



МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

Лабораторна робота №3

з дисципліни **Криптографія** на тему:

« Криптоаналіз афінної біграмної підстановки »

Перевірів:

Чорний О.М.

Виконали:

Студенти групи ФБ-91

Красний П.В.

Прищепа М.О.

Київ 2021

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 елемента 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.

Хід роботи:

Найчастіші біграми шифрованого тексту для варіанту 9

ээ: 0.016543706684551754
вд: 0.012743125419181758
гн: 0.012519561815336464
цг: 0.012519561815336464
чф: 0.012519561815336464

Усі можливі утворені ключі

(502, 230)	(802, 100)	(820, 861)	(219, 705)	(300, 897)
(318, 697)	(678, 541)	(18, 867)	(378, 711)	(360, 529)
(642, 810)	(750, 571)	(103, 499)	(617, 20)	(108, 788)
(422, 716)	(936, 237)	(314, 34)	(828, 516)	(514, 206)
(693, 884)	(127, 873)	(439, 930)	(913, 148)	(395, 55)
(707, 112)	(220, 291)	(312, 163)	(786, 342)	(474, 864)
(883, 748)	(331, 292)	(221, 34)	(904, 640)	(409, 571)
(299, 313)	(21, 919)	(851, 809)	(573, 454)	(683, 330)
(644, 467)	(914, 314)	(738, 670)	(101, 102)	(270, 874)
(94, 269)	(418, 662)	(785, 462)	(148, 855)	(324, 117)
(511, 748)	(579, 292)	(314, 34)	(780, 640)	(68, 571)
(764, 313)	(269, 919)	(696, 809)	(201, 454)	(466, 330)
(768, 777)	(511, 748)	(707, 112)	(783, 846)	(704, 37)
(900, 362)	(15, 135)	(196, 431)	(272, 204)	(76, 458)
(208, 679)	(719, 400)	(692, 710)	(152, 183)	(511, 748)
(484, 97)	(905, 531)	(934, 416)	(394, 850)	(421, 158)

Шифрований текст за варіантом 9

тгтгрэцрюфмнйбмйшугдээдзйбггэдайжаишуикггуоитлчмтлвшаэвмхдвдлгццмб
пврыэггзухлураятаиэншчфэчучкштфьэзукштбцнчфвшафнрагрэцрцлцэюоксбмч
фцгссошпруйедйгцгрэчсммцлжлочщетйсегрхчяэйекааэндвдчбоцгзгдэуирищцэ
эятгглплъчкчедйгцгчдфэучюшщясеплэньфюфюбмйячвдогяфруопогшэпбмйячюо
аэсмплизфрюбдукжюдээщшсвурятаэггшйячбдйгьойсегммцшмэцгпмкаурюбщп
дуафйшлнрсээпблвтфцшкуцншмймщяээжсшшщятгдэцгчббйядогцоцгтнвризоек
аныклгнурюбдухжогоууэчдцябдайгогвшкайгогошплфдошплкуопогруопчсопйчяэ
аэнсрелуртукжэсфнйфгдэээсглкчрзяаьемщпмэумвдкгсгнчпщвшзэалжвурдуоп
огруопогруопогрухсопогбггнчфьдечхшюбнргдфпчбфэкдчтйгйшнрдуиээдиэвнч
фцзгрвштфвешыэшочйшяаяффдкчвчтшаиешшившэдечлфюфэнветйячыяюшмэс
дггснаяээюгсеелфчкпогюггнодядкчешфчывээечогьоуэучжобьэхшгчэйжутйггдсэд
шшветйячыяцгцлнрэсснаявштэумэтогжлэеблээишлтдгфшврхлячщшцнбйесгнфр
тйбмйсстчжокгпбфэцрюбдувешыючрэщмбйетьдцчкдээпбцццркжцлураяючрж
апюфвштэчяьорэтлурюфнрагкдзэцгрэтлурфчычжлиекаэнчфьйзйлуирсмчфцгячь

ээйуиагшйдрйшиэпувдюошшишаыэмсвдхтгэкчэыйпнрмйчсартйфдчстгцшаззй
рэыэчйхялуцшдуопогошзэалжвурээыунрбдяуэчждэсетьдечнпзякяцгггпмэтсхб
мйячюоцгдэявжкйчггедоддэявжкаиаягчезюшуркйтеопечкгсшцлучшшазелурчбе
звчпмцлуруйячэрдшртклуйлрфмйшймплэеггдбуйишртгбцшнэгтждтхуэвчээгтж
дюгэдссммюфябцнчфцгфэзшмйсссшвриэяэчэсеплэнэвээятрээржуснцзшуснвдцэ
юоиэгмкаурмйцзнурушдуэчтоэчггаувймйсеябчфцньэцдогцояфюфтыкгюгогрэпут
фээпбфэпутфаярссгжемйээрэврзюйдечдэллцаявчяаиечмбэкдрэцрябмйэшфунчгф
штейеонтйугюоибдуиэнгждятгльчькснтбитчйэчувюдгнцчыэлгвдфечфучжеуыкч
яэыйусигджуиаяыожчвшлукжвдгэопогылэеэсвдлуэдэсвдцорэцгжехлвчкдбмюяг
шшчфбэреапопечээжечбитогенчфезфрюйэчлмэсглсгвдугггждцгврзюышцкдкюд
фбцдешймплндешйшуйэчлгкджлаыэшьяыэфпечрэюгеджчиюуруйогцэмйэчычю
шдчялкугтетгмвшеншигнвевшзэумшутэкдцрийшкльчькирфпвддбэнушмэучжолв
эшйфиэбдяучфзснчгнуявдшчпэфшуиуйягвдюдбэеяукчыээээтждээнчячщшнфйшй
мэтвчимышьдечвдэщезюнэнирхдбнряээзгэчвдэчучкшзшычччысыэфпечцгэчг
ауышрэмцдштйгвдкгучвдйэбоятцньюятчучфтыкгюгоггггвштйндтгогыьэуицэ
юохэнечмэечмлнчфишмбмйээпуяищшснрфмдуюезгьяоаягэрнщпчфурэвэжюдчсч
чусцэчяыогтччхштэйэсвшщццлфчюрвууиыйтффедаюнчбтйиэгнушкмээкчешфчк
печкмщпсгвштуйскбуяэдэйслцнэрдшбйббйбэоэюоыэчскбцдечфучфширчяэлгы
эумнрлвдлюмлсечибчфкдьовшябфэцрхчычялиелгвдятччтогнуявдтчцчввэертдй
фруцээшштфьюыэрзюбядгнпмшипчлмэдцгопфсучтчайтеюнбпвчюегмьйцнкчдг
яэтажюэеыэшоашсвйшураяплггйнчфныжвиявчяэцнсссгдяэсаэкгцгвдюгпдвшиэв
нйсцэйфшцлчдждвдгнэяждчслшнфцлогбшнфюягйэдйсрхжртбаирэшлщюгфэ
щруиплггчзгрчдфэюдшдтлфруйетчэубэеэеяауряэфээдтгггйфпсгяэбэцдогыняцэ
элукчонвштбфэйээедмтяуазцдзсбшльвьсштфвравчмзвджмвштбдуйеэдьоцнээя
ынвежучфпчлмплюйтеышцлунрбшьзчетйьчшньюдшцнчфдльчггршезгршылныэн
цээывтйячщшщяшчсчедиэяэщпвшфмтэцгккюгогцойэаэшшшимззйрэвчешшиггт
лурйшшиицгсепьплггнгээшсятаэыйфпдузйшнлярснвшкдучяэээцмчфкчешурмйжчя
нуйтеыщысщгчдфэеьорнплмйыэйгемчмогвяйдючвшэдечвчклччгнярснээцузсж
чцчяэжекуяукжкгфруыурипфэлсээзшмэфечфртмсягджаойтеазшчьфнрршоилуу
рюмаикдыэцулзnrзжзэюшзйкгнчывээцггэятбойэфэдпфурэвкмчфкдыэцулзnrзж
эшазшусндбвеюнюэрэвдядюдфэеьорночяэтгвчжокгойзйтеэшкгдуцггуцстечфт
фшцзгрплээретфойтфярснвшжемйэсайжаапзяэсгльчыэитшчюорстэцгдфцнцибы
ядэцгкчяэюггнелчдждшртбнфуййшяфбпогюгждюдбцнчфжеэжвдэьедискчшрхчкл
тгвчжюыэгбвчячиэомвесдямзйжчянрцээыэцутэуфзйвюдббйдягнуяглдавчйчгтшэ
ыэяэгнврэвкмфдтуйскбвшпырнмэцгкдыэцулзnrзжэшазшуснсэйлуснушазшусн
дфояыоаяфрябогкгьохчсныэшазшуснгэгшшлвээвшиедуфртыуштыэчпцээмзгрт
йжчянадькзйжчянрцээчсччуснмцнвеoirэщмгглтйгснаякчэдедьмшиябыяучэйжа
куэеклеяждмзфээдибмэсеопйдгтндсгснейекафрлуйгипдужеэщдуюнхьсгнцээкпве
дуцгрнисвдхтцуклжвэеюфцльчуэнтфиэынезцсщдьончыкйшшаюбмйвчшшхчте
бпдутаэсшдкнцчыцээдфэеьоиэьчвтйссштбфэгнмйжчянблрншивчтшуиизудрэ
ьуурюмяфлаэчзуюфйшишфпвекачфцгкрчшврпльчынмэкддбмнурэдечвдшрлжур
югыйкйьэцылажоузааышцвчятйгайрдээсаэкдшэцруйтецнпггглаыжапуриябчбфээ
ьнишиэмсбтягюшшиычмштфтечбйшючрэззйэфэртусгнвемйогшэкшщятехлфд
ршуифечфыэкчмфнрзшцнцигвдылэимюнчфрэшркжиэчччаюфэнэеььцэюохэб
щггмешижеюмгтошшифпдажкюнкдпччэальчяэылснэнимтуьэтфвшэжвдэжвдцл
цнмйлгиээдвдцоцгзгдэьмггююцлфрлажюхдплггцаечцонцээгбфэяггнябмйцчедуч
кшшиагщэяттуйсйямйцггээудаэцоьйжвфпмэюшкмщпсгкчшацгснйштбшижчал

ьчыншыцлсншччтжчюшочрштбфэаржуиэвнэшлуэеклачюлшукжвдьэыаюбыщф
пкдэшьяхляуюэкддфэнэеьзузйюйпльчдэшшхдйчйскгшешыюнсгшешыюнтфцш
тблвшуфрмйушмэывфпчфюфхляуцнрзжзйфрушйчмфкчйчяэкчныирхдвшэншы
жвдлгнпсснрнцшысаээдшсясфедалндааээчычжвээюглфрмийнюфршлагдьчцвтй
гтрэчаснлаячщщнщацгудифшыиэгтгггнхдйэехлиэкчгнэнойфрушнфешсвюнг
нэнблеемйитзлпльчкчлнржэшхчешсвюнзылакдкчибцдшчндигкчзниймшицгечбш
шипдлгечвдынбсгнужогятжецнцлцгжлбппыдйгсцгшэршлвуйчфкчкддекаэтиг
вдфпчфвешыэшочршплуюэцэшпаэтфкшнрдучфяэхрплчршлнцдрэйэаэчаэрэдбй
штбхжирдэфэпэвчечкчвдйсюдйшщпхчшстуйсйялгаэлвэшхаззыэээзшплиэшощгв
чячвдьбфэцрщпдуюмлзтопмаиэчячяниймьэээиэындацгудпцээавтийоьйрщэьечом
яылтцвирплуюмдройазоедкчедийалэшртнштйэчячдуйшыуишгнэчюшоизгпбмйаз
зйцчедэчвдыэяэщшшызйалкуйсбдкрвууицльчулзодэйслцнкгыиуагошшаймцд
удуогнишржхайгьощгрэдэчобыэшскгыэяуирцнийфюбщпаэадалдуиэспиээчжозэшш
лвшуплзкиэиряуэшвкйчспиээчжойдьйюмвшучиэькяакунряэгэггшйэчлгюггэнпд
уцнщпгмймрэвдпчйюдэшсвэсибфэосштйгьобылождеэцгцдкгждячшшюьгггнцч
ьэнчюшюьтечбйшрсйшишуиюгксюжюнычшчжорэшшщпюфрвууиыээээтклдф
шнэшхдюдэсэйдшюбчфакадсгнчзйвдвшуйуиаггннрфмплчяадгныщдгнгйэзназэг
ныцгэчкшцнймвшодзйьоячщшоижемзшидэнчфаыщвчгнэсьоюгтеуйюмцшлтуэт
шшнтсячюяьйсньэлузйшнряснаылажорнмэедиэучгньэршяаюбиэээумэтядзэмек
жфрмйушэнчфймймшэсекжюнирушоишуиеуэаакуфэщглфюфэншызээедиэкгнцс
сждэсссуикчучяэцгечшнюйдшйштйвяээгнцзггкгкдцгюгыдссэюяыччйтфадкцг
ыэийядсспдкйочедкчюшлщанэнплкдцгрэвдпдмчншюмыэшсезггядьоаясечфзйез
гнэчюшщпмйэецюбгьйеэцюзйьэтфвшишяиечюрэжушзэгэвддээалгычкдйдгнгг
млрнмфйшлнмбэеяукггунфгнодэйьэшннрфммйьэжакусвфдкгуоигэмыэшзгжчэ
ержюнинвйпльчдээдубшиждрнвекайшхльчцуэнчфжешпаэадцмчфгмюггныяджа
иипвевчябцдщгайемтгячдядэдбдуйшыуаиуимфэеснийфнрфрвшкчечогншюфкдуч
яэсрхщщпчбюбюбцдечэйшшэмеишьяучцчовтйхчщрлучфишкмщпвшазшуснтгьож
лйшвртййбцнфэтдямкледрсйвжкмфюфетюгчснгкчцэйжужфэщгьдспнрмйчфпмк
аурээдйкдщштвфпвшзйфсудаэцоетюгкчяэкчцэйойкдщштвфпвшзйфсудаэцовш
ьйфпсгьэтлггиснаярняфесячспнрмйтгячцдтлэширцнцгжеьыэшьяойээггэпллвфр
рфчшсйээдшеопшигэфэяэншяцяджегмзаеттфурэвэжюдьйэехлиэвчдстшюбфэаэ
мщпсгкдлсбовшрэпуснсссгмзнрзжэшклэекчэйззнрзжэшклэекчэйбцээдэнчээешс
вэнэвээопдуиэмедуыпябцгнмбкдюдьотгкччвтйтшоишравяиапогршочдфэеьоду
йшьэьйуиьйирэшиэнштйэчячждбруэтниймэщяэфээдчюдсмяыгэониймнчячщщн
ймнчдуйшгмгмяылтвниймнчцнйфпмэтержэшсмяыгэдьэисцгбтуйьэюняиртжев
шсдячюортаазсртршдчтлчмуйсеябюдьэифшашмецядцпведужюмшчпйэчлгиэш
эщшшызйалчфячкчжгкгыээшзэюятшочкчрэжчкшочдуйшлвзйальгкчэчгэмтзэреа
птвээюгзгбтигфнкгжныядцгндешблрнэщяэфээдммыщрэиэагдэцэггудйгснаявче
чпяыдшсцгшэщекамфбйтфачечдядйаггньышэьйрщгнвевшфедаюнжседычяфемц
нвечфбйжчянийфэнюйиэйгфечфыэрэтлурхлячщщншуопогруопцлшеопезюблвд
лгньэйгвдынцнмйфсудаэцобылэеимисдэцмвдгнурмйпльчонэщмэкдкчешурынезе
лфчзниймщяядчдцгшчдбцчечюощгззяалтчгюшщяядчдцгнучяэюгдэявуруйэчувю
дцнучяэкгкгбцээшсжетвйшюбцггузэкдкдыэцуишысдэцмурйшкмщпсгешсвюне
шсвюньчцвтйынцнмйфсудэйемкауимйюэреапцгжеыпфчэйьэтвэерттфлжхтузйе
фчальчюяьйзйфрвйчяыдцпведудыээдзчафцгшщпхчждвдьэсеопэчвдкгшнэжйш
юбфэтдлгюшлщфэшэшрзйпллунрийшйшймэнелпыдйеймйжемзшийэлфплцузй
езймлакуггжфвелтьэфнцгфсэсьойезйеуртийюячкгогцогныщлуртийблдуэсээимг

дъйюфчфьчмупчядчдртятвдвшафюфдээзлцньчцвтйьдхфйшлнавээээщравюная
 ынцнмйфсудэйойэчувюдййтфнрагфаэчзувэсгнфруйиниймкджмлвээкгнчэйщбфэ
 дякдйсрйшюбурсюыщмйлгкчэйщбданрцнфдяшзйучгнхаэчзувшаииеюдюмнрй
 вхчйэетйячтекалсчгснядчдцгййзэгнцншюбыянчюшуишылуишхчхщкгжнтфиэ
 есгнчшиэкгфзййжерътшодтуйсцуурюмдуурюмдатэреапчфязазаязузййфюфлумф
 юффдошплюфюфюфюфлукжвчщжвчщжвчыфагэйдшщпцлячюшуйртунахзьяфбд
 уэсплггнгвщхщцнчфкчнсэйшнфэтфурэвэжюммеэнчсартйагхрцлшужчкдпывшчг
 юзфплнйэйэжсфаэчзуелтлфруйблэчющээшдзузйшнйфрвдвшплныурэшртюсвд
 ээалдяэсвдылодфэвмуьйэчувюдюггнцчыэлгвдячщщцнтэйссягогуйеснгюшщяхж
 иеыжэшцгжааэмшщяцнгнмбфрюбцнэеслюбтчядаляуюэцгшэйтфнызйезггогцор
 эндэдьоаяцлшеопуилгйпйсцэрэжчдгвдкмщпсгячщщцнтэжщитэсогээзшплнрцгъэ
 ретфозюрцлфдешйчъэешкмвддфояцотеочтгюоудчзфюфээпбцдэчядоекадлгмйс
 цаюбыщаэчсартйчфэчбоцнкчяэьйфпсгягяшснрэээонггъэпуэекляждэчалщфхдйс
 потфйгпбцггйэюнрэлмюфнрдушиучаээчыэюяэдогтггцнйчгнггйээдщряуишзэг
 нурмйинчфешурвшишкмщпсгзылакдкдыэшсжеяцээкчггшйкгнчтшкмщпсгиэгнг
 гыцээтшхльчцутэгнишснаяцшйчтукжйдтукжснчфэншыснтфиэшрснкчншлвьв
 шэжвдгэдэчйягьокгешцвехжлвээчсартйндьэомймйэфэхэиштэшшбйюмцшчслгщ
 шймггкэреапчшсрэчстгаэцоцусндурюмчбмйшстшчфбэюгцчюшчфврцшшивч
 нсцгжлвгчсыэпбцнчфршламбдунрйштбфэфехщцнуррэяагэиывщяюшмйэдгнир
 ээзшезянфэшртдыиряартпаэчтоюгчршуфраяршлвюнчфврфпаяжбмйячюобьягэд
 ймеэнчфэчцошешытэубцдщркжцлураяоцээшылуисслумфурсгвчыэсгвчыэлгспе
 чьчцвтйгвюнаярэяапыфрэщжльйфэшшоимеэнисжчфэалмйягвчкдпрфпюдффиэя
 эвчтшкакуьэаллгрсцыэшлвхуопогщрууурыягэдэтшфпчбыщаэрэээждрнезгргмй
 мьэйжазгньээпбээзилгчуфэщгьээюоыэжлклъкьяешпыцгэчкшемкуопжехжтблг
 аэямймхчдуцгынвшлвьвнытйиэячщшыгшеопщязйвдждгнээзсрфишыэцуишмзшу
 блзгдэыуиртбмйтеодифыжйшбйаггнеяшэреапчфуиййэхлиэкчшэыркуэнхуопог
 оштфиэяэрэчстгглблээцдынцнвйкгюгаэкдмфнрэйшзсвдпчршыаюобиэгтзууруйз
 жапмзвднччраыклцнвшиснчрэуэекляждьэрряучфишэнфэссиетфюфтимйьэуис
 еплэнийшфпфэьммйкгюгогягяглуснийшзэчдчртимг

Розшифруємо для кожного знайденого ключа 50 перших букв шифрованного тексту

key = (502, 230):	эуэуптлрюьжапноофыбиостнтфюкузомфвгвзмщжузбжщлкпелк
key = (802, 100):	ыбыбфтзхцфгоасщпнэишстчтисцбщшэпжщнунчэбыэцмяхцмя
key = (820, 861):	ыоыоштэылниэтелкмшэгствтюдееобгукэрчадххоышэххуфиху
key = (219, 705):	бхбхлтдмрьоыафгшзюажстетпфйхэжэшшдорбиэхмюоитщьктщ
key = (300, 897):	эпэпуэычкдйофйрвфбфтшэоэсйопвтлвежвряядпубпяпиелпи
key = (318, 697):	эоэопхцдофичкжнзгрхтбхюхжжяоэтьззвзеугьомрягуаууп
key = (678, 541):	тытыьмлпьооиилдйкйтшмямрлоыытзйжуунпсфычцшсзшшрзш
key = (18, 867):	яояохшбнньвтэзядгиввбшкшйшшомвудшухкярвоизэржляжл
key = (378, 711):	тжтжщягоогтцрпзгубебечеьраждбнзбхощжмьжпуамщэечщэ
key = (360, 529):	зтзтхгждэоммхнчвкьжефгцггнртцешвиылшдптгдзпсзгщсз
key = (642, 810):	сзсзитэйкммявхмьжужастятйхюзсагыпэвптгглзюуцгснхжсн
key = (750, 571):	жужуптшрсьяахюбфэбгостнтыноууовяфцгьзншпуйбзщбкцебк
key = (103, 499):	щащацтшчзлхбужснхоиэстытцжиаыэцньйляыртацокрбзтдбз
key = (617, 20):	эрэрхтщцладчльоэхьыстштбьврьюаотсыйкдкрдхцдогьног
key = (108, 788):	яфяфшбщщссыаошфикуптабсбршюфьтнigyйфкпфхуяклдтвд

key = (422, 716): гагаюрйсмьжщкыепчйдтэрярчымафтжпыйиожозоасйсэефызеф
 key = (936, 237): кчкчфцафоацдрвдшумтцтцхвччлтвшлзмллоучаеюоойоо
 key = (314, 34): **мамапошламьтыпосудуитомотправилсязанейкаждьзвукзв**
 key = (828, 516): пыпыджсэвартайопнзфунжыжзийыауепэрыггцйыеззцфбищфб
 key = (514, 206): гтгтчэясгаяцхлеивмьжгэмэвлэтжжщиьчбопфжтжмнфчпшгчп
 key = (693, 884): йьйьятцавжклгшщехфцнстмтсшвыннзезывмауэьефиулицщли
 key = (127, 873): хфхфнткодеинвйжцяпйкстйтмйрфзквциуюьжбифчпщбщвючщв
 key = (439, 930): юнюнътжэбдрптщлиокмзстжтщцынсзхифаилоопнркноийыхиь
 key = (913, 148): тотоштныбнээчоекшшюгствтгеовггкшртакхнозшгхчуаичу
 key = (395, 55): вцвцпьябцранмякююфнтепипряцжтьюмггабвгцфхвмхесмх
 key = (707, 112): рнрнфожрщечбыгиммацттоцохггнчткмцюьщшззнааязоцьоц
 key = (220, 291): йэйэгыдцзнгхбсчяччзтзыяылсдэтуяэьлднийэрчбйакпаак
 key = (312, 163): гнгнвкдднжжтумррэхиюикькгмлнеюкрдьиизаянвхфаосявос
 key = (786, 342): еегушязонптэаымбътфжщбщлаюгфимтотуаышгрьиюпьбоп
 key = (474, 864): фтфтлзсррнчынодлюсжгцвзфзцдитчщфюмэкгцгытжцяцнммунм
 key = (883, 748): ввввжоязшяфнажлхщбланояовжбвчадхьинцтчтвбэчусупус
 key = (331, 292): щбщбиояйихйагыфуьтидногоаылбхдпуэчьвнрббытюрбщнэбщ
 key = (221, 34): мамакойлймштопусцдщинозожпраиирсмзвндйкайдыйшвлкшв
 key = (904, 640): ййййчогшиахлшхждгжжгновояхжйпгрдзьщзцкыйежхкичнсич
 key = (409, 571): пупустмрфьяязюсфдбиоутптмюэузопфмгозвщшурбьщйкыейк
 key = (299, 313): уауаьйаьлхлрогечвзьоййойагыаеочцбфвпйиаатзбияуйвяу
 key = (21, 919): елелжшвуаахкхенюхэролшбштецлюоинотвжмйымлфэщыфдюзфд
 key = (851, 809): ыаыаздемяязолцэьюкяфядпдццеагфьувчсузхамкмзоепщое
 key = (573, 454): лглгчпбибаыоцзмцчвюбяпрпшзкгкбецийщчкшьггвфшзтррзт
 key = (683, 330): йойорижьуаашнмыфдягпэидиммщэпофблгдшубооуууцвчуц
 key = (644, 467): щцщцэочюршсщбйчяйвьнномокийецунзяжтнубидцмвинмхгнм
 key = (914, 314): ййййвжорзщятнпжщхябоанояосживыатхпиюечщвкбпчщсхппс
 key = (738, 670): рнрнпоцргехбогнмпаэтносойггнютпмдюющчззнгаюзауауац
 key = (101, 102): язязьоцэюнордяеаяйллнокоаябзтлуанырюцьюзийвьтисмти
 key = (270, 874): тхтхрбрчщыднждикчвжошбзбндяхсоакфлнюосмхпвтскьнфкь
 key = (94, 269): бнбнтзэычячюлиухуюоаязжзэлснийоуюкцгттшнаютихкцих
 key = (418, 662): дрдрфэжхшнвьжфвдыплоьэнэифгрчоыддцеелжфржпхжжагюжа
 key = (785, 462): снсншаремшсодуаязьфкфаязуанзкдышщамфюкниьдхфысхф
 key = (148, 855): алалигнтннщотюшулцьвшггыюллувиуязсизэкложэвбгчвб
 key = (324, 117): ыоыогтшыбншэхевкушлгытлтбееопгкксерзамхховшехйуцийу
 key = (511, 748): рврвлосзсятнлжгхблатодонжпвчаьххимцшчбвмбгчосапос
 key = (579, 292): ббббноайахйаяыоуютетдоиюьтбтдшугчквбрибэтсрхщчэхщ
 key = (314, 34): **мамапошламьтыпосудуитомотправилсязанейкаждьзвукзв**
 key = (780, 640): кйкйэоршиаелрхгдажагтозоцхзийегндкьмзякьйржюкочисоч
 key = (68, 571): шушуутарчьяашовфлбнохтстюжумоафвгбзцщвучбрщскяеск
 key = (764, 313): уауазйггыхярдгдцфзбокйпйхгыакоццсфопгиаезыииучвиу
 key = (269, 919): флфлушлуааюкщяюаэхошшошщцежлгошюбвэмеьляэхысдрзсд
 key = (696, 809): ыаыаддьмчямокцаьжкпфьдмдхцеауфиьввтсжзхафкязтедщте
 key = (201, 454): бгбгдпыибааойзлцжвеблпэлзлагсбдцкйачшсгсввшйтдрйт
 key = (466, 330): оооокийьуаншдмлфэяппциюигмяойляфрладвужозяэутциттц
 key = (768, 777): ицицвокюйшпщмйпярвьнтосохйуцуняятмузитцувхиимвгим
 key = (511, 748): рврвлосзсятнлжгхблатодонжпвчаьххимцшчбвмбгчосапос
 key = (707, 112): рнрнфожрщечбыгиммацттоцохггнчткмцюьщшззнааязоцьоц
 key = (783, 846): азазбодэюнорьявакйблтопочавзилрарыгюяязуйкьшиммши
 key = (704, 37): ьхьхтбдчэьднчдшкявлоьбйбядихцопкклаюгсххцвзстьсфть
 key = (900, 362): бнбнузаыпяпчулзуиюуоазззтлснныуокггмтшнтюзтсхшщсх
 key = (15, 135): урурвэпхшнкькфудепройэьэмфтрэомдтцьезждррпсжгахюга
 key = (196, 431): снснцазеешцогувыпьексабажуанчкызыцымзюкнрьцющфпсщф
 key = (272, 204): хлхлфгзтнняяоеючушцгвгдоюбывзуазчифэалэцгэдбцдб

key = (76, 458):	аоаозтыбнжэметкмшчгфтетчекоьгыкбрдаххыоышохиуэиу
key = (208, 679):	ефефдаждцдцкмогщйэбюннаыхгсфйнрйчкмэрыяфбяржыоужы
key = (719, 400):	эбэблаюяйцншлтвпотьнайаюлкбсьрвярпфезжбьоязечфтеч
key = (692, 710):	снснтаыежшиоужыеъркначапуангкльецймаюкнжьпюфхсфф
key = (152, 183):	вювюсабдгнжешйльйгоинахаойзюрипътядцнспюргщсррыщр
key = (511, 748):	рврвлосзсятнлжгхблатодонжпвчаьххимщшчбвмбгчосапос
key = (484, 97):	ынынгюйящйюзэипэбцаавюдюкиднрарэйхбуцкжныцщкцвофцв
key = (905, 531):	мемедсвжнщснюпбжстиаюдщдгпщезаяжяфлшолхеютилюьтцюь
key = (934, 416):	дндняьчщщщаеэояцсвхвььээинрхлятффыоцвнйсецфпччфп
key = (394, 850):	вивиэущкщнмайщшэбфлбжууурцоицбпэвюдркдьишфодзоаззо
key = (421, 158):	яаяаакяяынждфшухьщфулкфкбшшаяуихюерьбвваащяввэбрвэ

для ключа (314, 34) бачимо розшифрований текст схожий на нормальный текст:

key = (314, 34): **мамапошламытьпосудуитомотправилсязанейкаждыйзвукзв**

Такий текст існує :

<https://knijky.ru › books › vino-iz-oduvanchikov> ▼

Книга Вино из одуванчиков читать онлайн Рэй Бредбери ...

Мама пошла мыть посуду, и Том отправился за ней. Каждый звук, звон ложки или тарелки гулко раздавался в знойном вечернем воздухе. Потом они молча **пошли** в ...

Отже, ключ (314, 34) вірний.

Але у вже розшифрованому тексті бачимо, що букви «Ь» та «Ы» неправильно розташовані, вони займають місце один одного. Тому змінимо у розшифрованому тексті всі «Ь» на «Ы», а «Ы» на «Ь» .

Можна зробити припущення, що для розшифрування має використовуватися алфавіт російської мови, де змінений порядок букв «Ы» та «Ь» .

Розшифрований текст за варіантом 9

мамапошламытьпосудуитомотправилсязанейкаждыйзвукзвонложкиилитарелки гулвораздавалсявзнойномвечернемкоздухепотомонимолчапошливбольшуюком натуснялисдиванаподушкивдвоемраскрылиегоиразложиливедьнасамодделеэтоб ылвовщенедиванашироченнаякроватьмамапостелилаимсдугласомпостельловко взбилаподушкитомначалбылорасстегиваььрубашкуноонасказалапогодиминутку томпочемунадотыкакаяточуднаямамонаопустиласьнастулноспразпюевсталаподо шлакдвериипозвалаоназваласноаисноवादугласдугдуугееголосуплывалвдушну ютьмуитонулвнейбезксякогооткликадажеэхонечотвечалодугласдугласдугласдуу углаастомщиделнаполуиегопронизывалхолодновинойтомубылонеморкюеноеи незимаинелетнийзнойонвиделмаматорастеиянноозираетсятозакрываетглазастои тинезнаекчтоделаьиоченьколнуетсядасразувиднорастеиянаиволнуетсяонаоткр ыладверьверандышагнулавтемнотуспустиласьпоступенькампрошлаподоркюкеп одкустыщиренитомприслушивалсякеешагамонаопяьпозваламолчаниеонапозва лаеседваразатомксесиделвкомнатекотсейчассдлиннойдлиннойузвойулицыдоне

щетсцголосдугласаидумаамнебесповойсяидунодугласнеотвечалтоддолгиедвеминутыщиделглядянараскрытуюпостельнамолчащеерадиоимолчащийпатефонналюстругдекакнивчемнебывалопоблескивалистеклянныевисюлькинаковеррасписанныйпунцовымиифиолетовымизавитушкамипотомнарочностукнулнойокроватъчтобыпоглядетьбудетлибольшооказалосьбольшодверьверандысоскрипомоткориласьимамасказалапойдемтопройдемсякудапростопоулицеидемонвзялеезарукуонипошлипосентджеймсстритасфальтподногамибылвщенщетепокрытыйсверчкистревогаталигромчепрбюнегосгушавшейсяямеонишлидоуглайвернулиидвинулисьпонаправлениюкзападномууврагугдетопроплылаавтомобильсверкнулвдалифараминаулицчхникакихпризнаковжизнинисветанидвдюенрявоегдепозадимерцалислабоосвесенниеэквдратыоконвтойсторонеоткудаонишлиневщенщелеглиспатьнооченьоченьмногиедомаужестоялибезогнейиспалиапереднекоторыеитожетемныминакрылечкчхщиделиихобитателиивполголосавеливечернвжбещеудвоегденаверандчхпоскрипываликачелихобьбыотнцбылдомаказаламамаонасжималаксвоейбольшойрукеукутоманупостойдаймнетолькодобраьсядоэтогомальчишкидушегубопьяьвышелнаохотуонубиваетлюдейксемгрозитопасностьниктонеизнаетгдеикогдаонвдругпоявитсяавотклянусьпусьтольводугпридетдомойяеготавогтолочувекбудетпомншьонипрошлиесекварталитеперьстоялипередчернымсилуэтомнемнцвойбаптистскойцерквианауглечепелстритигленрокксотнешаговзацервовьюначиналсяоврагомпноечуялегооттудалянулоканализационнойтрубойсгнившимилистьямидушнымивлажнымзапахомсплошныхзеленыхзарослейоврагбылширокийизвилистыйонперерезалгородимамаксегдагокорилаптоэтоиднемтонепоходимыедебриаужночзжкнемулучшеиблизконеподходиьоттогопторядомцерковстрчхидолжныбрасцетясянотомувщеравнобылкуютвовэтокчастьмнаябезединогоогонькаонаказаласьхолоднойибесполезнойразвалинойнакрджоврагатомубыл оксегодесятьлетонничеготолкомнезналосмертистрчхэужащесмерьэтовосвоваякуклавсясикееонвиделеевшестьлеттогдаумерегопрадедушкаилбюалвгробуточноогромныйупавшийястреббепмолвныйидалекийнивогдабольшеоннескажечтонадобььхорошиммальчикомнивогдабольшенебудетспоритьополитикесмерьэтоегомаленькаясестренкаоднаждыутромемубыловтовремясемьлетонпроснулсязаглянулвеевольтелькуаонасмотритпиямонанегозастывшимислепымисинимиглазмиапотомпришлипждиунеслиеемаленьвойплетенойкорзинкесмертьэтовогдаонмесьяцспустястоялвзлеееевысогостульчикаивдругпонялптоонанивогдабольшенебудеттутсидетьнебудетсмеяьсяилиплакаьиемупюенебудетдосадночтоонародиласьнасветэтоибыласмертьинщесмертьэтодушегубкоторыйподкрадываетсяневидифкойипиячетсязадеревьямиибродитпоокругеивыжидаетиразилидвавгодприходитхждаэтотгороднаэтиулицыгдевечерамивщегдатемноптобыубийьеещинузапоследниетригодаонубилтрэнэтосмерьнощейчастьтупенпростосмертьвэтойлетнейночипомдалекимизвездаминанегоразомнахлынуловщептоониспыталвиделислышалзаксюскощюизньионзчхлебывалсяитонулонисошлистротуараизчшагалипопроточтаннойусыпаннойсебнемтропинкепообестороныгусторосласорнаятраваивнейгромвонеумолчноотрещалийверчкиотомпослушношелзаматерзжбольшойхрабройпрекраснойегозащитницейотвщегойветатаквдкоемонишлиилишливотостановилисьнасамофкраюцивилизацииоврагздесьвэтойпропастипосредичернойчащобывдругсосредоточилоськсечегоонникогданеузнаетинепойметвщепткуюиветбезыменноевнепрогляднойтенидеревьеввдушликодзапчхегниенряведьонисматерзжздесьсовщемоднииеерукадркюитдадркюитемунепочудилосьноокчегомамавед

ь больше сильнее умнее его не поели он так же чувствует эту неуловимую угрозу то зло
овесечто затаилось там внизу ищейчас выползет из темноты значит мкюновырастии
ксеравно не стать сильным значит стать взрослым вовщ не утешение значит юи зни
нет прибежища нет такой надежной цитадели то устояла бы против на джгсх ся у
жасовно сомнения разрывали его моркюное вновь обожгло его холодом горловщ
евнутри похолодело по спине пошел мороз оледенели руки и ноги ему вдруг стало оче
ньзябвотчновновьяналетели прошлогодкабрьский ветер так тоноптозначитэт
оучась ксехпждейкюодый человек для себя один единственный на свете один единс
твенный сам посебесредивеливогмнкюествоа других людей и вщегда боится вот как в
ейчас ну закричишь станешь звать на помощь вомукавое делотьмапоглотит в одномг
новенье одно чудовищное еленье е мгновенье и ксеконченонщезадолго до рассвет
азадолго до того как полицейскиеначнут прощупывать в твоимифонах ритмичж
растреконеннчжтропинку и на ней зашуршит себень под ногами людей вотoryевсмя
тениикинутся на помощь и даже если они сейчас только пятистчхшагахоттебяапюн
аверно такоиесь темный прибор может зчхлестнуьзатрисекунды и отнять у тебя
ксеткойдесять лет дюизньэто одиночество в незапное открытие обрушилось на томак
аксокрушительный удар и он задрожал маматкюоединока в эту минуту ей нечего наде
яться на святость брака и на заситупжбясейсемьи на вонституцию соединенны
х штатов на полицию ей некому обратиться кроме собственного сердца аксердцес
коемонайдет лишь неодолимое отвращение и страх в эту минуту перед каждым стои
тская только скоя задача и каждый дозюенсамеерешить ты совщемодинпоймиэтора
и вщегда томпроглотил комок застрявший в горле и прижался к материгосподи не д
ай ей умереть моли лоннеделай намни чего плохого папа придет с собранья через час и
если доманикого не будет маьдвинулась по тропинке в дикую чащу мамты задуганебо
йся дрожащим голосом сказал томснимни чего не случилось ты занебо не бойся снимни
чего не случилось он ксегдакозвращаетсяэтим путемголос матери звенелотнапргюе
нряясторазговорила ему ходидругой дорогой ноэти проклятыемальчишки ксеравно
лезутнапролофкогда ибудьонпойдеттуда и больше не вернется больше не вернется
это может означать что угоднобродцгипреступникиьманесчастныислучайаглавно
есмерььодинкоксейселеннойна светемиллионтак ихгородишек вкюдомтакжет
емнотакже одиноко кюдыйтакжеотксегоотрешен вкюдомскоиужасыискоитайн
ыпронзительные заунывные звуки скрипки котмузыкаэтихгородишек безсветаносо
мнкюествомтеней акавоенеобятноенепомерное одиночество вцане ведомые оврагичт
о засасывают как тияшина жизнь вэтихгородишкчхпоночамо борачивается леденя
и мужасомразумсемьедетямсчастжжсоксехсторонгрозитчудисеимякоторомусме
ртьмать снова громвопозвала в темнотудугласдугивдругоба почувствовали что сл
училосьйверчкиумолклисталосовщемтихоони не зналптобываеттакая тишина бес
предельная бездыханная тишина отчего замолчали сверчки отчего какаяэтомупричи
напреждеони нивогданэумолкали и никогдзначитзначитщейчасптотослучитсяказа
лось врагнапрцгаetskoi черныемышцы вбирает вщексесилыспяихгородови ф
ермнамногиемиликокругвеликая тишина пропитанных росой лесовидолини накат
ывджсхсякак прибор холмовгдесобаки задравморды коютна лунку ся собиралась
текалась стцгивалась в одну точку и ксамомщердцетишины были они мама и томвотщ
ейчас щиюминутучтотослучитсяптотослучится сверчки ксемолчатзвезды опустил
ись такнизко что кажется протяни руку и напальцхостанется позолота ихнесчастьзв
ездондюаркиеколючие ксерастетразбужает тишина ксеострейнапаяженной кюида
ниеохкактемнопустыннокак беспрмжтно и вдруг далекодалеко за врагомголосзд

есьмаמידумамаисновамамамаמידушлепшлепшлезмчатсяногивтеннисныхтуфля
хподнуоврагасхохотомнесутсятроемальчишекбратдугласчарливудмениаюонхаф
бегутхохочутзвездывзвилисььвверхточнодесятьмиллионовпюаленныхулитоквтя
нулийвоирожкисверчкизастревоталитемнотаотступалаиспуганнаяошарченная
злобнаяотступилапотеряваппетитведьонасоксемпюособраласьпожививьсяивдру
гейтакгрубопомешалииикогдатеьмнотаотхлынулаточноволнаковремяотливаизнее
козниклисмеясьтроемальчишекмамомприветисразувокругзапчхлодугласомвед
ьотнегоксегдапахнетпотомтракойдеревьямиветвямииручьемвампредстоитпорка
молодойчеловевобявиламамаотеестраховиследанеосталосьтомзналонаникогдаю
юизниинивомупроэтонерасскажетникогданостранэтотнавщегдаостанетсяяунеевду
шеивдушетоматкуюетемнойлетнейночзжонишлидомойспаькакхорошчтодугла
сжикойкакхорошоанаоднусекундутамакраюоврагаемуподумалосьгдетодалеко
посмутномуозаренномулунойлесунадвиадувомпотомвнизуподолинепрогрохота
лпоездонокчаянносвистелточнобезыменныееелезныйзверьзаблудилсявночитом
улегсявпостельиядомсбратомвесьдркюаонприслушивалсякэтомуйвистуидумалд
алеводалевотамгдещейчасмчитсяпоезаюилихдвтжродныйбратиумеротвоспален
иялегкихмноголетназадкотвтакуюоночьдугласлбюалиядомотнегопчхлопотом
изтобылокакколшебсткотомпересталдрожатьтольводдвевнщрянджнавернякадуг
прошепталонкакиеоднаптоночзжпюаснотемнцадругаяеслимистерауфманвогдан
ибудьвсамодделепостроитмчшинусчастьясоврагомейксеравнонесощладатьдугл
аснемногоподумалповториптотысказалониумолклинаулицевнезапнораздалисьш
агиближеблдюевотониужепомдеревьямикозледоманатротуаремамасоскоейкров
атинегрофкосказалапапаидетинеошибласья

Висновки:

У ході виконання цього комп'ютерного практикуму ми розшифрували текст за варіантом за допомогою шифру афінної підстановки для біграм. А також підраховували необхідні дані за допомогою модульної арифметики. Застосовували частотний аналіз для визначення завідомо не відомого ключа до шифротексту. Засвоїли метод «взлому» шифрованого тексту афінної підстановки для біграм, не маючи ключа.