МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра Інформаційної Безпеки

Криптографія

Комп’ютерний практикум №3

Криптоаналіз афінної біграмної підстановки

Мета:

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

Перевірив:

_____

Виконали:
студенти III курсу
групи ФБ-01
Приходько І.Ю.
та Сахній Н.Р.

Київ 2022

Постановка задачі:

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.
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:

1. Найчастіші біграми відкритого та шифрованого тесту мови

1.1. Порівняємо Top-5 найчастіших біграм російської мови (ВТ)

- У російській мові вважається, що п'ятьма найчастішими біграмами (в порядку спадання частот) є сполуки «**ст**», «**но**», «**то**», «**на**», «**ен**».
- Однак під час виконання комп'ютерного практикуму №1 було встановлено, що п'ятьма найчастішими біграмами відповідно є «**то**», «**но**», «**ст**», «**ов**», «**на**».

1.2. Напишемо знайдені Top-5 найчастіших біграм шифртексту (ШТ)

У запропонованому шифртексті, який збережений у файлі **`cipher_text.txt`**, п'ятьма найчастішими біграмами стали наступні сполуки: ['ээ', 'вд', 'гн', 'цг', 'чф']

2. Дешифруємо шифртекст для кожного кандидата на ключ, однак кожний отриманий текст будемо перевіряти на змістовність, а в результаті у звіт випишемо лише істинний змістовний відкритий текст.

➢ Зашифрований фрагмент тексту за варіантом №9 (**`cipher_text.txt`**) ↓↓↓

```
тгтгрэцрюфмнйбмйшугдээдэибггэдайжаишуикггуоитлчмтлвшаэвмхдвдлгцчцмб
пврыэггзухлураятаиэншчфэчучкштфьээзукщтбцнчфвшяфнрагрэцрцлцэюоксбмчф
цгссошпруйедйгцгрэчсммцлжлочщетйсегрхчяэйекааэндвдэчбоцгзгдэыуирщцэ
ээятглпльчкчедйгцгчддфэучюшщясеплэнйфюфюбмйячвдогяфруопогшэпбмйячюоаэ
смплизфрюбдукжюдээщшсвурятаэггшйячбдйгьойсегммцшмэцгпмкаурюбщпдуяфй
шлнрсээпблвтфцшкуцншмймщяээжсшшщятгдэцгчббйядогцоцггнвриэоеканыклгн
урюбдухжогууэчцдябдайгогвшкайгогошплфдошплкуопогруопчсопйчяэаэнссре
луртукжэсфнйфгдэээсглкчрзяаьйемщпмэумвдкгсгнчпщвшзэалжвурдуопогруоп
```

огруопогрухсопогбггнчфьдечхшюбнргдфпчбфэкдчтйгйщнрдуиээдиэвнчфщзгрв
штфвешыэшочйшяаяффдкчвчтшаиешшившэдечлфюфэнветйячыяюшмэсдггснаяээюг
сеелфчкпогюггнодядкчешфчывээечогьоуэучжоьэхшгчэйжутйггдсэдшшветйячы
яцгцлнрэсснаявштэумэтогжлэеблэеишлтдгфшврхлячщшцнбйесгнфртййбмйсстч
жокгпбфэцрюбдувешыючрэщмбйетьдцчкдээпбцдщркжцлураяючржапюфвштэчяьор
этлурюфнрагкдзэцгрэтлурфчычжлиекаэнчфьйзйлуирсмчфцгячьээйуиагшйдрйш
иэпувдюшшишаыэмсвдхтгэкчьчэйыпнрмйчсартйфдчстгщшазззйрэыэчйхялуцшдуо
погошзэалжвурээыунрбдяуэчждэсетьдечнпзякяцгггпмэтссхбмйячюоцгдэявжк
йчггедоддэявжкаиягячеэюшуркйтеопечкгсшцлучщшазелурчбезвчпмцлуруйячэ
рдшртклуйлрфмйшймплэеггдбуйишртгбцшнэгтждтхуэвчээгтждюгэдссммюфябцн
чфцгфэзшмйсссшвриэяэчэсеплэнэвээятрэаржуснцзшуснвдцэюоиэгмкаурмйцзн
рушдуэчтоэчггаувймйсеябчфцньэцдогцояфюфтйкгюгогрэпутфээпбфэпутфаярс
сгжемйээрэврзюйдечдэллцявчяаиечмбэкдрэцрябмйэшфунчгфшйтеюнтйугюоибд
уиэнгждятгльчькснтбитчйэчувюдгнцчыэлгвдфечфучжеуыкчяэьйусигджуиаяьо
жчвшлухжвдгэопогылэеэсвдлуэдэсвдцорэцгжехлвчкдбмюгягшшчфбэреапопечэ
эжечбитогенчфезфрюйэчлмэсглсгвдуггггждцгврзюыщкдкгюдфбцдешймплндешйш
уйэчлгкджлаыэшьяыэфпечрэюгеджчиюуруйогцэмйэчычюшдчялкуггетгмвшеншиг
нвевшзэумшутэкдцрйшкльчькирфпвддбэнушмэучжолвэшйфиэбдяучфзснчгнуявд
шчпэфшуиуйягвдюбэеяукчыээээтждээнчячщшнфйшймэтвчимыщьдечвдэщезюнэни
рхджбнряэаэзгэчвдэчучкшзьшчьччсыэфпечцгэчггауыщрэпмцдштйгвдкгучвдйэ
ьоятцньюятчучфтйкгюгогттгтгвштйндтгогьйьэуицэюохэнечмэечмлнчфишмбмйэ
эпуяищшсннрфмдуезггьоаягэрнщпчфурэвэжюдчсччусцэчяьогтччхштэйэссвшщз
цлфчюрвууиьйтффедаюнчбтйиэгнушкмээкчешфчкпечкмщпсгвштуйскбуяэдэйслц
нэрдшбййббйьоээюоыэчскбцдечфучфширчяэлгыэумнрлвдлюмлсечибчфкдьовшяб
фэцрхчычялиелгвдячтчтогнуявдтчцчввэертдйфруцээщштфьюыэрзюбядгнпмшип
члмэдцгопфсучтчайтеюнбпвчюегмьйцнкчдгяэтажюэеыэшоашсвйшураяплггйнчф
ныжвиявчяэцнсссгдяэсаэкгцгвдюгпдвшиэвнйсцэчйфшцлчджджвдгнеяждчслшнфц
логбшнфюгягйэдйсрхжртбаирэшлщюгфэщруиплггчзгрчдфэюдщдтлфруйетчэубэе
эеяауряэфэедтгттгьйфпсгяэьэцдогыняцээлукчонвштбфэйэедмтяуазцдзсбшлвь
ьсштфвравччмзвджмвштбдуйэедьоцнээяэынвежучфпчлмплюйтеыщлунрбшьзчетй
ьчшнюйдшцнчфдльчггршезгршылныэнцээывтйячщшщяшчсчедиэяэщпвшфмтэцгкгю
гогцойэаэшшшшимззйрэвчешшиггтлурйшшицгсепьплггнгээшсятаэьйфпдузйшняр
снвшкдучяэээцмчфкчешурмйжчянуйтеыщысщгьчдфэеьорнплмйыэйгемчмогвяыдю
чвшэдечвчклччгнярснээцузсжчцчяэжекуяукжкгфруыурипфэлсээзшмэфечфртмс
ягджаиойтеазшчьфнрршоилуурюмаикдыэцулзнрзжзэюшзйкгнчывээцггэятьойэф
эчдпфурэвкмчфкдыэцулзнрзжэшазшусндбвеюнюэрэвдядючдфэеьорночяэтгвчжо
кгойзйтеэшкгдуцггуцстечфтфщзгрплээретфойтфярснвшжемйэсайжаапзяэсглй
чыэитшчюорстэцгдфцнцдибыядэцгкчяэюггнелчдждщртбнфуййшяфбпогюгждюбцн
чфжеэжвдэьедискчщрхчклтгвчжоыэгбвчячиэомвесдямзйжчянрцээыэцутэуфзйв
юдббйдягнуяглдавчйчгтшэыэяэгнврэвкмфдтуйскбвшпрынмэцгкдыэцулзнрзжэш
азшуснссэйлуснушазшусндфояьоаяфрябогкгьохчшсныэшазшуснгээгшшлвээвши
едуфртйуштйэчпцээмзгртйжчянадькзйжчянрцээчсччуснмцнвеоирэщмгглтйгсн
аякчэдедьмшиябыяучэйжакуэеклеяждмзфэедибмэсеопйдгтндсгснйекафрлуйги
пдужеэщдуюнхьсгнцээкпведуцгрнисвдхтцуклжвэеюфцльчцуэнтфиэынезцсшдьо
нчыкйшшаюбмйвчшшхчтебпдутээсшдкнцчыцээдфэеьоиэьчцвтйсстштбфэгнмйжчя
нблрншивчтшуииэудрэьуурюмяфлаэчзуюфйшишфпвекачфцгкрчшврпльчынмэкддб
мнурэдечвдщрлжурюгьйкйьэцылажоуэааыщвчятйгайрдэээсаэкдшэцруйтецнпгг
глаыжапурябчбфэээьнишиэмсбтягюшшиычмштфтечбйшючрэеззйээфэртусгнвемй
огшэкшщятехлфдршуифечфыэкчмфнрзшцнцчигвдылэеимюнчфрэщркжиэччаюфэнэ
еььцэюохэбщггмешижеюмггошшифпдажкюнкдпччэальчяэылснэнймтуьэтфвшэжвд
эжвдцлцнмйлгиээдвдцоцгзгдэьмггююцлфрлажюхдплггцаечцонцээгбфэяггнябм

йцчедучкшшиагщэяттуйсяймйцчгэээудаэцоьйжвфпмэюшкмщпсгкчшацгснйштбши
жчальчыншыцлсншччтжчюшочрштбфэаржуиэвнэшлуэеклачюлшукжвдьэыаюбыщфпк
дэшьяхляуюэкддфэнэеььзузйюйпльчдэшшхдйчйскгшешыюнсгшешыюнтфцштблвшу
фрмйушмэывфпчфюфхляуцзнрзжзйфрушйчмфкчйчяэкчныирхдвшэншыжвдлгнпсснр
нцшысаээдшсясфедалндааээчычжвээюглгфрмйинюфршлагдьчцвтйгтрэчаснлаяч
щшцнщацгудифшыиэгттгггнхдьйэехлиэкчгнэнюйфрушнфешсвюнгнэнблеемйитзлп
льчкчлнржэшхчешсвюнзылакдкчибцдшчндигкчзнймшицгечбшшипдлгечвдынбсгн
уяогятжецнцлцгжлбппьыдййгсщгшэршлвуйчфкчкддекаэтйгвдфпчфвешыэшочршп
люэцэшпаэтфкщнрдучфяэхрпльчршлнцдрэйэаэечаэрэдбйштбхжирдэфэпэвчечкч
вдйсюдйшщпхчшстуйсяйлгаэлвэшхаззыэээзшплиэшоцгвчячвдьбфэцрщпдуюмлзт
опмаиэчячянймьэээиэындацгудпцээавтйьоьйрщэьечомяылтцвирплюмдройазоэ
едкчедийалэшртнштйэчячдуйшяуйшгнэчюшоизгпбмйаззйцчедэчвдыэяэщшшызйа
лкуйсбдкрвууицльчцулзодэйслцнкгыйуиагошшаймцдудуогнишржхайгьоцгрэдэ
чоыэшскгыэяуирцнйфюбщпаэядалдуиэспиээчжозэшшлвшуплзкиэиряуэшвкйчспи
ээчжойдьйюмвшучиэькяакунряэгэггшйэчлгюггэнпдуцнщпгмймрэвдпччйюдэшсв
эсибфэосштйгьоылодждеэцгцдкгждячщшюьгггнцчьэнчюшюьтечбйшрсйшишуиюгк
сюжюнычшчжорэшшщпюффрвууиыээээтклдфшнэшхдюдэсэйдшюбчфакадсгнчзйвдвш
уйуиаггннрфмплчяядгныщдгнгйэзназэгныцгэчкшцнймвшодзйьоячщшоижемзшид
энчфаыщвчгнэсьоюгтеуйюмцшлтуэтшшнтсячюяьйсньэлузйшнярснаылажорнмэед
иэучгньэршяаюбиэээумэтядзэмекжфрмйушэнчфймймшэсекжюнирушоишуиеуэаак
уфэщглфюфэншызэедиэкгнцссждэсссуикчучяэцгечшнюйдшйштйвяээгнцзггкгкд
цгюгыдссэьюяыччйтфадкдцгыэийядсспдкйочедкчюшлщанэнплкдцгрэвдпдмчншю
мыэшсезггядьоаясечфзйезгнэчюшщпмйэецюбгьйэецюзйьэтфвшишяиечюрэжушзэ
гэвддэээалггычкдйдгнггмлрнмфйшлнмбэеяукггунфгнодэйьэшннрфммйьэжакус
вфдкггуоигэмыэшзгжчэержюнинвйпльчдэедубшиждрнвекайшхльчцуэнчфжещпаэ
ядцмчфгмюггныяджаиипвевчябцдщгайемтгячцдяэдбдуйшяуяиуимфэеснйфнрфрв
шкчечогншюфкдучяэсрхщщпчбюбюбцдечэйшэмеишьяучцчовтйхчщрлучфишкмщпвш
азшуснтгьожлйшвртййбцнфэтдямкледрсйвжкмфюфетюгчснгкчцэчйжуфэщгыдспн
рмйчфпмкаурээдйкдщштвфпвшзйфсудаэцоетюгкчяэкчцэчйойкдщштвфпвшзйфсуд
аэцовшьйфпсгьэтлггигснаярняфесячспнрмйтгячцдтлэширцнцгжеьыэшьяойээг
гэпплвефрфчшсйэедшеопшигэфэяэншяцяджегмзяеттфурэвэжюдьйэехлиэвчдстш
юбфэаэьмщпсгкдлсбовшрэпуснсссгмзнрзжэшклэекчэйззнрзжэшклэекчэйбцээд
энчээешсвэнэвээопдуиэмедуыпябцчгнмбкдюдьотгкччвтйтшоищравяиапогршоч
дфэеьодуйшьэьйуиьйирэшиэнштйэчячждбруэтнймэщяэфэедччюдсмяыгэонймнчя
чщшцнймнчдуйшгмгмяылтвнймнчцньйфпмэтержэшсмяыгэдйьэисщгбтуйьэюняирт
жевшсдячюортяазсртршдчтлчмуйсеябюдьэифшашмецядцпведуэжюмшчпйэчлгиэш
эщшшызйалчфячкчжгкгыээшээюятшочкчрэжчкшочдуйшлвзйальгкчэчгэмтззреап
твээюгзгбтйгфнкгжныяьдцгндешблрнэщяэфэедммыщрэиэагдэцэггудйгснаявче
чпяыдшсщгшэщекамфбйтфачечдядйаггнььшэьйрщгнвевшфедаюнжседычяфемцнве
чфбйжчянйфэнюйиэйгфечфыэрэтлурхлячщшцншуопогруопцлшеопезюблвдлгньэй
гвдынцнмйфсудаэцоылэеимисдэцмвдгнурмйпльчонэщмэкдкчешурынезелфчзнйм
щяядчдцгшчдбцчечюоцгззяалтчгюшщяядчдцгцнучяэюгдэявуруйэчувюдцнучяэк
гкгбцээшсжетвйшюбцчгузэкдкдыэцуишысдэцмурйшкмщпсгешсвюнешсвюньчцвтй
ынцнмйфсудэйемкаурмйюэреапцгжеыпфчэйьэтвэерттфлжхтузйефчальчюяьйзйф
рвйчяыдцпведуыээдзчафцгщшщпхчждвдьэсеопэчвдкгшнэжйшюбфэтдлгюшлщфэшэ
шрзйпллунрйшйшймэнелпьыдййемймжемзшийэлфплцузйезймлакуггжфвелтьэфнц
гфсэсьйойезйеуртйюйячкгогцогныпцлуртйблдуэсээимгдьйюфчфьчмупчядчдрт
ятвдвшяфюффдээзлцньчцвтйьдхфйшлнавээээщравюнаяынцнмйфсудэйойэчувюдь
йтфнрагфаэчзувэесгнфруйинймкджмлвээкгнчэйщбфэдякдйсрсйшюбурсюыщмйлг
кчэйщбданрцнфдяшзйучгнхаэчзувшаыиеюдюмнрйвхчьйэетйячтекалсчгснядчдц
гьйзэгнцчншюбыянчюшуишылуишхчхщкгжнтфиэесгнчшиэкгфззйжерьтшодтуйсцу

урюмдуурюмдатэреапчфяэаэаязузййфюфлумфюффдошплюфюфюфюфлукжвчщжвчщжв
чыфагэйдшщпцлячюшуйртунахзяфбдуэсплггнгвщхщцнчфкчнсэйшнфэтфурэвэжюм
меэнчсартйагхрцлшужчкдпывшчгюзфплнйэйэжсфаэчзуелтлфруйблэчющээзшдуз
йшнйффрвдвшплныурэшртюсвдээялдяэсвдылодфэвмуйэчувюдюггнцчыэлгвдячщш
цнтээйссягогуйеснгюшщяхжиеыжэшцгжааэмшщяцнгнмбфрюбцнэеслюбтчядаляую
эцгшэьйтфнызйезггогцорэндэдьоаяцлшеопуилгйпйсцэрэжчдгвдкмщпсгячщшцн
тэжщитэсогээзшплнрцгьэретфоэюрцлфдешйчьэешкмвддфояцотеочтгюоудччзфю
фээпбцдэчядоекадлгмйсцаюбыщаэчсартйчфэчбоцнкчяэьйфпсгягяшснрэээонгг
ьэпуэеклеяждэчалщфхдйспотфйгпбцчгйээюнрэлмюфнрдушиучаээчыэюяэдогтгт
гцнйчгнггйээдщряуишзэгнурмйинчфешурвшишкмщпсгзылакдкдыэшсжеяцээкчгг
шйкгнчтшкмщпсгиэгнггыцээтшхльчцутэгнишснаяцшйчтукжйдтукжснчфэншыснт
фиэшрснкчншлвьььвшэжвдгэдэчйягьокгещвехжлвээчсартйндьэомймйэфэхэиштэ
шшбйюмцшчслгщшймггкэреапфчшсрэчстгаэцоцусндуурюмчбмйшстшчфбэюгцчюшч
фврцшшивчнсцгжлвгчсыэпбцнчфршламбдунрйштбфэфехщцнуррэяагэиэывщяюшмй
эдгнирээзшезяанфэшртдыиряартпаэчтоюгчршуфраяршлвюнчфврфпаяжбмйячюоы
ягэдймеэнчфэчцошешытэубцдщркжцлураяоцээшсылуйсслумфурсгвчыэсгвчыэлг
спечьчцвтйгвюнаярэяапыфрэщжлйьфэшшоимеэнисжчфэалмйягвчкдпрфпюдффиэя
эвчтшкакуьэаллгрсцыэшлвхуопогщруыурыягэдэтшфпчбыщаэрэээждрнезгргмйм
ьэйжазгньэээпбэезйлгчуфэщгьоээюоыэжлклькьяешпьцгэчкшемкуопжехжтблга
эямймхчдуцгынвшлвььныгтйиэячщшьгшеопщязйвджднэезсрфишыэцуишмзшублзг
дэыуиртбмйтеодифыжйшбйаггнеяшэреапчфуиьйэехлиэкчшэыркуэнхуопогоштфи
эяэрэчстглбплээцдынцнвйкгюгаэкдмфнрэрйшзсвдпчршяаюбиэггзууруйзжапмз
вднччраыклцнвшиснчрэьуэеклеяждьэрряучфишэнфэссиетфюфтймйьэуисеплэнй
шфпфэьммйкгюгогягяглуснйшзэчдчртймг

➢ Дешифрований текст (**decrypted_text.txt**) за допомогою знайденого ключа:

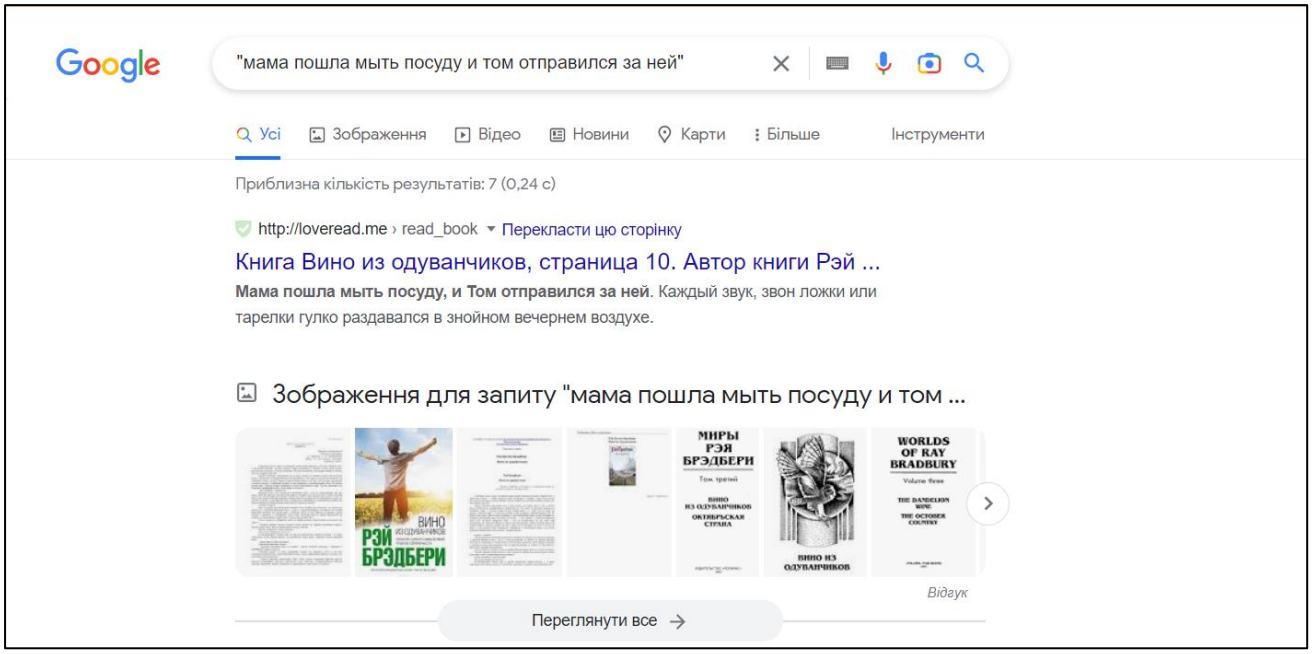
- Key: **a = 314, b = 34 | (a,b) → (314,34)**

мамапошламьтыпосудуитомотправилсязанейкаждьйзвукзвонложкиилитарелки
гулвораздавалсявзнойномвечернемкоздухепотомонимолчапошливболышуюком
натуснялисдиванаподушкивдвоемраскрьлиегоиразложиливедынасамодделеэт
обьлвовщенедиванашироченнаякроватымамапостелилаимсдугласомпостелыло
вковзбилаподушкитомначалбьлорасстегиваыырубашкуноонасказалапогодими
нуткутомпочемунадоткакаяточуднаямамонаопустиласынастулносразпюевст
алаподошлакдвериипозвалаоназваласновaисновадугласдугдуугееголосупль
валвдушнуютымуитонулвнейбезксякогоотклikадажеэхонеотвечалодугласдуг
ласдугласдуууглааастомщиделнаполуиегопронизьвалхолодновинойтомубьло
неморкюеноеинезимаинелетнийзнойонвиделмаматорастеиянноозираетсятоза
крьваетглазастоитинезнаекчтоделаыыиоченыколнуетсядасразувиднорастеи
янаиволнуетсяонаоткрьладверыверандьшагнулавтемнотуспустиласыпоступе
ныкампрошлаподоркюкеподкустьщиренитомприслушивалсякеешагамонаопяыып
озваламолчаниеонапозвалаеседвараза томксесиделвкомнатекотсейчассдлин
нойдлиннойузвойулицьдонещетсцголосдугласаидумамнебесповойсяяидуноду
гласнеотвечалтоддолгиедвеминутьщиделглядянараскрьтуюпостелынамолчащ
еерадиоимолчащийпатефонналюстругдекакнивчемнебьвалопоблескивалистек
лянньевисюлыкинаковерраспиcанньйпунцовьмиифиолетовьмизавитушкамипот
омнарочностукнулногойокроватычтобьпоглядетыбудетлиболыноокazалосыбо
лынодверыверандьсоскрипомоткориласыимамасказалапойдемтомпройдемсяку
дапростопоулицеидемонвзялеезарукуонипошлипосентджеймсстритасфалытпо
дногамибьлвщенщетепльйсверчкистревоталигромчепрбюнегоксгущавшейсяыы
меонидошлидоуглайвернулиидвинулисыпонаправлениюкзападномуоврагугдет

опропльлавтомобилысверкнулвдалифараминаулицчхникакихпризнаковжизнин
исветанидвдюенрявоегдепозадимерцалислабоосвесенньеквадратьоконвтойс
торонеоткудаонишлиневщенщелеглиспатынооченыоченымногиедомаужестояли
безогнейиспалиапередневоторьмитожетемньминакрьлечкчхщиделииихобитате
лиивполголосавеливечернвжбещедувоегденаверандчхпоскрипьваликачелихо
ыыбьотнцбьлдомасказаламамаонасжималакскоейболышойрукерукутоманупост
ойдаймнетолыкодобраыысядоэтогомалычишкидушегубопяыывьшелнаохотуонуб
иваетлюдейксемгрозитопасностыниктонезнаетгдеикогдаонвдругпоявитсяво
тклянусыпусыытолыводугпридетдомойяеготавотколочувекбудетпомниыыонип
рошлиесекварталитеперыстоялипередчерньмсилуэтомнемнцвойбаптистскойц
ерквинауглучепелстритигленрокксотнешаговзацервовыюначиналсяоврагтом
пюечуялегооттудатянулоканализационнойтрубойсгнившимилистыямидушньми
влажньмзапахомсплошньхзеленьхзаростлейоврагбьлширокийизвилистьйонпер
ерезалгородимамаксегдагокорилаптоэтоиднемтонепроходимьедебриаужночз
жкнемулучшеиблизконеподходиыыоттогопторядомцерковыстрчхидолжндбьрас
щеятысянотомувщеравнобьлкюутвовэтокчастемнаябезединогоогонькаонаказ
аласыхолоднойибесполезнойразвалинойнакрджоврагатомубьлоксегодесятыл
етонничеготолкомнезналосмертистрчхэужащесмерыыэтовосвоваякуклавясик
еонвиделеевшестылеттогдаумерегопрадедушкаилбюалвгробуточноогромньйу
павшийястреббепмолвньйидалекийнивогдаболышеоннескажекчтонадобьыыхор
ошиммалычикомнивогдаболышенебудетспоритыополитикесмерыыэтоегомалены
каясестренкаоднаждьутромемубьловтовремясемылетонпроснулсязаглянулве
евольбелыкуаонасмотритпиямонанегозастьвшимислепьмисинимиглазамиапот
омпришлипждииунеслиеевмаленывойплетенойкорзинкесмертыэтовогдаонмеся
цспустястоялвозлееевьсовогостулычикаивдругпонялптоонанивогдаболышен
ебудеттутсидетынебудетсмеяыысяилиплакаыыиемупюенебудетдосадночтоона
родиласынасветэтоибьласмертыинщесмертыэтодушегубкоторьйподкрадьвает
сяневидифкойипиячетсязадеревыямиибродитпоокругеивьжидаетиразилидвав
годприходитхждавэтотгороднаэтиулицьгдевечерамивщегдатемноптобьубиыы
жеещинузапоследниетригодаонубилтренэтосмерыынощейчастутнепростосмер
тывэтойлетнейночипомдалекимизвездаминанегоразомнахльнуловщептоонисп
ьталвиделисльшалзаксюскощюизныионзчхлебьвалсяитонулонисошлистротуар
аизчшагалипопроточтаннойусьпанной себнемтропинкепообестороньгусторос
ласорнаятраваивнейгромвонеумолчнотрещалийверчкитомпослушношелзамате
рзжболышойхрабройпрекраснойегозащитницейотвщегойветатаквдкоемонишли
ишлиивотостановилисынасамофкраюцивилизацииоврагздесывэтойпропастипо
средичерной чащобьвдругсосредоточилосыксечегоонникогданеузнаетинепой
метвщепткюиветбезьменноевнепроглядной тенидеревыеввудушликодзапчхегн
иенряаведыонисматерзжздесысовщемодниииерукадркюитдадркюитемунепочуд
илосыноокчегомамаведыболышесилынееумнееегонепюелиионаткюечувствуетэ
тунэуловимуюугрозутозловесеечтозатаилосытамвнизуищейчасвьползетизте
мноть значитмкюновьрастиикссравнонестатысилыньмзначитстатывзросльмво
вщенеутешениезначитююизнинетприбежищанеттакойнадежнойцитаделиптоуст
оялабьпротивнадвигджсихсяужасовночисомненияразрьвалиегоморкюеноевно
выобожглоемухолодомгорловщевнутрипохолоделопоспинепошелморозоледене
лирукииногиемувдругсталооченызябвоточновновыналетелиппрошлогодекабр
ыскийветертаккотоноптозначитэтоучасыыксехпждейкьюдьйчеловекдлясебяо
динединственньйнасветеодинединственньйсампосебесредивеливогомнкюест
вадругихлюдейивщегдабоитсяваткавсейчаснузакричишыстанешызваыынапомо
щывомукавоеделотымапоглотитводномгновеныеодночудовищноеледенящеемгн
овеныеиксеконченонщезадолгодорассветазадолгодотогокакполицейскиенач

нутпрощупьваыыйвоимифонарикамитемнчжрастрекоженнчжтропинкуинанейзаш
уршитсебеныподногамилюдейвоторьевсмятениикинутсянапомощыидажееслион
исейчастолыковпятистчхшагахоттебяапюнавернотаконоиесыытемньйприбойм
ожетзчхлестнуыызатрисекундьиотнятыутебяксеткоидесятылетдюизныэтооди
ночестковнезапноеоткрытиеобрушилосынатомакаксокрушителыньйударионза
дрожалмаматкюеодинокавэтуминутуейнечегонадеятысянинасвятостыбракани
назаситупжбясейсемыининавонституциюсоединенньхштатовнинаполициюейне
квомуобратиыысякромесобственногосердцааксердцескоемонанайдетлишынео
долимоеотвращениеистрахвэтуминутупередкаждьмстоитскоятолыкоскоязада
чаикаждьйдозюенсамеерешитытьсовщемодинпоймиэторазинавщегдатомпрогло
тилкомокзастиявшийвгорлеиприжалсякматеригосподинедайейумеретымолило
ннеделайнамничегоплохогопапапридетссобранрячерезчасиеслидоманикогон
ебудетмаыыдвинуласыпотропинкевдикуючащумамтьзадуганебойсядрожасимго
лосомсказалтомснимничегонеслучилосытьзанегонебойсяснимничегонеслучи
лосыонксегдакозвращаетсяэтимпутемголосматеризвенелотнапргюенряястор
азговорилаемуходидругойдорогойноэтипроклятьемалычишкиксеравнолезутн
апролофкогданибудыонпойдеттудаиболышеневернетсяболышеневернетсяэтом
ожетозначатычтоугоднобродцгипреступникиыыманесчастньйслучайаглавное
смерыыодинкоксейкселеннойнасветемиллионтакихгородишекивкьюдомтакжет
емнотакжеодинококьюдьйтакжеотксегоотрешенвкьюдомскоиужасьискоитайнь
пронзителыньезауньвньезвукискрипкикотмузькаэтихгородишекбезсветанос
омнкюествомтенейакавоенеобятноенепомерноеодиночествцаневедомьеовраг
ичтозасасьваюткактиящинажизнывэтихгородишкчхпоночамоборачиваетсялед
енясимужасомразумусемыедетямсчастзжсоксехсторонгрозитчудисеимякотор
омусмертыматысновагромвопозвалавтемнотудугласдугивдругобапочувстков
алиптотослучилосыйверчкиумолклисталосовщемтихоонинезналптобьваеттак
аятишинабеспределынаябездьханнаятишинаотчегозамолчалисверчкиотчегок
акаяэтомупричинапреждеонинивогданэумолкалиникогдазначитзначитщейчас
птотослучитсяказалосыоврагнапрцгаетскоичерньемьшцьвбираетвщебяксеси
льспясихгородвовифермнамногиемиликокругвеликаятишинапропитанньхросо
йлесовидолининакатьвджсихсякакприбойхолмовгдесобакизадравмордькоютн
алунуксясобираласыстекаласыстцгиваласыводнуточкуиксамомщердцетишинь
бьлионимамаитомвотщейчасщиюминутучтотослучитсяптотослучитсясверчкик
семолчатзвездьопустилисытакнизкочтокажетсяпротянирукуинапалыцчхоста
нетсяпозолотаихнесчестызвездондюаркиеколючиексерастетразбухаеттишин
аксеострейнапияженнейкюиданиеохкактемнопустьннокакбеспрмжтноивдругд
алекодалекозаоврагомголосяздесымамидумамаисновамамамамидушлепшлепшл
езмчатсяногивтеннисньхтуфляхподнуоврагасхохотомнесутсятроемалычишек
братдугласчарливудмениаюонхафбегутхохочутзвездьвзвилисывверхточноде
сятымиллионовпюаленньхулитоквтянулийвоирожкисверчкизастреволитемн
отаотступалаиспуганнаяошарчшеннаязлобнаяотступилапотеряваппетитведы
онасоксемпюесобраласыпоживиыысяивдругейтакгрубопомешалиикогдатемнот
аотхльнулаточноволнаковремяотливаизнеекозниклисмеясытроемалычишекма
мтомприветисразувокругзапчхлодугласомведыотнегоксегдапахнетпотомтра
койдеревыямиветвямииручыемвампредстоитпоркамолодойчеловевобявиламам
аотеестраховиследанеосталосытомзналонаникогдаююизнинивомупроэтонера
сскажетникогданостранэтотнавщегдаостанетсяунеевдушеивдушетоматкюете
мнойлетнейночзжонишлидомойспаыыкакхорошочтодугласжикойкакхорошоанао
днусекундутамнакраюоврагаемуподумалосыгдетодалекопосмутномуозаренно
мулунойлесунадвиадувомпотомвнизуподолинепрогрохоталпоездонокчаяннос
вистелточнобезьменньеюелезньйзверызаблудилсявночитомулегсявпостелыи

ядомсбратомвесыдркюаонприслушивалсякэтомуйвистуидумалдалеводалевота
мгдещейчасмчитсяпоезаюилихдвтжродньйбратиумеротвоспалениялегкихмног
олетназадкотвтакущюеночыдугласлбюалиядомотнегопчхлопотомиэтобьлокак
колшебсткотомпересталдрожаыытолыводвевнщрязнджнавернякадугпрошептал
онкакиеоднаптоночзжпюаснотемнцадругаяеслимистерауфманвогданибудывса
модделепостроитмчшинусчастыясоврагомейксеравнонесощладатыдугласнемн
огоподумалповториптотьсказалониумолклинаулицевнезапнораздалисышагиб
лижеблдюевотониужепомдеревыямикозледоманатротуаремамасоскоейкровати
негрофкосказалапапаидетинеошибласыа



Висновки:

У ході виконання лабораторної роботи були здобуті практичні навички частотного аналізу на прикладі розкриття моноалфавітної підстановки. При цьому ми здобули досвід у розв’язуванні основних задач модулярної арифметики.

Ми провели своєрідну атаку на афінний шифр, при цьому знаючи лише зашифрований текст. Основний метод, що допоміг дешифрувати ШТ, називається частотний аналіз тексту. Він ґрунтується на такому спостереженні: афінний шифр зберігає статистичні властивості мови, пов’язані із частотами біграм.

Щоб повноцінно знайти ВТ із шифрованого тексту, заданого відповідно за варіантом, необхідно було також реалізувати автоматичне визначення змістовного тексту, оскільки правильний ключ при розшифруванні дає змістовний текст, в той час як неправильні ключі будуть давати випадкові тексти.