркжцлураяоцээшсылуйсслумфурсгвчыэсгвчыэлгспечьчцвтйгвюнаярэяапыфрэщжлйьфэшшоимеэнисжчфэалмйягвчкдпрфпюдффиэяэвчтшкакуьэаллгрсцыэшлвхуопогщруыурыягэдэтшфпчбыщаэрэээждрнезгргмймьэйжазгньээпбэезйлгчуфэщгьоээюоыэжлклькыяешпьцгэчкшемкуопжехжтблгаэямймхчдуцгынвшлвььныт йиэячщшьгшеопщязйвджднгэезсрфишыэцуишмзшублзгдэыуиртбмйтеодифыжйшбйаггнеяшэреапчфуиьйэехлиэкчшэыркуэнхуопогоштфиэяэрэчстглбплээцдынцнвйкгюгаэкдмфнрэрйшзсвдпчршяяюбиэггзууруйзжапмзвдннчраыклцнвшиснчрэьуэеклеяждьэрряучфишэнфэссиетфюфтймйьэуисеплэнйшфпфэьммйкгюгогягяглуснйшзэчдчртймг

Розшифрований текст

мамапошламытьпосудуитомотправилсязанейкаждыйзвукзвонложкиилитарелкигулкораздавалсявзнойномвечернемвоздухепотомонимолчапошливб ольшуюко мнатуснялисдиванаподушкивдвоемраскрылиегоиразложиливедьнасамомделеэтобылвовсенедиванашироченнаякроватьмамапостелилаимсдугл асомпостельл овковзбилаподушкитомначалбылорасстегиватьрубашкуноонасказалапогодиминуткутомпочемунадотыкакаяточуднаямамонаопустиласьнастулно сразужевстал аподошлакдвериипозвалаоназваласноваисновадугласдугдуугееголосуплывалвдушнуютьмуитонулвнейбезвсякогоотклик адажеэхонеотвечалодугласдугласдугл асдуууглааастомсиделнаполуиегопронизывалхолодновиноййтомубылонемороженоеинезимаинелетнийзнойонвиделмаматорастерянноозирается ито закрываетг лазастоитинезнаетчтоделатьиоченьволнуетсядасразувиднорастерянаиволнуетсяонаоткрыладверьверандышагнулавтемнотуспустилась поступенькампрошлапо дорожкеподкустысиренитомприслушивалсякеешагамонаопятьпозваламолчаниеонапозвалаещедваразатомвсесиделвкомнатевотсейчассдлиннойдлиннойузко йулицыдонесетсяголосдугласаидумамнебеспокойсяяидунодугласнеотвечалтомдолгиедвеминутысиделглядянараскрытуюпостельнамолчащеерадиоимолчащи йпатефонналюстругдекакнивчемнебывалопоблескивалистеклянныевисюлькинаковерраспсанныйпунцовымиифиолетовымизавитушкамипотомнаро чностукн улногойокроватьчтобыпоглядетьбудетлибольнооказалосьбольнодверьверандысоскрипомотвориласьимамаскасказалапойдемтомпройдемсякудапростопоулицеи демонвзялеезарукуонипошлипосентджеймсстритасфальтподногамибылвсеещетеплыйсверчкистрекоталигромчепрежнеговсгущавшейсятьмеонидо шлидоуглас вернулиидвинулисьпонаправлениюкзападномуоврагугдетопроплылавтомобильсверкнулвдалифараминаулицахникакихпризнаковжизнинисветанидвижениях оегдепозадимерцалислабоосвещенныеквадратыоконвтойсторонеоткудаонишлиневсеещелеглиспатьнооченьоченьмногиедомаужестоялибезогней испалиапер еднекоторымитожетемныминакрылечкахсиделиихобитателиивполголосавеливечернююбеседукоегденаверандахпоскрипываликачелихотьбыотецбылдомаска заламамаонасжималавсвоейбольшойрукерукутоманупостойдаймнетолькодобратьсядоэтогомальчишкидушегубопятьвышелнаохотуонубиваетлюде йвсемгроз итопасностьниктонезнаетгдеикогдаонвдругпоявитсяворотклянусьпустьтолькодугпридетдомойяеготакотколочувекбудетпомнитьонипрошлиещекварта литеперьст оялипередчернымсилуэтомнемецкойбаптистскойцерквинауглучепелстритигленроквсотнешаговзацерковьюначиналсяоврагтомужечуялего оттудатянулоканали зационнойтрубойсгнившимилистьямидушнымивлажнымзапахомсплошныхзеленыхзарослейоврагбылширокийизвилистыйонперерезалгородимамавсе гдагово рилачтоэтоиднемтонепроходимыедебриаужночьюкнемулучшеиблизконеподходитьоттогочторядомцерковьстрахидолжныбырассеятьсянотомувсеравнобыло жутковэтотчастемнаябезединогоонькаоназаласьхолоднойибесполезнойразвалиной накрающоврагатомубыловсегодесятьлетонничеготолком незналосмерти страхеужасесмертьэтовосковаякуклавящикеонвиделеевшестьлеттогдаумерегопрадедушкаилежалвгробуточноогромныйупавшийястреббезмолвныйидалекийн икогдабольшеоннескажетчтонадобытьхорошиммальчикомникогдабольшенебудетспоритьополитикесмертьэтоегомаленькаясестренкаоднаждыутр омемубыло втовремясемьлетонпроснулсязаглянулвееколыбелькуаонасмотритпрямонанегоза стывшимислепымисинимиглазамиапотомпришлилюдииунеслиеевмаленько йплетенойкорзинкесмертьэтокогдаонмесяцспустястоялвозлееевысокогостульчикаивдругпонялчтоонаникогдабольшенебудеттутсидетьнебуде тсмеятьсяилипла катьиемуженебудетдосадночтоонародилась наснаветэтоибыласмертьищесмертьэтодушегубкоторыйподкрадываетсяневидимкойипрячетсязадеревьямиброд итпоокругеивыжидаетиразилидвавгодприходитсюдавэтотгороднаэтиулицыгдевечерамивсегдатемночтобыубитьженщинузапоследниетригодаону билтрехэтос мертьносейчастутнепростосмертьвэтойлетнейночиподдалекимизвездаминанегоразомнахлынуловсечтоониспыталвиделислышалзавсюсвоюжизньионзахлебы валсяитонулонисошлистротуараизашагалипопротоптаннойусыпаннойщебнемтропинкепообестороныгустосласорнаятраваивнейгромконеумолч нотрещалисв ерчкитомпослушношелзаматерьюбольшойхрабройпрекраснойегозащитницейотвсегосветатквдвоемонишлиишлиивотостановилисьнасамомкраюцивилизаци иоврагздесьвэтойпропастипосредичерной чащобывдругсосредоточилосьвсечегоонникогданеузнаетинепойметвсечтоживетбезыменноевнепрогл яднойтенидер евьеввудушливомзапахегниенияаведьонисматерьюздесьсовсемодниееерукадрожитдадрожитемунепочудилосьноотчегомамаведьбольшесильнееумн еегоне ужелиионатожечувствуетэтунеуловимуюугрозутозловещеечтозатаилосьтамвнизуисейчасвыползетизтемнотызначитможновырастиивсеравнон естатьсильнымз начитстатьвзрослымвовсенеутешениезначитвжизнинетприбежищанеттакойнадежнойцитаделичтоустоялабыпротивнадвигающихсяужасовночисом ненияразры валиегомороженоевновьобожгloемухолодомгорловсевнутрипохолоделопоспинепошелморозоледенелирукииногиемувдруг сталоченьзябкоточновновьналет елизпрошлогодекабрьскийветертаквотоночтозначитэтоучастьвсехлюдейкаждыйчеловекдлясебяодинединственныйнасветеодинединственныйса мпосебесред ивеликогомножествадругихлюдейивсегдабоитсяваткаксейчаснузакричишьстанешьзватьнапомощькомукакоеделотьмапоглотитводномгновеньеодночудовищн оеледенящеемгновеньеивсеконченоещезадолгодорассветазадолгодотогокакполицейскиеначнутпрощупыватьсвоимифонарикамитемнуюрастрево женнуютро пинкуинанейзашуршитшебеньподногамилюдейкоторыевсмятениикинутсянапомощьидажеелсионисейчастольковпятистахшагахоттебяаужнавернотаконоиесть темныйприбойможетзахлестнутьзатрисекундыиотнятьутебявсетвоидесятьлетижизньэтоодиночествовнезапноеоткрытиеобрушилосьнатомакакс окрушительны йударионзадрожалмаматожеодинокавэтуминутуейнечегонадеятьсянинасвятостьбраканиназащитулюбящейсемьининаконституциюсоединенныхштатовнинап олициюейнеккомуобратитьсякромесобственногосердцаавсердцесвоемонанайдетлишьнеодолимоеотвращениеистрахвэтуминутупередкаждымстои тсвоятольк освоязадачаикаждыйдолженсамеерешитьтысовсемодинпоймиэторазинавсегдатомпроглотилкомокзастрявшийвгорлеиприжалсякматеригосподинедайейумер етьмолилоннеделайнамничегоплохогопапапридетссобраниячерезчасиеслидоманикогонебудетматьдвинуласьпотропинкевдикуючащумамтызадуг анебойсядр ожащимголосомсказалтомснимничегонеслучилосьтызанегонебойсяснимничегонеслучилосьонвсегдавозвращаетсяэтимпутемголосматеризвенелотнапряжени яясторазговорилаемуходидругойдорогойноэтипроклятыемальчишкивсеравнолезутнапроломкогданибудьонпойдеттудаибольшеневернетсябольш еневернется этоможетозначатьчтоугоднобродягипреступникитьманесчастныйслучайглавноесмертьодинвовсейвселеннойнасветемиллионтакихгородишекивкаждо мтакже темнотакжеодинококаждыйтакжеотвсегоотрешенвкаждомсвоиужасыисвоитайныпронзительныеузаулывыезвукискрипкивотмузыкаэтихгородишек безсветано сомножествомтенейакакоенеобятноенепомерноеодиночествоаневедомыеоврагичтозасасываюткактрясинажизньвэтихгородишкахпоночамоборач иваетсяледе нящимужасомразумусемьедетямсчастьюсовсехсторонгрозитчудищеимякоторомусмертьматьсновагромкопозвалавтемнотудуг ласдугивдругобапочувствовалич тотослучилосьсверчкиумолклисталосовсемтихоонинезналчтобываеттакаятишинабеспредельнаябездыханнаятишинаотчегозамолчалисверчкиот чегокакаяэтому причинапреждеонияникогданеумолкалияникогдазначитзначитсейчасчтотослучитсяказалосьоврагна прягаетсвоичерныемышцывбираетвсебявсесилыспящихгоро дковифермнамногиемиливокругвеликаятишинапропитанныхросойлесовидолининакатывающихсякакприбойхолмовгдесобакизадравмордывоютналу нувсясоб ираласьстекаласьстягиваласьводнуточкуивсамомсердцетишиныбылионимамаитомвотсейчассиюминутучтотослучитсячтотослучитсясверчкивсемолчатзвездыо пустилисьтакнизкочтокажетсяпротянирукуинапальцахостанетсяпозолотаихнесчестьзвездонижаркиеколючиевсерастетразбухаеттишинавсеострейнапряженней ожиданиеохкактемнопустыннокакбесприютноивдругдалекодалекозаоврагомголосязде сьмамидумамаисновамамамамидушлепшлепшлепмчатсяногивтеннисн ыхтуфляхподноуврагасхохотомнесутсятроемальчишекбратдугласчарливдумениджонхафбегутохохочутзвездывзвились вверхточнодесятьмиллион овужаленныху литоквтянулисвоирожкисверчкизастрекоталитемнотаотступалаиспуганнаяошарашеннаязлобнаяотступилапотеряваппетитведьонасовсемужесобраласьпоживи тьсяивдругейтакгрубопомешалиикогдатемнотаотхлынулаточноволнавовремяотливаизнеевозниклисмеясьтроемальчишекмамтомприветисразуво кругзапахлод угласомведьотнеговсегдапахнетпотомтравойдеревьямиветвямииручьемвампредстоитпоркамолодойчеловекобявиламамаотеестраховиследанеосталосьто мзн алонаникогдавжизниникомупроэтонерасскажетникогданострахэтотнавсегдаостанетсяунеевдушеивдушетоматожетемнойлетнейночьюонишлидом ойспатькакх орошочтодугласживойкакхорошоанаоднусекундутамнакраюоврагаемуподумалосьгдетодалекопосмутномуозаренномулунойлесунадвиадукомпото мвнизупод олинепрогрохоталпоездоноточаянносвистелточнобезыменныйжелезныйзверьзаблудилсявночитомулегсявпостельрядомсбратомв есьдрожаонприслушивалсякэ томусвистуидумалдалекодалекотамгдесейчасмчитсяпоезджилихдвоюродныйбратиумеротвоспалениялегкихмноголетназадвотвтакуюженочьдугл аслежалрядо мотнегопахлопотомиэтобылокакволшебствотомпереставдрожатьтолькодвевещиязнаюнавернякадугпрошепт алонкакиеодначтоночьюужаснотемноадругаяесл имистерауфманкогданибудьвсамомделепостроитмашинусчастьясоврагомейвсеравнонесовладатьдугласнемногоподумалповторичтотысказалони умолклинаул ицевнезапнораздалисьшагиближеближевотониужеподдеревьямивозледоманатротуарема масосвоейкроватинегромкосказалапапаидетинеошибласьа

Код програми

```
#include <iostream>
#include <fstream>
#include <string>

using namespace std;

wchar_t *alpha = L"абвгдежзийклмнопрстуфхцчшщыьэюя";

void set_locale(wfstream &file)
{
      setlocale(LC_ALL, "");
      locale loc("");
         wcout.imbue(loc);
         file.imbue(loc);
}

void read_file(wstring &str, wfstream &file)
{
      getline(file, str);
}

int get_from_alphabet(wchar_t c)
{
      for (int i = 0; i < 31; i++)
            if(c != alpha[i])
                  continue;
            else
                  return (i);
      return (-1);
}


int   *create_bigrams(wstring str, int cur, int flag, int str_size, int **bigrams,
int **converted_text)
{
      int alpha_size = 31;
      int bigram_size = alpha_size * alpha_size;
      int *bigram = new int[bigram_size];
      int i = -1;
      int *conv_text = new int[str_size / 2];
      while (++i < bigram_size)
            bigram[i] = 0;
      i = -1;
      while (++i < str_size)
      {
            switch (flag)
            {
                  case 0:
                  {
                        flag = 1;
                        cur += 31 * get_from_alphabet(str[i]);
                        break ;
```

```
                }
                case 1:
                {
                      flag = 0;
                      cur = get_from_alphabet(str[i]) + cur;
                      bigram[cur]++;
                      int ind = i / 2;
                //    cin >> forcin;
                      conv_text[ind] = cur;
                      cur = 0;
                      break ;
                }
          }
      }
      *bigrams = bigram;
      return (conv_text);
}

void  search_best(int *bigrams, int **best_bigrams)
{
      int *candidates = new int[5];
      int best;
      int i = 0;
      int l;
      i = -1;
      while (++i < 5 && (l = -1) && !(best = 0))
      {
            while (++l < 961)
                  (bigrams[l] > bigrams[best]) ? (best = l) : 0;
            candidates[i] = best;
            bigrams[best] = -1;
      }
      *best_bigrams = candidates;
}
void  *create_rus_bigrams(int **rus_bigrams)
{
      int *rus = new int[5];
      wchar_t *data1 = L"снтне";
      wchar_t *data2 = L"тооан";
      int i = -1;
      while (++i < 5)
            rus[i] = get_from_alphabet(data1[i]) * 31 + get_from_alphabet(data2[i]);
      *rus_bigrams = rus;
}

void normal(int &num)
{
      (num < 0) ? (num = 961 + num) : 0;
}

int calc(int &a, int &b, int &x, int &y)
{
      int q, r, x1, x2, y1, y2;
      x2 = 1; x1 = 0; y2 = 0; y1 = 1;
      if (b == 0)
```

```
	{
		x = 1;
		y = 0;
		return (a);
	}
	while (b > 0)
	{
		q = a / b;
		r = a - q * b;
		x = x2 - q * x1;
		a = b;
		b = r;
		x2 = x1, x1 = x, y2 = y1, y1 = y;
	}
	x = x2;
	y = y2;
	return (a);
}

int evklid(int a, int n)
{
	int d, x, y;
	d = calc(a, n, x, y);
	if (d == 1)
	{
		if (x > 0)
			return x;
		else
			return (n + x);
	}
	return (0);

}

int gcd(int razx, int temp)
{
	return ((temp == 0) ? razx : gcd(temp, razx % temp));
}

void get_a(int razx, int razy, int &size_of_a, int* &mas_a)
{
	normal(razx);
	normal(razy);
	int min = gcd(razx, 961);
	mas_a = new int[min];
	if (min != 1 && razy % min == 0)
	{
		razx = razx / min;
		razy = razy / min;
		int start;
		start = evklid(razx, 961 / min) * razy;
		start %= 961;
		normal(start);
		int i = -1;
		while (++i < min)
```

```
            {
                  size_of_a++;
                  mas_a[i] = start + i * 961;
                  mas_a[i] %= 961;
                  normal(mas_a[i]);
            }
      }
      else
      {
            if (min == 1)
            {
                  size_of_a = min;
                  int i = 0;
                  mas_a[i] = (evklid(razx, 961) * razy) % 961;
                  normal(mas_a[i]);
            }
      }
}

void get_b(int &rus, int &best, int &size_of_a, int* mas_a, int* &mas_b)
{
      mas_b = new int[size_of_a];
      int i = -1;
      while (++i < size_of_a)
      {
            mas_b[i] = (best - mas_a[i] * rus);
            mas_b[i] %= 961;
            normal(mas_b[i]);
      }
}

double index(int size, wchar_t *tmp, double ret)
{
      int count[31];
      int i = -1;
      while (++i < 31)
            count[i] = 0;
      i = -1;
      while (++i < size)
            count[get_from_alphabet(tmp[i])] += 1;
      i = -1;
      while (++i < 31)
      {
            double f = ((double)((count[i] - 1) * (count[i]))) / ((double) ((size - 1)
* (size)));
      }

      for (int i = 0; i < 31; i++)
      {
            double first = (double)(count[i] * (count[i] - 1));
            double second = first / (double) (size * (size - 1));
            ret += second;
      }
      return (ret);
}
```

```
void print(int *mas_a, int *mas_b, wchar_t *tmp, int cur)
{
	wcout << mas_a[cur];
	wcout << " ";
	wcout << mas_b[cur] << "\n";
	wcout << tmp;
	wcout << "\n\n\n";
}

bool verify_text(int* mas_a, int* &mas_b, int &size_of_a, int* &bigrams, int size,
int* &conv_text)
{
	wcout << mas_a[0] << endl;
	wchar_t *tmp = new wchar_t[size * 2 + 1];
	tmp[size * 2] = 0;
	int cur = -1;
	while(++cur < size_of_a)
	{
		if (evklid(mas_a[cur], 961) == 0)
			continue;
		else
		{
			double index_text = 0;
			int i = -1;
			while (++i < size)
			{
				int forcin;
				int x = (evklid(mas_a[cur], 961) * (conv_text[i] -
mas_b[cur]))%961;
			//	cin >> forcin;
				normal(x);
		//		wcout << "getting x cur = " << cur << " i = " << i << " x = "
<< x <<  endl;
				tmp[i * 2] = alpha[(x - (x % 31)) / 31];
				tmp[1 + i * 2] = alpha[x % 31];
			}
			index_text = index(size * 2, tmp, 0);
			wcout << index_text;
			wcout << "\n";
			if (index_text > 0.055)
			{
				print(mas_a, mas_b, tmp, cur);
				return (1);
			}
		}
	}
	return (0);
}

void process_all(int *bigrams, int *conv, int *best, int *rus, int size)
{
	int i;
	int l;
	int j;
```

```
	int k;
	for (i = 0; i < 5; i++, l = 0)
	{
	for (; l < 5; l++, j = 0)
	{
	for (; j < 5; j++, k = 0)
	{
		if (j == i)
			continue;
	for (; k < 5; k++)
	{
		if (k == l)
			continue;
		int size_of_a = 0;
		int *mas_a;
		int *mas_b;
		get_a(rus[i] - rus[j], best[l] - best[k], size_of_a, mas_a);
		wcout << mas_a[0] << endl;
		get_b(rus[i], best[l], size_of_a, mas_a, mas_b);
		wcout << mas_a[0] << mas_b[0] << endl;
		if (verify_text(mas_a, mas_b, size_of_a, bigrams, size / 2, conv))
			goto escape;
	}
	}
	}
	}
escape:
	return ;
}

int main(int argc, char **argv)
{
	wfstream file(argv[1]);
	set_locale(file);
	wstring str;
	wcout << alpha << endl;
	read_file(str, file);
	wcout << "our file is\n" << str << endl;
	int size = str.size();
	int bigrams_size = size / 2;
	int *bigrams;
	int *converted_text;
	converted_text = create_bigrams(str, 0, 0, size, &bigrams, &converted_text);
	int *best_bigrams;
	int *rus_bigrams;
	create_rus_bigrams(&rus_bigrams);
	search_best(bigrams, &best_bigrams);
	process_all(bigrams, converted_text, best_bigrams, rus_bigrams, size);
}
```

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