Міністерство освіти і науки України
Національний технічний університет України
"Київський політехнічний інститут імені Ігоря Сікорського" Фізико-технічний інститут

КРИПТОГРАФІЯ
КОМП'ЮТЕРНИЙ ПРАКТИКУМ №3

Криптоаназіл афінної біграмної підстановки

Виконали:
Вісловух Владислав
Ісаченко Федір
Варіант 9

Група: ФБ-06

Київ - 2022

Мета роботи

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

Порядок виконання роботи

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

Хід роботи

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.

Спочатку ми реалізували розширений алгоритм Евкліда extended_euclid, який окрім НСД знаходить також такі числа x та y що ax+by=НСД(a, b). Потім використовуючи цю функцію, ми написали функцію get_inverse, яка знаходить обернений за множеннням елемент до числа a за модулем n.

Далі ми реалізували одразу 3 функції: solve_linear_comparison, get_first_key_element, get_second_key_element. Перша функція розв'язує нам наші лінійні рівняння, а дві інші існують для того, щоб отримувати першу та другу пару коренів.

2. За допомогою програми обчислення частот біграм, яка написана в ході виконання комп’ютерного практикуму №1, знайти 5 найчастіших біграм запропонованого шифртексту (за варіантом).

Ми взяли функцію з попередньої лабораторної для пошуку біграм і переписали її так, щоб ми могли сортувати, та вибирати крок. Нам ця функція потрібна для 5 найчастіших біграм і перевірки на ентропію різних текстів для ключів.

5 найчастіших біграм
[('ээ', 102), ('гн', 69), ('гг', 64), ('эч', 63), ('вд', 60)]

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).

Для цього пункту була написана функція bigram_to_number, яка переводить букви до в індекс числа в алфавіті. За формулою нижче:

$$(x_{2i-1}, x_{2i}) \leftrightarrow X_i = x_{2i-1}m + x_{2i}.$$

Потім була написана функція gnc_keys, в якій виростовується всі вище перечисленні функції. Вона бере найчастіші біграми в нашому тексті і найчастіші біграми в російській мові, потім перетворюємо їх на числа.

Після цього ми формуємо всі можливі набори біграм, щоб на їх основі скласти системи рівнянь і знайти корені.

4. Для кожного кандидата на ключ дешифрувати шифртекст. Якщо шифртекст не є змістовним текстом російською мовою, відкинути цього кандидата.

Для цього було реалізовано функцію check_text_correctness, яка перевіряє ентропію для букв в тексті і для біграм в тексті. Так ми перевіряли змістовності тексту, дивлячись на ентропію, яка повинна бути в діапазоні від 4.2 до 4.5.
Таким чином ми підібрали ключ, який розшифровую наш текст (314, 34).

Шифротекст

тгтгрэцрюфмнйбмйшугдээдэибггэдайжаишуикггуоитлчмтлвшаэвмхдвдлгцчцмбпврыэггзухлу
раятаиэншчфэчучкштфьэ
зукщтбцнчфвшяфнрагрэцрцлцэюоксбмчфцгссошпруйедйгцгрэчсммцлжлочщетйсегрхчяэйека
аэндвдэчбоцгзгдэыуирщц
ээятглпльчкчедйгцгчдфэучюшщясеплэнйфюфюбмйячвдогяфруопогшэпбмйячюоаэсмплизфр
юбдукжюдээщшсвурятаэггшй
ячбдйгьойсегммцшмэцгпмкаурюбщпдуяфйшлнрсээпблвтфцшкуцншмймщяээжсшшщятгдэцг
чббйядогцоцггнвриэоеканыкл
гнурюбдухжогууэчцдябдайгогвшкайгогошплфдошплкуопогруопчсопйчяэаэнссрелуртукжэсф
нйфгдэээсглкчрзяаьйем
щпмэумвдкгсгнчпщвшзэалжвурдуопогруопогруопогрухсопогбггнчфьдечхшюбнргдфпчбфэкд
чтйгйщнрдуиээдиэвнчфщз
грвштфвешыэшочйшяяффдкчвчтшаиешшившэдечлфюфэнветйячыяюшмэсдггснаяээюгсеелф
чкпогюггнодядкчешфчывээеч
огьоуэучжоьэхшгчэйжутйггдсэдшшветйячыяцгцлнрэсснаявштэумэтогжлэеблэеишлтдгфшврх
лячщшцнбйесгнфртййбмй
сстчжокгпбфэцрюбдувешыючрэщмбйетьдцчкдээпбцдщркжцлураяючржапюфвштэчяьорэтлур
юфнрагкдзэцгрэтлурфчычжл
иекаэнчфьйзйлуирсмчфцгячьээйуиагшйдрйшиэпувдюшшишаыэмсвдхтгэкчьчэйыпнрмйчсарт
йфдчстгщшаззйрэыэчйхялу
цшдуопогошзэалжвурээыунрбдяуэчждэсетьдечнпзякяцгггпмэтссхбмйячюоцгдэявжкйчггедод
дэявжкаиягячеэюшуркй
теопечкгсшцлучщшазелурчбезвчпмцлуруйячэрдшртклуйлрфмйшймплэеггдбуйишртгбцшнэгт
ждтхуэвчээгтждюгэдссмм
юфябцнчфцгфэзшмйсссшвриэяэчэсеплэнэвээятрэаржуснцзшуснвдцэюоиэгмкаурмйцзнрушду
эчтоэчггаувймйсеябчфцн
ьэцдогцояфюфтйкгюгогрэпутфээпбфэпутфаярссгжемйээрэврзюйдечдэллцявчяаиечмбэкдрэцр
ябмйэшфунчгфшйтеюнтй
угюоибдуиэнгждятгльчькснтбитчйэчувюдгнцчыэлгвдфечфучжеуыкчяэьйусигджуиаяьожчвш
лухжвдгэопогылэеэсвдлу
эдэсвдцорэцгжехлвчкдбмюгягшшчфбэреапопечээжечбитогенчфезфрюйэчлмэсглсгвдуггггждцг
врзюыщкдкгюдфбцдешйм
плндешйшуйэчлгкджлаыэшьяыэфпечрэюгеджчиюуруйогцэмйэчычюшдчялкуггетгмвшеншиг
нвевшзэумшутэкдцрйшкльчьк
ирфпвддбэнушмэучжолвэшйфиэбдяучфзснчгнуявдшчпэфшуиуйягвдюбэеяукчыээээтждээнчя
чщшнфйшймэтвчимыщьдечвд
эщезюнэнирхджбнряэаэзгэчвдэчучкшзьшчьччсыэфпечцгэчггауыщрэпмцдштйгвдкгучвдйэьоя
тцньюятчучфтйкгюгогтг
тгвштйндтгогьйьэуицэюохэнечмэечмлнчфишмбмйээпуяищшсннрфмдуезггьоаягэрнщпчфурэв
эжюдчсччусцэчяьогтччхш
тэйэссвшщзцлфчюрвууиьйтффедаюнчбтйиэгнушкмээкчешфчкпечкмщпсгвштуйскбуяэдэйслц
нэрдшбййббйьоээюоыэчскб
цдечфучфширчяэлгыэумнрлвдлюмлсечибчфкдьовшябфэцрхчычялиелгвдячтчтогнуявдтчцчвв
эертдйфруцээщштфьюыэрз
юбядгнпмшипчлмэдцгопфсучтчайтеюнбпвчюегмьйцнкчдгяэтажюэеыэшоашсвйшураяплггйнч
фныжвиявчяэцнсссгдяэсаэ
кгцгвдюгпдвшиэвнйсцэчйфшцлчджджвдгнеяждчслшнфцлогбшнфюгягйэдйсрхжртбаирэшлщю

гфэщруиплггчзгрчдфэюдщдтл
фруйетчэубэеэеяауряэфэедтгтгьйфпсгяэьэцдогыняцээлукчонвштбфэйэедмтяуазцдзсбшлвььс
штфвравччмзвджмвштб
дуйэедьоцнэээяэынвежучфпчлмплюйтеыщлунрбшьзчетйьчшнюйдшцнчфдльчггршезгршылны
энцээывтйячщшщяшчсчедиэяэ
щпвшфмтэцгкгюгогцойэаэшшшимззйрэвчешшиггтлурйшшицгсепьплггнгээшсятаэьйфпдузй
шнярснвшкдучяэээцмчфкчеш
урмйжчянуйтеыщысщгьчдфэеьорнплмйыэйгемчмогвяыдючвшэдечвчклччгнярснээцузсжчцчя
эжекуяукжкгфруыурипфэлс
ээзшмэфечфртмсягджаиойтеазшчьфнрршоилуурюмаикдыэцулзнрзжзэюшзйкгнчывээцггэятьо
йэфэчдпфурэвкмчфкдыэцу
лзнрзжэшазшусндбвеюнюэрэвдядючдфэеьорночяэтгвчжокгойзйтеэшкгдуцггуцстечфтфщзгрп
лээретфойтфярснвшжемй
эсайжаапзяэсглйчыэитшчюорстэцгдфцнцдибыядэцгкчяэюггнелчджджщртбнфуййшяфбпогюгж
дюбцнчфжеэжвдэьедискчщр
хчклтгвчжоыэгбвчячиэомвесдямзйжчянрцээыэцутэуфзйвюдббйдягнуяглдавчйчгтшэыэяэгнвр
эвкмфдтуйскбвшпрынмэ
цгкдыэцулзнрзжэшазшуснссэйлуснушазшусндфояьоаяфрябогкгьохчшсныэшазшуснгэзгшшлв
ээвшиедуфртйуштйэчпцээ
мзгртйжчянадькзйжчянрцээчсччуснмцнвеоирэщмгглтйгснаякчэдедьмшиябыяучэйжакуэеклея
ждмзфэедибмэсеопйдгт
ндсгснйекафрлуйгипдужеэщдуюнхьсгнцээкпведуцгрнисвдхтцуклжвэеюфцльчцуэнтфиэынезц
сшдьончыкйшшаюбмйвчшш
хчтебпдутээсшдкнцчыцээдфэеьоиэьчцвтйсстштбфэгнмйжчянблрншивчтшуииэудрэьуурюмяф
лаэчзуюфйшишфпвекачфцг
крчшврпльчынмэкддбмнурэдечвдщрлжурюгьйкйьэцылажоуэааыщвчятйгайрдэээсаэкдшэцруй
тецнпггглаыжапурябчбфэ
ээьнишиэмсбтягюшшиычмштфтечбйшючрэеззйээфэртусгнвемйогшэкшщятехлфдршуифечфы
экчмфнрзшцнцчигвдылэеимюн
чфрэщркжиэччаюфэнэеььцэюохэбщггмешижеюмггошшифпдажкюнкдпччэальчяэылснэнймт
уьэтфвшэжвдэжвдцлцнмйлгиэ
эдвдцоцгзгдэьмггююцлфрлажюхдплггцаечцонцээгбфэяггнябмйцчедучкшшиагщэяттуйсяймй
цчгэээудаэцоьйжвфпмэюш
кмщпсгкчшацгснйштбшижчальчыншыцлсншччтжчюшочрштбфэаржуиэвнэшлуэеклачюлшук
жвдьэыаюбыщфпкдэшьяхляуюэкд
дфэнэеььзузйюйпльчдэшшхдйчйскгшешыюнсгшешыюнтфцштблвшуфрмйушмэывфпчфюфхл
яуцзнрзжзйфрушйчмфкчйчяэкчны
ирхдвшэншыжвдлгнпсснрнцшысаээдшсясфедалндааээчычжвээюглгфрмйинюфршлагдьчцвтй
гтрэчаснлаячщшцнщацгудиф
шыиэгтгггнхдьйэехлиэкчгнэнюйфрушнфешсвюнгнэнблеемйитзлпльчкчлнржэшхчешсвюнзыл
акдкчибцдшчндигкчзнймши
цгечбшшипдлгечвдынбсгнуяогятжецнцлцгжлбппьыдййгсщгшэршлвуйчфкчкддекаэтйгвдфпч
фвешыэшочршплюэцэшпаэтф
кщнрдучфяэхрпльчршлнцдрэйэаэечаэрэдбйштбхжирдэфэпэвчечкчвдйсюдйшщпхчшстуйсяйл
гаэлвэшхаззыэээзшплиэшо
цгвчячвдьбфэцрщпдуюмлзтопмаиэчячняймьэээиэындацгудпцээавтйьоьйрщэьечомяылтцвирп
люмдройазоэедкчедийал
эшртншгйэчячдуйшяуйшгнэчюшоизгпбмйаззйцчедэчвдыэяэщшшызйалкуйсбдкрвууицльчцул
зодэйслцнкгыйуиагошшайм

цдудуогнишржхайгьоцгрэдэчоыэшскгыэяуирцнйфюбщпаэядалдуиэспиээчжозэшшлвшуплзки
эиряуэшвкйчспиээчжойдьй
юмвшучиэькяакунряэгэггшйэчлгюггэнпдуцнщпгмймрэвдпччйюдэшсвэсибфэосштйгьоылодж
деэцгцдкгждячщшюьгггнцч
ьэнчюшюьтечбйшрсйшишуиюгксюжюнычшчжорэшшщпюффрвууиыээээтклдфшнэшхдюдэсэ
йдшюбчфакадсгнчзйвдвшуйуиаггн
нрфмплчяядгныщдгнгйэзназэгныцгэчкшцнймвшодзйьоячщшоижемзшидэнчфаыщвчгнэсьоюг
теуйюмцшлтуэтшшнтсячюяьй
сньэлузйшнярснаылажорнмэедиэучгньэршяаюбиэзэумэтядзэмекжфрмйушэнчфймймшэсекж
юнирушоишуиеуэаакуфэщглф
юфэншызэедиэкгнцссждэсссуикчучяэцгечшнюйдшйштйвяээгнцзггкгкдцгюгыдссэьюяыччйтф
адкдцгыэийядсспдкйочед
кчюшлщанэнплкдцгрэвдпдмчншюмыэшсезггядьоаясечфзйезгнэчюшщпмйэецюбгьйэецюзйьэ
тфвшишяиечюрэжушзэгэвддэ
зэалггычкдйдгнггмлрнмфйшлнмбэеяукггунфгнодэйьэшннрфммйьэжакусвфдкггуоигэмыэшзг
жчэержюninвйпльчдэедуб
шиждрнвекайшхльчцуэнчфжещпаэядцмчфгмюггныяджаиипвевчябцдщгайемтгячцдяэдбдуйш
яуяиуимфэеснйфнрфрвшкчеч
огншюфкдучяэсрхщщпчбюбюбцдечэйшэмеишьяучцчовтйхчщрлучфишкмщпвшазшуснтгьож
лйшвртййбцнфэтдямкледрсйвжк
мфюфетюгчснгкчцэчйжуфэщгыдспнрмйчфпмкаурээдйкдщштвфпвшзйфсудаэцоетюгкчяэкчцэ
чйойкдщштвфпвшзйфсудаэцо
вшьйфпсгьэтлггигснаярняфесячспнрмйтгячцдтлэширцнцгжеьыэшьяойээггэпплвефрфчшсйэе
дшеопшигэфэяэншяцядже
гмзяеттфурэвэжюдьйэехлиэвчдстшюбфэаэьмщпсгкдлсбовшрэпуснсссгмзнрзжэшклэекчэйззн
рзжэшклэекчэйбцээдэнч
ээешсвэнэвээопдуиэмедуыпябцчгнмбкдюдьотгкччвтйтшоищравяиапогршочдфэеьодуйшьэьйу
иьйирэшиэнштйэчячждбр
уэтнймэщяэфэедччюдсмяыгэоним нчячщшцнймнчдуйшгмгмяылтвнймнчцньйфпмэтержэшсмя
ыгэдйьэисщгбтуйьэюняиртже
вшсдячюортяазсртршдчтлчмуйсеябюдьэифшашмецядцпведуэжюмшчпйэчлгиэшэщшшызйалч
фячкчжгкгыээшзэюятшочкчрэ
жчкшочдуйшлвзйальгкчэчгэмтзэреаптвээюгзгбтйгфнкгжныяьдцгндешблрнэщяэфэедммыщрэ
иэагдэцэггудйгснаявчеч
пяыдшсщгшэщекамфбйтфачечдядйаггньышэьйрщгнвевшфедаюнжседычяфемцнвечфбйжчянй
фэнюйиэйгфечфыэрэтлурхляч
щшцншуопогруопцлшеопезюблвдлгньэйгвдынцнмйфсудаэцоылэеимисдэцмвдгнурмйпльчонэ
щмэкдкчешурынезелфчзнйм
щяядчдцгшчдбцчечюоцгззяалтчгюшщяядчдцгцнучяэюгдэявуруйэчувюдцнучяэкгкгбцээшсже
твйшюбцчгузэкдкдыэцуиш
ысдэцмурйшкмщпсгешсвюнешсвюньчцвтйынцнмйфсудэйемкаурмйюэреапцгжеыпфчэйьэтвэ
ерттфлжхтузйефчальчюяьйзй
фрвйчяыдцпведуыээдзчафцгщшщпхчждвдьэсеопэчвдкгшнэжйшюбфэтдлгюшлщфэшэшрзйпл
лунрйшйшймэнелпыыдййемймже
мзшийэлфплцузйезймлакуггжфвелтьэфнцгфсэсьйойезйеуртйюйячкгогцогныпцлуртйблдуэсээ
имгдьйюфчфьчмупчядчд
ртятвдвшяфюффдээзлцньчцвтйьдхфйшлнавээээщравюнаяынцнмйфсудэйойэчувюдьйтфнрагф
аэчзувэесгнфруйиняймкджм
лвээкгнчэйщбфэдякдйсрсйшюбурсюыщмйлгкчэйщбданрцнфдяшзйучгнхаэчзувшаыиеюдюмн

рйвхчьйэетйячтекалсчгсняд
чдцгьйзэгнцчншюбыянчюшуишылуишхчхщкгжнтфиэесгнчшиэкгфззйжерьтшодтуйсцуурюмд
уурюмдатэреапчфяэаэаязузй
йфюфлумфюффдошплюфюфюфюфлукжвчщжвчщжвчыфагэйдшщпцлячюшуйртунахзяфбдуэ
сплггнгвщхщцнчфкчнсэйшнфэтфурэв
эжюммеэнчсартйагхрцлшужчкдпывшчгюзфплнйэйэжсфаэчзуелтлфруйблэчющээзшдузйшнй
ффрвдвшплныурэшртюсвдээял
дяэсвдылодфэвмуйэчувюдюггнцчыэлгвдячщшцнтээйссягогуйеснгюшщяхжиеыжэшцгжааэмш
щяцнгнмбфрюбцнэеслюбтчяд
аляуюэцгшэьйтфнызйезггогцорэндэдьоаяцлшеопуилгйпйсцэрэжчдгвдкмщпсгячщшцнтэжщит
эсогээзшплнрцгьэретфоэ
юрцлфдешйчьэешкмвддфояцотеочтгюоудччзфюфээпбцдэчядоекадлгмйсцаюбыщаэчсартйчфэ
чбоцнкчяэьйфпсгягяшснрэ
ээонггьэпуэеклеяждэчалщфхдйспотфйгпбцчгйээюнрэлмюфнрдушиучаээчыэюяэдогтгтгцнйчг
нггйээдщряуишзэгнурмй
инчфешурвшишкмщпсгзылакдкдыэшсжеяцээкчггшйкгнчтшкмщпсгиэгнггыцээтшхльчцутэгн
ишснаяцшйчтукжйдтукжснчф
эншыснтфиэшрснкчншлвььвшэжвдгэдэчйягьокгещвехжлвээчсартйндьэомймйэфэхэиштэшшб
йюмцшчслгщшймггкэреапфч
шсрэчстгаэцоцусндуурюмчбмйшстшчфбэюгцчюшчфврцшшивчнсцгжлвгчсыэпбцнчфршламб
дунрйштбфэфехщцнуррэяагэиэ
ывщяюшмйэдгнирээзшезяанфэшртдыиряартпаэчтоюгчршуфраяршлвюнчфврфпаяжбмйячюо
ыягэдймеэнчфэчцошешытэубцд
щркжцлураяоцээшсылуйсслумфурсгвчыэсгвчыэлгспечьчцвтйгвюнаярэяапыфрэщжлйьфэшшо
имеэнисжчфэалмйягвчкдпр
фпюдффиэяэвчтшкакуьэаллгрсцыэшлвхуопогщруыурыягэдэтшфпчбыщаэрэээждрнезгргмймь
эйжазгньэээпбэезйлгчуфэ
щгьоээюоыэжлклькьяешпьцгэчкшемкуопжехжтблгаэямймхчдуцгынвшлвььнытйиэячщшьгше
опщязйвджднэезсрфишыэцу
ишмзшублзгдэыуиртбмйтеодифыжйшбйаггнеяшэреапчфуиьйэехлиэкчшэыркуэнхуопогоштф
иэяэрэчстглбплээцдынцнвй
кгюгаэкдмфнрэрйшзсвдпчршяаюбиэггзууруйзжапмзвднччраыклцнвшиснчрэьуэеклеяждьэрря
учфишэнфэссиетфюфтймй
ьэуисеплэнйшфпфэьммйкгюгогягяглуснйшзэчдчртймг

Розшифрований текст

мамапошламытьпосудуитомотправилсязанейкаждыйзвукзвонложкиилитарелкигулкораздавал
сявзнойномвечернемвоздухепотомонимолчапошливбольшуюкомнатуснялисдиванаподушкив
двоемраскрылиегоиразложиливедьнасамомделеэтобылвовсенедиванашироченнаякроватьмам
апостелилаимсдугласомпостельловковзбилаподушкитомначалбылорасстегиватьрубашкуноон
асказалапогодиминуткутомпочемунадотыкакаяточуднаямамонаопустиласьнастулносразужев
сталаподошлакдвериипозвалаоназваласновоисновадугласдугдуугееголосуплывалвдушнують
муитонулвнейбезвсякогоотклика дажеэхонеотвечалодугласдугласдугласдуууглаастомсиделн
аполуиегопронизывалхолодновинойтомубылонемороженоеинезимаинелетнийзнойонвиделма
маторастерянноозираетсятозакрываетглазастоитинезнаетчтоделатьиоченьволнуетсядасразуви
днорастерянаиволнуетсяонаоткрыладверьверандышагнулавтемнотуспустиласьпоступенькамп
рошлаподорожкеподкустысиренитомприслушивалсякеешагамонаопятьпозваламолчаниеонап
озвалаещедваразатомвсесиделвкомнатевотсейчассдлиннойдлиннойузкойулицыдонесетсяголо

сдугласаидумамнебеспокойсяяидунодугласнеотвечалтомдолгиедвеминутысиделглядянараскр
ытуюпостельнамолчащеерадиоимолчащийпатефонналюстругдекакнивчемнебывалопоблески
валистеклянныевисюлькинаковерраспсанныйпунцовымиифиолетовымизавитушкамипотомн
арочностукнулногойокроватьчтобыпоглядетьбудетлибольнооказалосьбольнодверьверандысо
скрипомотвориласьимамасказалапойдемтомпройдемсякудапростопоулицеидемонвзялеезарук
уонипошлипосентджеймсстритасфальтподногамибылвсеещетеплыйсверчкистрекоталигромче
прежнеговсгущавшейсятьмеонидошлидоугласвернулиидвинулисьпонаправлениюкзападному
оврагугдетопроплылавтомобильсверкнулвдалифараминаулицахникакихпризнаковжизнинисв
етанидвиженияюегдепозадимерцалислабоосвещенныеквадратыоконвтойсторонеоткудаониш
линевсеещелеглиспатьнооченьоченьмногиедомаужестоялибезогнейиспалиапереднекоторыми
тожетемныминакрылечкахсиделиихобитателиивполголосавеливечернююбеседукоегденавера
ндахпоскрипываликачелихотьбыотецбылдомасказаламамаонасжималавсвоейбольшойрукерук
утоманупостойдаймнетолькодобратьсядоэтогомальчишкидушегубопятьвышелнаохотуонубив
аетлюдейвсемгрозитопасностьниктонезнаетгдеикогдаонвдругпоявитсявотклянусьпустьтольк
одугпридетдомойяеготакотколочувекбудетпомнитьонипрошлиещеквартелитеперьстоялипере
дчернымсилуэтомнемецкойбаптистскойцерквинауглучепелстритигленроквсотнешаговзацерк
овьюначиналсяоврагтомужечуялегооттудатянулоканализационнойтрубойсгнившимилистьям
идушнымивлажнымзапахомсплошныхзеленыхзарослейоврагбылширокийизвилистыйонперер
езалгородимамавсегдаговорилачтоэтоиднемтонепроходимыедебриаужночьюкнемулучшеибл
изконеподходитьоттогочторядомцерковьстрахидолжныбырассеятьсянотомувсеравнобыложут
ковэтотчастемнаябезединогоогонькаонаказаласьхолоднойибесполезнойразвалинойнакраюовр
агатомубыловсегодесятьлетонничеготолкомнезналосмертистрахеужасесмертьэтовосковаякук
лавящикеонвиделеевшестьлеттогдаумерегопрадедушкаилежалвгробуточноогромныйупавший
ястреббезмолвныйидалекийникогдабольшеоннескажетчтонадобытьхорошиммальчикомниког
дабольшенебудетспоритьополитикесмертьэтоегомаленькаясестренкаоднаждыутромемубылов
товремясемьлетонпроснулсязаглянулвееколыбелькуаонасмотритпрямонанегозастывшимисле
пымисинимиглазамиапотомпришлилюдииунеслиеевмаленькойплетенойкорзинкесмертьэтоко
гдаонмесяцспустястоялвозлееевысокогостульчикаивдругпонялчтоонаникогдабольшенебудетт
утсидетьнебудетсмеятьсяилиплакатьиемууженебудетдосадночтоонародиласьнасветэтоибыла
смертьиещесмертьэтодушегубкоторыйподкрадываетсяневидимкойипрячетсязадеревьямиибро
дитпоокругеивыжидаетиразилидвавгодприходитсюдавэтотгороднаэтиулицыгдевечерамивсег
датемночтобыубитьженщинузапоследниетригодаонубилтрехэтосмертьносейчастутнепростос
мертьвэтойлетнейночиподдалекимизвездаминанегоразомнахлынуловсечтоониспыталвиделис
лышалзавсюсвоюжизньионзахлебывалсяитонулонисошлистротуараизашагалипопротоптанно
йусыпаннойщебнемтропинкепообестороныгусторосласорнаятраваивнейгромконеумолчнотре
щалисверчкитомпослушношелзаматерьюбольшойхрабройпрекраснойегозащитницейотвсегос
ветатаквдвоемонишлиишлиивотостановилисьнасамомкраюцивилизацииоврагздесьвэтойпроп
астипосредичернойчащобывдругсосредоточилосьвсечегоонникогданеузнаетинепойметвсечто
живетбезыменноевнепрогляднойтенидеревьеввудушливомзапахегниенияяведьонисматерьюзд
есьсовсемодниииерукадрожитдадрожитемунепочудилосьноотчегомамаведьбольшесильнееум
нееегонеужелиионатожечувствуетэтунеуловимуюугрозутозловещеечтозатаилосьтамвнизуисе
йчасвыползетизтемнотызначитможновырастиивсеравнонестатьсильнымзначитстатьвзрослым
вовсенеутешениезначитвжизнинетприбежищанеттакойнадежнойцитаделичтоустоялабыпроти
внадвигающихсяужасовночисомненияразрывалиегомороженоевновьобожглоемухолодомгорл
овсевнутрипохолоделопоспинепошелморозоледенелирукииногиемувдругсталоченьзябкоточ
новновьналетелизпрошлогодекабрьскийветертаквотоночтозначитэтоучастьвсехлюдейкаждый
человекдлясебяодинединственныйнасветеодинединственныйсампосебесредивеликогомножес
твадругихлюдейивсегдабоитсяваткаксейчаснузакричишьстанешьзватьнапомощькомукакоеде
лотьмапоглотитводномгновеньеодночудовищноеледенящеемгновеньеивсеконченоещезадолго

дорассветазадолгодотогокакполицейскиеначнутпрощупыватьсвоимифонарикамитемнуюраст
ревоженнуютропинкуинанейзашуршитщебеньподногамилюдейкоторыевсмятениикинутсянап
омощьидажееслионисейчастольковпятистахшагахоттебяаужнавернотаконоиестьтемныйприб
ойможетзахлестнутьзатрисекундыиотнятьутебявсетвоидесятьлетижизньэтоодиночествовнеза
пноеоткрытиеобрушилосьнатомакаксокрушительныйударионзадрожалмаматожеодинокавэту
минутуейнечегонадеятьсянинасвятостьбраканиназащитулюбящейсемьининаконституциюсое
диненныхштатовнинаполициюейнеккомуобратитьсякромесобственногосердцаавсердцесвоем
онанайдетлишьнеодолимоеотвращениеистрахвэтуминутупередкаждымстоитсвоятолькосвояза
дачаикаждыйдолженсамеерешитьтысовсемодинпоймиэторазинавсегдатомпроглотилкомокзас
трявшийвгорлеиприжалсякматеригосподинедайейумеретьмолилоннеделайнамничегоплохого
папапридетссобраниячерезчасиеслидоманикогонебудетматьдвинуласьпотропинкевдикуючащ
умамтызадуганебойсядрожащимголосомсказалтомснимничегонеслучилосьтызанегонебойсяс
нимничегонеслучилосьонвсегдавозвращаетсяэтимпутемголосматеризвенелотнапряженияясто
разговорилаемуходидругойдорогойноэтипроклятыемальчишкивсеравнолезутнапроломкогдан
ибудьонпойдеттудаибольшеневернетсябольшеневернетсяэтоможетозначатьчтоугоднобродяги
преступникитьманесчастныйслучайаглавноесмертьодинвовсейвселеннойнасветемиллионтаки
хгородишекивкаждомтакжетемнотакжеодинококаждыйтакжеотвсегоотрешенвкаждомсвоиуж
асыисвоитайныпронзительныезаунывныезвукискрипкивотмузыкаэтихгородишекбезсветанос
омножествомтенейакакоенеобятноенепомерноеодиночествоаневедомыеоврагичтозасасывают
кактрясинажизньвэтихгородишкахпоночамоборачиваетсяледенящимужасомразумусемьедетя
мсчастьюсовсехсторонгрозитчудищеимякоторомусмертьматьсновагромкопозвалавтемнотуду
гласдугивдругобапочувствоваличтотослучилосьсверчкиумолклисталосовсемтихоонинезналчт
обываеттакаятишинабеспредельнаябездыханнаятишинаотчегозамолчалисверчкиотчегокакаяэ
томупричинапреждеонининикогданеумолкалиникогдазначитзначитсейчасчтотослучитсяказалос
ьоврагнапрягаетсвоичерныемышцывбираетвсебявсесилыспящихгородковифермнамногиемил
ивокругвеликаятишинапропитанныхросойлесовидолининакатывающихсякакприбойхолмовгд
есобакизадравмордывоютналунувсясобираласьстекаласьстягиваласьводнуточкуивсамомсерд
цетишиныбылионимамаитомвотсейчассиюминутучтотослучитсячтотослучитсясверчкивсемол
чатзвездыопустилисьтакнизкочтокажетсяпротянирукуинапальцахостанетсяпозолотаихнесчес
тьзвездонижаркиеколючиевсерастетразбухаеттишинавсеострейнапряженнейожиданиеохкакте
мнопустыннокакбесприютноивдругдалекодалекозаоврагомголосяздесьмамидумамаисновама
мамамидушлепшлепшлепмчатсяногивтеннисныхтуфляхподнуоврагасхохотомнесутсятроемал
ьчишекбратдугласчарливудмениджонхафбегутхохочутзвездывзвилисьвверхточнодесятьмилл
ионовужаленныхулитоквтянулисвоирожкисверчкизастрекоталитемнотаотступалаиспуганная
ошарашеннаязлобнаяотступилапотеряваппетитведьонасовсемужесобраласьпоживитьсяивдру
гейтакгрубопомешалиикогдатемнотаотхлынулаточноволнавовремяотливаизнеевозниклисмея
сьтроемальчишекмамтомприветисразувокругзапахлодугласомведьотнеговсегдапахнетпотомт
равойдеревьямиветвямииручьемвампредстоитпоркамолодойчеловекобявиламамаотеестрахов
иследанеосталосьтомзналонаникогдавжизниникомупроэтонерасскажетникогданострахэтотна
всегдаостанетсяунеевдушеивдушетоматожетемнойлетнейночьюонишлидомойспатькакхорош
очтодугласживойкакхорошоанаоднусекундутамнакраюоврагаемуподумалосьгдетодалекопос
мутномуозаренномулунойлесунадвиадукомпотомвнизуподолинепрогрохоталпоездонотчаянн
освистелточнобезыменныйжелезныйзверьзаблудилсявночитомулегсявпостельрядомсбратомв
есьдрожаонприслушивалсякэтомусвистуидумалдалекодалекотамгдесейчасмчитсяпоезджилих
двоюродныйбратиумеротвоспаленияслегкихмноголетназадвотвтакуюженочьдугласлежалрядо
мотнегопахлопотомиэтобылокакволшебствотомпересталдрожатьтолькодвевещиязнаюнаверн
якадугпрошепталонкакиеодначтоночьюужаснотемноадругаяеслимистерауфманкогданибудьв
самомделепостроитмашинусчастьясоврагомейвсеравнонесовладатьдугласнемногоподумалпо
вторичтотысказалониумолклинаулицевнезапнораздалисьшагиближеближевотониужеподдере

вьямивозледоманатротуаремамасосвоейкроватинегромкосказалапапаидетинеошиблась

Висновки

Після виконання комп’ютерного практикуму ми навчилися працювати з частотним аналізом афінного шифру і реалізували допоміжні функції модулярної арифметики, і змогли розшифрувати даний шифртекст за допомогою частотного аналізу.

Також було побудовано примітивний розпізнавач мови за допомогою ентропії, який дозволив автоматично відібрати ключ для розшифрування тексту.