



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

Криптографія

Комп'ютерний практикум №3

“ Криптоаналіз афінної біграмної підстановки ”

Перевірив:

Чорний О.М.

Завадська Л.О.

Савчук М.М.

Виконали:

Студенти групи ФБ-
71 Новик Л.А. Равкін
Д.Б.

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. Самостійно підібрати текст для шифрування (2-3 кб) та ключі довжини $r = 2, 3, 4, 5$, а також довжини 10-20 знаків. Зашифрувати обраний відкритий текст шифром Віженера з цими ключами.
2. Підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення.
3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта).

ТОП-5 біграм зашифрованого тексту:

- 1- хк
- 2- ек
- 3- пн
- 4- вю5- вх

Розпізнавач російської мови:

В якості розпізнавача російської мови використовувався метод заборонених біграм. Як такі було обрано наступні: "аы", "оы", "еы", "уы", "оь", "аь", "оь", "еь", "иь", "уь". В ході розшифрування, якщо зустрічалась одна з «заборонених» біграм, цикл припинявся, програма починала розшифровку тексту з наступною парою ключів. Під час роботи розпізнавач жодного разу не спацював хибно і коректно обробив всі варіанти, залишивши один єдино вірний.

ЗАШИФРОВАННИЙ ТЕКСТ

оклйазогтдхвоэштжсэллыэежяхбчехеквюхуашайейллокийбяктивндкпйзмйхшкшэхкиккптжпнуафйнрцэз
к
урлюхжыэвхбкдкшхяиожщбтхлцймтдщгхуюклцбьшнцмещврчччътакугэвжйулнекчвоцмахухкпюукгху
п
нфйллрзгдзкдохксавхцляплэенцяхкпюлюбйчдгцякбуейяждохксавхцляяхкпюлюбйтжхквгейчдгцхнцмы
ж
шжхжэьехтшфхййвнхкйеокгхйэоцмахутжджюхбжяежвбурзещежяхбчехжфлююющччэюхуевхвюйшыьо
р
жлвнкбгхвюдшчжуастхжыэжващцэежяюэранмафйфквхябчжщжшхкктхзюяжябтмюхййвнгцдпгфздьлпнз
юекябзюгцщдэтглюзжжэппптжмдшрпаьжцеазогтдвхгхьтвуййзмйхайгцпндоекякчхрмтдщгекыэвхддппф
йкудкшхйяйнырпцюкнфйаюпржфхажсююхкнмзджудпбхшхфжяжпрчжгнкцгцмвкгнъллыншжбгхвюсы
п
няконшуашяквюезлнлрудвурсюэякеххэыэлаебстещзколрзбьюуюкйькрьнякурлюмэпжзкынлюнлхббщгхь
п
ыптжфпыйююейейлллхлзкусэщмэьмуебююэряжхжуэпжйеекфхмуоньуцпккйегкюкындпфййцпэжлнйь
ыэьююиррюрзлкаббжпжихьщцкхэфпыйжуюююохкмкпжыэьзчмацоеуюкйькрьнябхклзкраирхулнтцп
р
вюкукцэрххьупртдахууймшхыэалофехжвхжддцънгцмвдхихвюкукьлэбьексрцпдэахуюэзтнрвмззихуеч
йтшьптэвцицкучььдмбдпхукхрптджусынгамчьюоцхуакхжйеххзаппийекдзтддпбагпгдяпкыщнгтвунклцм
в
тхтхкпстихихыхшхыэвхйькрьнчвхэхихуаэьмкэцийфрыизыашлхвюрыаыегтдэакптжчьяэябжуисщгэуеэ
г
пймхумбнэцаебпжоксоьюфбыврнийппнщбэумбсмкущбгцххккщппнокшхлзапхушжжнжзофлкьпкгпрфун
т
эрышжнствуюохкающбирэщвхвюйшрэтфежацлюздэштжчоебвхехцгнебхкыипрехбуэрсьетвудптжпюпн
ф
йтэябаяхклэзклнрзийьжйеекейейлллхэьмуебююэрстгдбьыэцеззцмтшьжыэвхежяхбчехвхцюлюяжлюмвф
н
щбикьджузкынтэыкчкчвскнббжюуирпвежчхшнзждкыэгжбьокяжунстздиктхлкзяхкпнцбирижожвюфбш
жюпобжэмкмчвьюсыакхкаблэчвдьбкзкйевючэшрвнгцпнсшклзчцецхвикбкпдлножикэбежсэбгцгпбг

ы
юашгжзуеынбчйчьгафйчьбхщбтхвхпуцпвынббэфндпшьбжхжтнтэыкфндпгдэшнбтптжчэоюкцеэокежйэя
э
тмййэржляждкиовмиржлвнебгхвюдшоцмахупнехуэвхяоебуецогдэшэбсьтмюьфжяжвлякябкынэрьжэь
щцфйзмийхэхккпыйжукцгцпнфхфуфзлюхуойэрзюфзфзшхчэыохкхэжъяехкшжхжгпвнзюхкоцихццдмам
у
фйююхкпвыэьцкбэьзютхокюгейжудпююэщчэоюкцккйегкньсэчэпжйеекбтхбокяжунлюпнокупдоектхвнв
юбжтнещбжунййчэьщжйблржлвнцхякхкхнрзгдхбтхдхмьывзхуеашпнмбьвюэумбфбудвурспддгфихо
н
зыежгниыекдегптдмапдкгпийзкюпзнщбэудткухложфуфзвырэуцдпмвщдебвюэухуэщнхуягрщижлийюк
х
эьвыэшкябшряжйрхбськцмахумбтцгцпрююпнюкьэтхшрфрззлюэруабкехчвмксэьэехедтэтллхмдицофп
нвнхбыэлхютщйхклзвняэудебцпфзузюльнфудхбжупющбхкцщцзтдижезппэуэвхнммащддпнекупийе
щлхвйэрфпчыгыэтхокюгэагбуэыкоkdзежпжекупгдиыщещцптжэьмуебхкчтэтллххддэтэтллхприребтхе
к
чэыэцеэцчькынфйпвийехвшэсаздирмбтхыкохцрлнеэхкунщбккмэшжбжяешэбкикчвлацюшрякенгцезшхз
х
жыщожгпнквхшэснзюэуззййогвжкмвтыптжябяэсвдхыэгжпвзмэхэхыэцеджкзгдейтляэйклкжэуеокмды
плюпжджзкизмэдкдхмэдхихддэтэтллххджьонтлкрхугокцвнкгхубщпжцпэжяншохкжвтхоктмдпзднлшь
о
кмэенлнекфхвжгхихбщзхжыщпптжурешыэцезкудзмжэьждхихпвийевхатчдбэуряфшжхжмксэнплхэжйечэ
сдкцздпэмбьдгэшжоцмакулюмбжвяфлкэещючьккунцмлюэтгцпщцпцхумбяпзкяйуфююхжшжтхыэякрт
ш
хйвдхшружяблндпфрезекчвшэщйтдирфквюьнппыэдхибгохкьвшжхжбкщныючрхугокцпыйжумбежсвып
тэытжлехокчэзхюргцдпжаыкбуьфжвашвышхчкиздоцюппуэхбюнийчкшхвцдпшхзквюиохвцдмбанчцхкмб
а
жфхфюфзйшпушуашфндпяпвжвюхбвжйнфрддтыждьюхыкнохкэрыпхутмстгдтмплюсьяюзкмрягддкуэ
у
окйждтэтллххщйтдэуазчцдпчьмаьжцежвддкуэубвжтхбьззшхзхжыщцппйтэуээнцдпшхцмыкхнэшвюкуэ
з
вумбикьдююзюыюбжцезкубчвхкиюьнофхжсштххжсштхпплюажйнэуазшхзхжыщцвмзьяквюрвьжмшажй
нэухуэудпужпяхкстпцекбжтнужйэхяфлкэзщбикьдююуцгцзыбыкыкрцезыкхкиюхуцяхкуаддхфогбщэцуф
щ
ыгфягаюзжюхпнфйщгжуяпдпбжьжгнппийфзещюхдхьюуцаздпгдяжвждкждзмпрккокехикфжизыквюбааз
г
дзюяптжгпгдеэхэокдяжщзкблхуеэуззкбуешхуьдхэюашйиапддхфогбщфуфзфуфзвхокяжяцдпмвхщццл
ь
нзнппгдаплххюэршхмтшсвдхзюсаздээьдюьхнужшжюуеэшжхжзюзонсбжжвлхяэзюбавмфйиохвмчймчд
ядмазксваувжыиожащыэхэююэржвпющбхкнляйтцпрщфхмшгндптжтхяэчэьжуеябжцожбжрэдкзкмэяюэ
рэмубеякбкэдююжукнщбикьдюювхяждкпюлююирфпыйжуюхбжцедкыкйуьбщбкехзжэвхкйэрфуфзв
х
ахьюисофлкыхзкоюиогдекюкмдвмфуфззколокихфуфзпплюаюуощйвхпагцздщолхжвэьфлкбплюддэтэтл
л
лхзхжышцирирофлкцбокйеокфжежизыкежчхзэьвхьяхклдпгджшгнфйжхуеисжуьфжшгнфйжхуеежизпнш
р
ынофзхуыйцгапыйхвлюшжгхлцдтжлехокдхщньухкабэулнжвккфюцюпзтдлнфблхфхихддэтэтллхсьчпы
й
екабдохкбушоэушцбшьвхьпбквжфхжшгнфйжхуеешцфлкфцпндоекаюдптжддълклнйшикаьдтщйюичжфп
ыйцюяплотжчоебфххрчдлбщхякхкндшхкзцмтшщьвхаюшдмазксвмбшхуьфпбгзмьжшвфхрюшхжыьжйфй
йююнэджбхуеэьмуебшжхжвюхушхтрофцпцюяпитцпхуокохпюыжщжжвтхкпыйнлсмйхфнфрстшхчкхню
ю
яэябтхчэихддэтэтллхсьяюкутцтэщбтхихцеййвхщбекдхюдмафпыйеклхидклцхуцпгдекфхбхбкунщблх
ф
хфюэрйясвьюздпнанююяэцпсьхкфжтптжчэцьяжеюшдцмцюужйдцлхэяэдхэмкыкахгзцмийюэзугффшдд
ц

мьюэаддмаоньохвюкджсвсжруюньохврзщцкэбдхинфрчэбксюпцхучвьэдхбцещхкзконлюдпждзмышжвж
ю
чцдпшхюхякчпыждьчвмксэыохкчйгдцьсьлцгцещхкыхэбфкэблхфхихзхжьщппашудебвхбэфхпвйхалфш
а
шсьчптжчэонгфлюнэяжиолндшжнийзмжввхсниймкудпанэтчцуащгдьщейвнмумахкйеокяжшкябшрокаж
у
нпниосычэонкушоэжоклийгцдпгдэцэрвхпжэуирыхдкмэжэзкстщжхклийцюлндтыпвынбиружшхенужудцпу
жкцщбужьпзюывоэпжхнуцпыйеклхынююяэшхзтгмвынбтпдптжвюздпнмзниеэзжбезкубякмуфйнлщхп
н
лхзлкышлхокдкхэжьяещпгдбэыхщнзюлхбзкбжвмшддппюхддппюхчхыкдзофяжжэшжоцэрвхбжйнлюгц
ы
хщнзюлхвжтнэщйдстлийжукгююодьшэибикьдцпыйнлтцшхжныжжшгндяхкдкмэрржлвнебгхвюдшддщбхк
и
жыоезоцгццмлющбьнгпьеоблхфхихехехяжрржлвнебгхвюдшзкэдмаэуэьмуебождьвюхуцмчвьюекпютэсь
х
квхдкмэхкоюгцвхьжшуашвхежяхбчехвхягантмлюдптжякшйзюлхынфйвкзптжлаебтхчэсьывзхуеашкцщг
с
вцдмаоклиймашртшякбжйнфпуэцелюшкшнжхвхудлнююашфогдхвчтэаонирябжулнекрмхулнтццщфэыко
ц
фзокхкмвйбийюющйзмйхххлийзюдпбьдмбтхяжиздпздуоцпцютцшкшненьцплоежяхбчехлоххкхтхьзыклу
г
зэуфквюхуебжюкутццшолхчкывюхшжзуюфлкафлкжйзмйхрбйэлкньюхмэнпйтцпхуокйбикьдююаплюсж
е
жхвуяежчюмэажоцщппхкикьэйецайрмбзчгдармбюдстгдтхоцмахухкчтеэотеафлкбптжшхрбвжшумбщх
з
кязокэувнеэлэенызмппнцптжгъауофбунлокгрекдяэбуьфатлкяэшкежхвюкаьпсмзгдейжнэрокхкмвтмьж
ф
худьохуэьмуебябехьдцпфшцегьчксцдпшхзкчятхажхжмийаюуогдэагпкхаюуогдэаьдьозюядоэжшуетежц
ф
лксзыкзклкунфшчвьэдхбцмажлззжуцуюиоектрешпплюаюьппныщбтхйебъагагеоцмахухкикбьюхмэюзч
ц
дпчвьюгцещйэлкчохкябгзвупзщюююсбцовюкузючщюпньуебнэкзлюгштжтнещлцьнвнирсндплнцжфхв
ждуппзкяйуфоэяклхэьмуебвюйшкацгдгышцембтхшхгбсфлюгохкхэжьяешхмтшьжуещзгдрзежтхяхфа
ш
хээшээшжвюмвсдмазкюхвцдпшхихчэвхтдпшэбокдзвудтэащпшоектчьюэихцевхяждквнппуцззцмхжтузж
дквхмуаоффптжсдийхвдбтхшхлрмбйэитлнюуеэххехяжикмуэтсблхфхуелхюптжаюпнуохуцбэквхгхвюд
пыйжуфйзюбщтгцхубщекщуппижхкунэрьляэуфкджхеюняэвжйелхыэпнмбхжсэокгхекэцазкбжвмбошч
к
ютьнъндпфквхьуйтхуебнэшэпнрьывзхыэцезкчпзюшэрбмбджоюыэчэьжихлхокхэджбхэюиэикдзщбяжаь
щ
бтхпучшвхяжабежсвлхрпсвйхэющблнхэшйфрвхьуисофгццмюхлпзюыноатлкхэвюгшээдхэюлзежжктугцф
йллмбжвфурзхблцдпекпнънкццмюххфяжккшубдйэранчжзкпдмаикзкьззчйижлхвйфшвжлкдевхьпыжз
мэчвунэрвжвюрзкуыптжлийуомбхкчввжпжхвддпуаышгцкьшхгнбавмлюдпежвхщзыхзлтшмнужжыххэцц
п
люыныюыпякээжыцсхыикцкцэрийпплзхукнейдпгдиьвхьэжвябжцещябцовнешщюпнгцфзэуебыафйкуфэ
т
мийфрмбйэитлнюудтвуцглнрэвхджхжгуцпфшанчжсдьнэумбфбтхмвнтэузюгюьхьдхукнужддцмшхгрщк
п
дыпяэудягапахкчкцбгжуэакбкыкинужшжхжххбкунужьежжвбудпэрябрзмэвжжвмбчэьжпжйевюдхчжб
ка
мешцлэенрьвжмшкыгхзубебжэекгмдпздэунквхзклцтдсадяхкьвлкфнссыскцапъжошуешкохлбгнфйжххкгряз
хклийэтвуьлхбуеьжашжэнгпньвежщлэдхзкэйцъаранаючщгзюашьжошуешкэйдхфсцюгозюбжеюэшцки
й
ькоюкутциохкнргдпжшщцефхыхдбуфцмщблнюэзухбрпийзнаэрвнхуожьдхлпфздьлствуцщбыхуевхьпкг
ш

ртжяжщзкбхкабтдзжякфхсэййвнчщещйжцрыпвюздпнюколнрхвуйздцмякшблнсывютдвнекупзюгшекмрж
укниспцмвйежцлюздещжэмкякоцмэпвдхыэвххмкудпешбудпеклюяоююыпфшддкзуювырэтмйивукгцюм
т
щкжшуелхчюлююхяббниокнеблндпхурзмэбуллцпфшщезлздгфсабжщеокачэвхтжокшввцэжежвюьумбуеа
п
чюпнгхклпржухбыврнфрекунфрщпицирякйекбжажыкпйнрхупншрвтгючрогзюякбутлцюашахфэпнддзз
й
йхэвжнббэашьжолвмуацюхфбьхкэбекдхтшфжжэвюьнзюмучйзюяпчцьлоктжекдхихрьчэсэлцгцийвнфхж
д
змпрякбхжныоцмхэойэркцмчгдвжшхыйаплллхбнфшззхжудевхибчйзюююшрекдкчвхмбтхяжьдебажй
в
дхуеокфьчжьдщйекжььжьдмамучйзюкныжжужуиспназэрхэпждьэйкхкшйаплляэокхкчьукдавхбццмюххко
йхууцэрююрзгдшьфжджщпбамдцюекллейэжзыклуэрыэйкьжгышцрьвжалбщшхбкдхуеашбквйбнщьпачэ
икшйтшщмяжтньфьпзютшокажавхалбщиошрдкзкмэхкэьдхлоцхбыэпрякпжжжужеякузийккыкццэржгышц
нкхкшйзюлючцвхякхкижжшужеяктпююашвхбжэффпыпыжрахуююешзьтнфрьпзюэрокхнцюижцпхэхемку
щбкбвжеюззийхжмдхчюцпхвдбиркузюдпшхййщдвырэщннтлнфйзкейшбирцмцмздуапнтхпникоюлмжь
ь
жюукгцюяпыпыжхнфйкгекдьдждлэщжвхтжекдхежмбикьдзютцгцщйцпююжукнужяженгцэружшрсабжйг
юхфюьмкишфагцшхянтнкнбсьыхгзгдейяжинфрьпзюэрфхмэюыкиктнрзиофпвюгзюкбтхлквюхфлютп
ныекдепняжшкюцяжкмихиэяббниокнвмвтофмстщйзюймшхуеуйтлхпжзуэщфхыхдблнюэябщьчэьжтн
ы
жрьбутльнекапекунешжэуэякбуягююйуюнтмщбирфрзьялпрлюсвмкехфнуаоежвюхэщвмстщйзюогыйц
юцжщжййвхшкябшряглнапгдйшгнфшшхбквюэкеквюздогеклзкбжэнбибтжекдхихцббжщжтнэщыкчкча
б
бжхкндьяждкыюшхякшнэщбкудзжзкыьщжхэшрдджухбжэсжхнцмщбюихбчпдпыныщцпждзмфхндзювх
вжвющьчэьжйяхкехежгеокдощйфзлюэрвхцупнююашкщцбяжнбкждкчьокньяконогдшежвюхэщвпнфпый
юовюгцънщфкуййхваббжлэгркуццэряжоцкутцйштучцймчьеяхкябдохкшрыюрзгдкнягекбклхфхпжйевюз
кхкдкпювкйдэрхвмрщддкхкщзмэмшуетмтэюхуешрфпхжпшякэьехуевхгптжхнфйажикмйкуфжчзийнрцю
фбтхлхаркуццфштучццмчьахпнчвэжыэщпийтгдтммэбыбюньнтмчгццмыкхнфшзкшназмэккщюшрект
х
цятхяженгцэрфшшрнрхбгнщбуепрэуыэпнзнапейэрьффхыхмкфнхбэрьфддгфихонфрежжмшрэгрчцыкзю
жудпзюыккптжаюздмаэрвхдхыэлкцевхикоюлмнкекизгшбышнмафйлюаюешпжхнлюшаазофдпщипцдпгь
а
хелнржуцмкудпгццьлэихцещпэасвежпжыэшранппвюхжвълхокснлхвшрзююкмвшрсаофлюжуцбфбекдх
пдщбююфбтпхжкьззкбуезкшнзхбынотмдптжшхфнчщйццюшрвхемыкехюхджхжбхвхякхнэуждхкнбзь
г
хвэсждкьжнбяэфузюоклийгцезфшщепнъвгбьэнбекдкйдэрекупкуекойбирешккйегкзгцзыпноклийхудтдпыйж
упннкмуллэуждкнлчвийньюпсжежбьэюшрексьвхякшнэутдлюекегжушйчцшкежекпмшобщзкбкйбыэшцэ
рхнцмдпийцхсьетвуцбьэшцэрхнцмбашрыэцпяжфхмндплючрхбпжекхпвюппэждзгдейхэблздгфдещюлю
л
ндйдхмумаеблкфнщбирьниояпждзммююньуьньнтмщблкфнкухбмучйжувхяждквжйххэажоцщшжрбхкй
е
окддсткгцюжюгцауадыцэуеашвьуеяжынопныноыаэтшхуеаштххйхууцщбхкйеокшжхжяжвюеэоклийфжяю
ююзжбетжсщтэафзебеквюеэшкжабкмкиктутмажхэтпфййнлкгцпнссвхджхжпждзмшжхжкюстещвж
йххэажоцщшжйэммздихикоюлмппяддхгбжцмэынзюаюшбыэшцэрбунлокгрекдкйурконцмиожудпуццю
л
нчрзюбыхцябхкыкбьмумаюэяоэаыэлхжбуфещбквйпзщбмзхумбэктжтножыэвюдшикоюлмьвлксэзпежф
ь
кулняяхкьвлкежгеикоюлмниьюэуцбьдэшфхыхзрбкбьххурцльнхвйбфхыхмкюцыкчэыйьфьнышщпгдпаа
з
офлхгйирпнирийхкцхжвюдпхэлхымзьмкяниобйгдапдшвюлнешдджчхыэвхяждкмбекдхлювоезхувнмафйд
жчхыэфкнбсьыхыэрюгцетожхэйцыкчэвюшошибщйпмблхлашртшьвихкбюуьннкыхалпрэумбуелпрежюы
ювхбжйнствупрэуыэтдсвекфеикоюлмазцмчьчхыэцефнхфбудпекпншжхжмксэнпдйфйьмлчдахыьшду
ц
езофбьыимзкяйкцещююрзлкдзвусыоцкутцзмахвлаазофдпзклцгжькюбаазофйвыкдклхеюрчжуццюгцы

хцнзюоклйтдмахжфжбеккийеяйцтдхкийжыэбьджзьффукуййбьжзыкежчхалзьяббниокннклцмвххкпбаэж
 ж
 пуанекаббжпжплюфхыхязкцьубщзкфаазофтжйеьжхжшжшукгшитмпнгцуфпнекабхкежбуэтэщфхыхшгжух
 к
 жмздцэщвуаддфклцмвххкбтьниояэфхыхзрофыкчвбмзкяйкцуашктжонтмщбфйирпнчядкьвьюэучькьююшх
 ошейкбпждеждедцщббьгбкждкихбкхэлхютщйхкхжджекчюхфпнтцдпяшеждкфхчькьикоюлмяконхбыхе
 щ
 вцуисткхэыхфуэугцмэгжскеквьюндпэуашмувтчдпсвйхпаазофуашрыэьошрмувтфжпнойьфхухфпжикаш
 фхшрчжвьюндпэуашйуюонтмвкудягвырэмрщдзкябшрьпыжндмаекстшхиэрьикоюлмйьфжяжвьлkdдкгяжд
 книйоилнышьвьюлюгоюьювьлкажхназкухэуетжсшфкгнзнзюгцжьбьжчптжлйнкфтхжгбьякжвлхибпзщбуфпр
 ыэвьюдшшэойчьжпаюэрекзкгрщдлнюкьвунцмпндохкенгцэрыжтмпнцммафйжууохкхклобадхалчжашмуу
 фпрщппнэрпнякахмэрдйещрюшхбжзконкбхкыкбойчьабагжуэаекбкыкинужхжйейвхжйейвбжэьрэрзык
 делюдкыкюхоцзкхекрээухбтдчхчвгджуфбшаэтыкэжтнцмогжуэаекбкыкинцмфзылюззынопзццлюздэрмж
 д
 ьвхбкийжаэюствулюныжсэбчплнекенгцэрыжюдейвндпуахвхкррвмьохбяэьюхумбехьцлюздэщйирзпнфй
 с
 туюашшраназгдчвязздофокхкыкдкпнуругзюокжныюфбхдицешвьабчдпцояптжмдшргзийекбхшэяклхж
 ььжжэкьюогдэафхыкбукцнрьнкцьогдэаикхжфхыхмкчэниюилнчщоцзкхегкыкэээжякюухбнкмйчэьгбтп
 ш
 жхжжзыхыхшэксэпулнийьпыждыпнойчьцзиофпвюзкдхсохкчпгдбкензжгндохкаждкййвхокхэлхынхби
 к
 утбйчцмаютццмюххккюхфнччихмэрбцюогрызкмксэихайхбпзкугхххлзкбэшддййкэлчщщбхкыкинщбсь
 ыхгзыхыхихиквюыкниюифшлхчюшрекхщзююыпзжнбтптмлюжубаазкуфхзюымихфхмдлюппллофвютэ
 к
 мьеужжньфщпицдпвнцмезоцкүлющкквьютдхэяэстогфжхвудазцпещпнойчьаьчэьжнпшжхжсэцмпнэкдкг
 е
 тухббьшнебуцанэьмбажпбекдхяктпэуашпншэбхнпюхыэбудпекажьюцмихтрпнчягаиргдвхвжвюуцмахуш
 б
 фбхкююбкщныюкнпяхкнбихьвскдкяжэпнякбхжнзюекцмпнуцдкхжыэикоюлмвхгхюзййудфйыпцюфбжц
 яждьддльлкбкпдьфжшгнфйжхуешэбьизхжвйдошршроьюхлкцеякбкьюззстыэфжпнщбтхекчэгббэицмвал
 м
 быафйгдапэर्वюхумучйзюкннкдкгежэмкокежтуяичжашзуиратжуыжсхлкхбьдхнхвьзчцмахуашикоюлмфя
 х
 кхкдкгедтвкоюрзгдэкенуохуйуюнтмщбдптжхнзююохкшхгеежаюлюцмпнкньотмпнхблэбхлкэбцмхждхжр
 п
 нчяжпыйжучьяэддлююныюужиждкпжзуыюкутцздицююжубейапуэопччьщцщбьдэтвумбудгюгюшрек
 хкянфйчълхшэяжякгпбгхвжуиснклэпулнхвюкетежоцирззихвжхэпнвнэавхсохкцмпнчрогзюьвуетхяэйкмй
 щглнрзийбахждхсохкцмпнчрогзюяжхкйеоклюхэехуеекыйппцюдйщгэаазофаюцмвкснатвушкябшрждме
 щккжпхбуеоцкутцвкоюгцддщбхкшулююхдхибкнжурзещекддышгнешмхоюмаеэжкьювкнухбекрабжцео
 к
 хкыкдкьпзюоквьюшхчвеххэыэюоширьяждкьвыэпущгхвапаьвьюьфхжжнисофмумавмихццфшэжубуеэжфл
 п
 пэщикудэщцекоцфзгюйьяждкьвыэбжчпмбжвгдцмюэхбыэьвуддпцждкдкдуэубкнмашраыфхыхфустцктж
 г
 еукмйкудквюйшюзмэбуллцпфшщечюрзлкдякьдхбяэдххэйщцбьдппчцчьщцщбьдэтвуцонлвнюэжэуэвхь
 в
 ихвхыэжхфуьйбщдтвудпхжпшякйэьжуеякийгдапдшшэцтыэиэфхпдьллнекзцкуоэззцмтшьжуевхшэубщбх
 кыкхвстмшуетмдпммтшбкаблкфнэрщдбжцешкюдейлююоэуашайхбшьаюцмчщбьдеблкфнэрщдаюкукг
 ш
 ищцвхзмтшвцкбчцвюхукцлюздэщаюэуьййкуинйтвуззгдуцдпцюаьндптэяжхкйеокцмпнтцмахуашвнф
 р
 жэуэвххкфжвьихвнещикоюлмякгпвньюаштубгуцаюешщбстешжэуэяжлюокхкыкзцмахушцбыаппмбжумб
 щ
 ймтфрщдкхфхпжикбьбулххудклкххаысэдкзкмэыэкпняжикюжщжшхчкпдцюэкажнддонэхюуцихлзцщеш
 е

кхкй дэражхкжээжшжхжхмдпздцпуэшэвнпхбчрщдфкхэяжлзцлтдмаучйыпхуождкпнуавхыэсжрутавхы
э
ежххенхуймздийежчхрэратдущещэпнгжфхпдъллнекюгжуэакбкыкинешокежфкхэдкзкмэыэстдптжшэя
ж
ьвлкбжрэчцлюздещпнвншрцмыэьвдкзкмэуеикоюлмвябчпдпхуаюфзогцпфрвнхквхщэлрхфдклкшкщзбаг
ь
гхалпрфнхфeklцируанрежхэбаыккпвнбчпкхякхкюцхкхкуадкзкмэалхфяконшумумаюэфпыйжуикоюлмй
ь
чэьжнпшжюпэщирогзюьвущептжяеикдмаьобщхкдклкшкцукцбьеждкихонэрогзюлнрзгштхуеашикоюлм
лювоезэурюшрексьюхягхонпнтешпжцежндпазыкщпшохухквгтмкуцбшэлквюззыкйэюцвхгрпнчярей
ежтнфзййльжужкудзмоквюшхйэьжыэжшпжыквютдкцдпийзюьфрюшрекийэхэоэммчькктфкуакзкьюлххэп
д
йцеэьеюяэююгцожфжпжхнщбвножчьзхшцфктнэавхсохкпрлюбжжэуеххсэпжцеоцмахуажлкбждцлюздэ
щякяббщчэсиквюдтвуанхфмуппхвйфлюююуцрчшрпнчяяркугхурлюхжбцгцпжхнфшсвпшэхибибьдхшл
х
йезюашябцуфйбьагхбэшбьйцчърцезлюэрчюлюфзыкэшбьеждьяюицчърцктнжудпоклофунтбьсофпвюгь
юнебнтжугтфзгюхвапммтшсвдкгшцэзцрчюкцгймхуаььвекаюствуфзмэщюекыэжхйэьжалхфзкудзмьяждкф
хыкбуймкбжвшэккыкюхшэекккыксвьвыэфзгшгнкэгцкьшхгнфзйвьомэфжхвщидицряюхфаыьжьюогнтву
ь
омбжвфкддщюхвоклйнкчзйймксэбцоквючьпнцптжяконшумбпзмэбжнбчпщдквююнлорзгдфбекдхкбж
у мбчрпнчяцзэуокйжкх

РОЗШИФРОВАННИЙ ТЕКСТ

когдапожарныеисоседиушлилеоауфманосталсясдедушкойсполдингомдугласомитомомвсеонизадумчиво
смотрелинадогорающиеостаткигаражалеоткнулногойвмокрууюзолуимедленновысказалточтолежалонаду
шепервоечтоузнаешьвжизниэточтотыдуракпоследнеечтоузнаешьэточтотывсетотжедуракмногоепередум
алязаодинтолькочасисказалсебедаведьтыслепойлеоауфманхотитеувидатьнастоящуюмашинуучастьяееиз
обрелитесьчилеттомуназадионавсеещеработаетневсгдаодинаковохорошонетновсетакиработаетионавс
евремяздесьапожарначалбылодугласдаконечнопожаргаражнолинаправадолгораздумыватьнадэтимнезач
емточтосгореловгараженеимеетникакогоотношениякчастьюонподнялсяпоступенямкрыльцаипоманили
хзасобойвотшепнуллеоауфманпосмотритевокнотишесейчасвывсеувидитедедушкассполдингдугласитомн
ерешительнозаглянулвбольшоеокновыходившеенаулицуитамвтепломсветелампыониувиделиточтохоте
лимпоказатьлеоауфманвстоловойзамаленькимстоликомсаулимаршаллигравившахматыребекканакрывал
астолкужинуюэмивырезалаизбумагиплатядлясвоихкуколругрисовалаакварельюджозефпускалпорельс
амзаводнойпаровоздверьвкухнюбылаоткрытатамвоблакепаралинаауфманвынималаиздуховкидымящую
сякастрюлюсжаркимвсерукивселицажилиидвигалисьиззастеколчутьслышнодоносилисьголосактотозвон
кораспевалпеснюпахлосвежимхлебомияснобылочтоэтосамыйнастоящийхлебкоторыйсейчаснамажутнас
тоящиммасломтутбыловсечтонадоивсеэтоживоеенеподдельноедедушкадугласитомовернулисьипоглядел
иналеоауфманаатотнеотрывносмотрелвокноиризовыйотсветлампилежалнаеголиценуконаченнобормотало
нэтооносамоеестьспервастихойгрустьюпотомсживымудовольствиеминаконецсоспокойнымодобрение
монследилкакдвижутсяцепляютсядругзадругаостанавливаютсяивновьуверенноировновертятсявсеинти
кииколесикиегодомашнегоочагамашинасчастьясказалонашинасчастьячерезминутегоуженебылоподо
кномдедушкадугласитомвиделикаконзахлопоталвдометопоправитчтонибудьтопередвинеттоскладкуразг
ладиттопылинкусдуеттакойжеделовитыйвинтикбольшойудивительнойбесконечнотонкойвечнотаинстве
ннойвечнодвижущейсямашиныапотомнепереставаяулыбатьсяониспустилисьскрыльцавпрохладнуюлетн
ююночьдваразавгодвдворвыносилибольшиехлопающиековрыирасстилалиихналучайкегдеонибылисов
семнекместуиказалиськакимитонеобитаемымипотомиздомавыходилимамаибабушкаврукахонинесликак
будтоспинкикрасивыхплетеныхкреселчтостоятвпаркеупавильонасгазированнойводойкаждомувручалит
акойжезлсширокойплетенойверхушкойивседугластомбабушкапрабабушкаимамастановилисьвкружокна
дпыльнымиузорамистаройарменииточносборищеведьмидомовыхзатемпознакупрабабушкиедваонамигн
етилиподожметгубывсевскидывалицепипринималисьбезпередышкимолотитьковрывоттебевоппригова
ривалапрабабушкабейтеблхмальчикинежалейтеившейнучтотытакоеговоришьукоризненнозамечалаейб
абушкавсесмеялисьвокругбушевалапыльнаябуряисмехпереходилвкашельвихрикормииструипесказолоти
стыхлопьятрубочного табакавзвивалисьввоздухитрепятиподбрасываемыевсеновыиминовымиударам
иостанавливаясьчтобыпередохнутьмальчикивиделиследысвоихбашмаковибашмаковвзрослыхтысячураз
отпечатавшиесянаузорахковравосточныйрисуноктоисчезалтопоявлялсявновьвместесмернымприбоемуд

аровчтоомывалегоберегавоттуттвоймужпролилкофеибабушкаударилапоковруздесьтыпролиласметануи прабабушкавыбилаизковраогромныйстолпылисмотритетутвесьворсвытоптанахребятаребятаявотчерни лапрабабушкаглупостиуменячернилалиловыеаэтообыкновенныесиниехлоппосмотритекакуюдорожкупр отопталиэтоизприхожейвкухнюохужэтаедаонадажельвовведетнаводопойдавайтекаповернемогдругимбокомаможетпростозаперетьвседверииникогонепускатилипустьразуваютсяещевприхожейхлопхлопнак онецковрыразвешанынавверевкахтомразглядываеузорхитроумныепетлиипереплетыцветыкакитозагадо чныефигурыразводызмеящиесялинииитомтычтостоишьвыбивайзанятновсетакивидетьвсякиевещиговор иттомдугласподозрительносмотритнанегочтотытамувиделдавесьгородлюдейдомавотинашдомхлопнаша улицахлопавонточерноеоврагхлопвотшколахлопавотэтачуднаязакорючкатыдугхлопвотпрабабушкабабу шкамамахлопсколькожелетпролежалунасэтотковерпятнацатьицелыхпятнацатьлетпонеумотопалидаже видныотпечаткибашмаковахнултомсилентыболтатьпареньсказалапрабабушкатутвидновсечтослучилось унасвдомезапятнацатьлетхлопконечноэтовсешлоеямогуибудущееувидатьвотсейчасзажмурюсьап отомрразпогляжунаэтиразводыисразуувиджугдемызавтрабудемходитьибежатьдугласпересталразмахиват ьвыбивалкойачтоещетытамвидишьглавнымобразомниткиивставилапрабабушкатуттолькоиосталасьоднао сновасразувиднокакеготкаливернозагадочносказалтомвэтусторонуниткиивтугожеявсевижучертирогаты егрешникивадухорошаяпогодаиплохаяпрогулкипраздничныеобедеземляничныепирыонсважнымвидомт ыкалвыбивалкойтоводнотовдругоеместоковрадапотвоемувыходитчтоядержутуткакойтопансионсказала бабушкавсякраснаяизапахавшаясятутвсевиднохотьинеченьяснодугтынагниголовунабокизажмурьоди нглазтольконесовсемконечноночьювиднолучшекогдаковервкомнателилампагоритивообщетогдатенибыва ютсамыеразныекривыеикосыесветлыеитемныеивиднокакниткиразбегаютсявовсестороныпощупаешьвор спогладишьаонкакшкуракакогонибудьзверяипахнеткакпустыняправдаправдажароипахнетипескомнавер нотакпахнеткаменныйгробгдежитмумиясмотривидишькрасноепятноэтогоритмашинасчастьяпростоке тчупскакогогосандвичасказаламаманетмашинасчастьявозразилдугласиемусталогрустночтоитутонагори тонтаннадеялсяналеоауфманаужнеготовсепоидетканнадоонвсехзаставитулыбатьсяикаждыйразкогдазе мляповернувшисьотсолнцанакренитсякчернымбезднамвселенноймаленькийгироскопкоторыйсидитудуг ласагдетовнутристанетповорачиватьсолнцуивотлеоауфманчтоототампрошляпилиосталасьтолькокучказ олыдапеплахлопхлопдугласссилойударилвыбивалкойсмотриетзеленыйэлектрическийавтомобильчик миссфернмиссробертасказалтомбиипбиипхлопвсерассмеялисьавоттвоилиниижизнидугонивсеузлахсли шкомногокислыхяблокисоленьеогурцыпередсномкоторыегедзакричалдугласвсматриваясьвзорковрав отэтатчерезгодэтатчерездваэтатчерзтричетыреипятьлетхлоппроволочнаявыбивалказашипелаточнозмеяв отэтанавсюостальнуюжизньсказалтомонударилпоковрустакойсилойчтовсяпыльпятитысячстолетийрван уласьизпотрясеннойтканинамгновеньезамерлаввоздухеипокадугласстоялзажмурясьистаралсяхотьчтони будьразглядетьвпереплетающихсянитяхипестрыхразводахковралавинаармянскойпылибеззвучнообруши ласьнанегоинавекипогреблаегонаглазахувсехродныхстараямиссисбентлиисаманемоглабысказатькарвсеэ тоначалосьоначастовиделадетейвбакалейнойлавкеточномошкиилиобезьянкимелькалионисредикочановк апустыисвязокбанановионаулыбаласьимиониулыбалисьвответмиссисбентливиделакаконибегаютзимой поснегуоставляянанемследыкаквдыхаютосеннийдымнаулицахакогдацветутяблонистряхиваютсяплечобла кадушистыхлепестковноонаникогдаихнебояласьдомунееобразцовомпорядкекаждаямелочьнасвоемпри вычномместеполывсегдацистовыметеныпровизияаккуратнозаготовленавпрокшляпныебулавкивоткнуты вподушечкиаящикикомодавспальнедоверхунабитывсякойвсячинойчтонакопиласьзадолгиегодымиссисб ентлибылаженщинабережливаяунеехранилисьстарыебилетытеатральныепрограммыобрывкикружевшар фикижелезнодорожныепересадочныебилетысловомвсеприметыисвидетельстваеедолгойжизниуменякуч апластинокговорилаонавоткарузоэтобыловньюйоркевдевятьсотшестнацатоммногодабылошестьдесят иджонбылещеживавотджунмунэтокажетсядевятьсотдвадцатьчетвертыйгодджонтолькочтоумертеперьза пахсухогосенаиплескводынапоминалиемукакхорошобылоспатьна свежемсене впустомсараепозадиодино койфермывсторонеотшумныхдорогподсеньюстариннойветряноймельницыкрыльякоторойтихопоскрипы валинадголовойсловноотсчитываяпролетающиегодылежатьбыопятькактогдавсюночьнасеновалеприслу шиваяськшорохузверьковинасекомыхкшелестулистьевктончайшимелеслышнымночнымзвукампозднове черомдумалонемубытьможетпослышатсяшагионприподниметсяиядетшагизатихнутонсноваляжетистан етглядетьвокошкосеновалаиувидиткакодинзадругимпогаснутогнимвоимикефермераидевошкаонаипрек раснаяседутемногоокнаистанетрасчесыватькосеетруднобудетразглядетьноеелицонапомнитемулицот ойдевушкикоторуюонзналкогдавовдалекомитеперьужебезвозвратноушедшемпрошломлицодевушкиуме вшейрадоватьсядождюнеуязвимойдляогненныхсветляковзнавшейочемговоритодуванчикеслиимпотерет ьподподбородкомдевушкаотойдетотокнапотомопятьпоявитсянаверхувсвоейзалитойлуннымсветомкомн аткеивнимаяголосусмертиподдревреактивныхсамолетовраздирающихнебенадвоедосамогогоризонтаонмо

нтэбудетлежатьвсвоемнадежномубежищена сеновалеисмотретькакудивительныенезнакомыеемузвезды тихоуходятзакрайнебаотступаяпереднежнымсветомзариутромоннепочувствуетусталостихотявсюночьон несомкнетглазивсюночьна губахегобудетигратьулыбкатеплыйзапахсенаивсеувиденноеиуслышанноевно чнойтишипослужитдлянегосамымлучшимотдыхомавнизуулестницыегобудетожидатьещеоднасовсемуж еневероятнаярадостьоносторожноспуститсясеновалаосвещенныйрозовымсветомраннегоутраполныйдо краевощущениемпрелестиземногосуществованияивдругамретнаместеувидевэтомаленькоечудопотомна клонитсаякоснетсяягорукойуподножьялестницыонувидитстакансхолоднымсвежиммолокомнесколькояб локигрушэтовсечтоемутеперьнужнодоказательствотогочтоогромныймирготовпринятьегоидатьемуврем яподуматьнадвсемнадчемондолженподуматьстаканмолокаяблокогрушаонвышелизводыберегринулсяна негокакогромнаяволнаприбоятемнотаиэтанезнакомаяемуместностьимиллионыневедомыхзапаховнесом ыхпрохладнымледенящиммокроетеловетромвсезторазомнавалилосьнамонтэаонотпрянулназадотэтойте мнотызапаховзвуквовушахшумелоголовакружиласьзвездылетелиемунавстречукакогненныметеорыему захотелосьсноваброситьсяяврекуйпуститьволнынесутеговсерванкудатеменнаягромадабереганапомнилаему т отслучайизегодетскихлеткогдакупаясьонбылсбитсногогромнойволнойсамойбольшойкакуюонкогдалибо виделонаоглушилаегоишвырнулавлзеленуютемнотунаполниларотносжелудоксоленожгучейводойслишко ммноговодятутбылослишкоммногоземлиивнезапноновтьместенуювставшейпереднимшорохчятотеньд ваглазасловносаманочьвдругглянулананегословнослегладелнанегомеханическийпесстолькопробежатьт акизмучитьсячутьнеутонутьзабратьсятакдалекостолькоперенестиикогдаужесчитаешьсебябезопасности исовздохомоблегчениявыходишьнаконецнаберегвдругпередтобоймеханическийпесизгорламонтэаыврв алсякрикнетэтослишкомслишкоммногодляодногочеловекатеньметнуласьвсторонуглазаисчезликаксухой дождьпосыпалисьосенниелистьямонтэбылодинвлесуоленьэтобылоленьмонтэощутилоострыйзапахмуск усасмешанныйзапахомкровиидыханиязверяззапахкардамонамхаикрестовникавглухойночидережьястено йбежалинанегоисноваотступалиназадбежалииотступаливтактбиениюкровистучащейввискахземлябылау стланаопавшимилистьямиихтутнавернобылимилиардыногимонтэапогружалисьвнихсловноонпереход илвбродсухуюшуршащуюрекучахнущуювоздикоитеплойпыльюсколькоразныхзапаховоткакбудтозап ахсырогокартофелятакпахнеткогдаразрежешьбольшуюкартофелинубелуюхолоднуюпролежавшуювсюн очьнаоткрытомвоздухевлунномсветеавотзапахпикулейвотзапахсельдерялежащегонакухонномстолесла быйзапахжелтойгорчицыизприоткрытойбаночкизапахмаровыхгвоздикизсоседнегосадамонтэапустилр укуитравянойстебелеккоснулсяеголадоникакбудторебеноктихоньковзялегозарукумонтэподнеспальцык лицуонипахлилакрицейоностановилсяглубоковдыхаязапахиземлиичемглубжеонвдыхалихтемосязаемеес тановилсядлянегоокружающиймирвовсемсвоемразнообразиимонтэауженебылопрежнегоощущенияпу стотытутбылочемнаполнитьсебяиотнынетакбудетвсегдаонбрелспотыкаясьпосухимлистьямивдругвэтом новоммиренеобычногонечтознакомоеегоногазаделачтотоотозвавшеесяглухимзвонмонпошарилрукойвт равеводносторонувдругуюжелезнодорожныерельсырельсыведущиепрочьотгородасквозьрощиилесаржа выерельсызброшенногожелезнодорожногопутипутьпокоторомуемунадойдтиэтобылотоединственнозна комоесрединовизнытотмагическийталисманкоторыйещепонадобитсяемунапервыхпорахкоторогоонсмо жеткоснутьсярукойчувствоватьвсевремяподногамипокабудетидтичереззаросликуманикичерезморезапах овиощущенийсквозьшорохишепотлесаондвинулсявпередпошпаламикудивлениусвоемуонвдругпочувст вовалчтотвердознаетнечточегооднаконикакнесмогбыдоказатькогдадавноклариссатожепроходилаздесь полчасаспустяпродрогшийосторожноступаяпошпаламостроющаякактемнотавпитываетсяеготелоза ползаевглазавротаушахстоитгуллесныхзвуковиногиисколотыокустарникиобожженыкрапивойонвдруг увиделвпередигоньогоньблеснулнасекундуисчезсновапоявилсяонмигалвдалисловночейтоглазмонтэга мернаместеказалосьстоитдохнутьнаэтотслабыйогонеконпогаснетноогонекгорелимонтэначалподкрад ыватьсякнемупрошлодобрыхпятнадцатьминутпреждечемемуудалосьподойтипоближеонстановилсяиук рывшисьзадеревомсталглядетьнаогоньтихоколеблющеесяпламябелоеиалоестраннымпоказалсямонтэгуэ тотогоньибоонтеперьозначалдлянегосовсемнечтораньшеэтотогоньничегонесжигалонсогревалмонтэв иделрукипротянутыекеготеплутолькорукителасидевшихвокругкострабылискрытытемнотойнадруками н еподвижныелицаоживленныеотблескамипламениони незналчтоогоньможетбытьтакимондаженеподозрев алчтоогоньможетнетолькоотниматьноидатьдажезапахэтогоогнябылсовсемдругойбогвестьскольконт а кпростоялотдаваясьнелепойноприятнойфантазиибудтоонлеснойзверькоторогосветкостравыманилизачщ иунегобыливлажныевгустыхресницахглазагладкаяшерстьшершавыймокрыйноскопытаунегобыливетвис тыерогаиеслибыкровьегопролиласьназемлюзапахлобыосеньюондолгостоялприслушиваяськтеплумупот рескиваниюкостравокругкострабылатишинаитишинабыланалицахлюдейибыловремяпосидетьподдеревь ямивблизизброшеннойколеипоглядетьнамирсостороныобнятьеговзглядомсловномирвьессосредоточи лсяздесьуэтогострасловномирэтолежащийнаугляхкусоксталикоторыйэтилюдидолжныбылиперековат

Бзано во ине толь ко о го нь ка зал ся ин ым ти ши на то же бы ла и но й мон т э г под ви ну л ся бли же к э той о со бой ти ши не от ко тор ой ка зал о сь за ви се ли сь су дь бы ми ра а за те мон ус лы шал го ло са лю ди го во ри ли но он не мо г е щ е ра з об р а т ь о чем ре чь их тек ла спо ко й но то г ром че то ти ше пе ре д го во ри в ш и ми бы л в сь ми ри он ин е сп е ша ра з г ляд ы ва ли е го о низ на ли зем лю зна ли ле са зна ли го ро д ле жа щ ий за ре кой в кон це за бро ш ен ной же ле зо до ро ж ной ко ле и он и го в о ри ли об ов се ми не бы ло ве щ и о ко тор ой он ин е мо г ли бы го во ри ть мон т э г чув ст во вал э то по жи вы ми н то на ц и я м их го ло со в по звуч ав ш и м в них нот ка ми зу м ле н и я и лю бо пы т ст ва а по том к то то из го во ри в ш их под ня л гла за и у ви дел мон т э га у ви дел в пер вый а мо ж е т бы т ь в с е дь м ой ра з и ч ей то го ло со к ли к ну ле го ла д но мо ж е те не пря т а т ь с я м он т э г от ступ ил в те м н о т у да у ж ла д н о не бой т е с ь с но ва про звуч ал то т же го ло си ло сти про сим к нам мон т э г ме д л ен но по до ш е л во круг ко ст ра си де ли пя те ро ста ри ко во де т ы х в те м н о си ни е из гру бой хол щ о вой тк а ни б р ю ки и ку рт ки и та к ие же те м н о си ни е ру ба ш ки он не зна л что и мо т ве т и т ь са ди т е с ь са ка зал че ло ве к ко тор ый по в с е й ви ди мо сти бы лу н их глав н ым хо ти те ко фе мон т э г мол ча см о тр ел как те м на я ды м я щ а я с т ру й ка л ь е т с я в ск ла д н у ю ж е с т я н у ю ку рж ку по том к то то про т я ну ле му э т у ку рж ку он не ло в ко от х ле б ну л чув ст ву я на се бе лю бо пы т н ы е в з г ляд ы го ря ч ий ко фе об жи га л гу бы но э то бы ло при ят но ли ца си де в ш и х во круг не го за ро сл и гу ст ы ми бо ро да ми но бор о ды бы ли оп рят ны и ак ку рат но под стри же ны и ру ки у э т их лю де й то же бы ли чи ст ы и оп рят ны ко г да он под хо д ил к ко ст ру он и в се по д ня ли с ь при вет ст ву я го с т я н о те пер ь с но ва ус е ли с ь мон т э г пи л ко фе а a a a

КОД

```
#include "windows.h"
#include <iostream>
#include <fstream>
#include<string>
#include<map>
#include<vector>
#include<algorithm>
#include<cmath>
#include <limits>
#include <iomanip>

using namespace std;
int A;
int B;
int x;
int y;
int gcd(int a, int b, int& x, int& y) {
    if (a == 0) {
        x = 0; y = 1;
        return b;
    }
    int x1, y1;
    int d = gcd(b % a, a, x1, y1);
    x = y1 - (b / a) * x1;
    y = x1;
    return d;
}
void ab(int Y1, int Y2, int X1, int X2, int m, int& a, int& b, bool& gcd_31, vector<int>& gcd_31_a,
vector<int>& gcd_31_b );
int main()
{

    SetConsoleOutputCP(1251);

    // ПУНКТ 2. 5 найчастіших біграм запропонованого шифртексту (за варіантом:12)-----
    -----
    map <string, int> bigrama_kvo; vector<pair<int, string>> kvo_bigrama; char ch1, ch2; string
ch1ch2;
    ifstream shifro_text_12("D:\\VISUAL STUDIO 4\\laba 3\\12.txt");
    while (!shifro_text_12.eof())
    {
        shifro_text_12.get(ch1);
        shifro_text_12.get(ch2);
        ch1ch2.push_back(ch1); ch1ch2.push_back(ch2);
```

```

        auto iterator_ch1ch2 = bigrama_kvo.find(ch1ch2);
        if (iterator_ch1ch2 == bigrama_kvo.end()) { bigrama_kvo.insert(pair<string, int>(ch1ch2,
1)); }

        else { iterator_ch1ch2->second++; }
        ch1ch2.clear();
    }
    for (auto it = bigrama_kvo.begin(); it != bigrama_kvo.end(); it++)
    {
        kvo_bigrama.push_back(make_pair(it->second, it->first));
    }
    sort(kvo_bigrama.rbegin(), kvo_bigrama.rend());
    //-----
    // ПУНКТ 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 ) , ( b а шляхом розв'язання системи (1). )-----

    map <char, int> alf{
    {'a',0},{ '6',1},{ 'В',2},{ 'Г',3},{ 'д',4},{ 'е',5},{ 'ж',6},{ 'з',7},{ 'и',8},{ 'й',9},{ 'к',10},{ 'л',11},{ 'м',
    ,12},{ 'н',13},{ 'о',14},{ 'п',15},{ 'р',16},{ 'с',17},{ 'т',18},{ 'у',19},{ 'ф',20},{ 'х',21},{ 'ц',22},{ 'ч',23
    },{'ш',24},{ 'щ',25},{ 'ь',26},{ 'ы',27},{ 'э',28},{ 'ю',29},{ 'я',30} };
    vector <int> X1_X2_X3_X4_X5 = { 545,417,572,403,168 };
    vector <int> Y1_Y2_Y3_Y4_Y5; string bigramaa; char a = 'a'; char b = '6'; int y1, y2; int
counter = 0;
    for (auto it = kvo_bigrama.begin(); it != kvo_bigrama.end(); ++it) //ЗАПОЛНЯЕМ ЧИСЛАМИ Y1 Y2 Y3
Y4 Y5
    {
        counter++;
        bigramaa = it->second;
        a = bigramaa[0];
        b = bigramaa[1];
        auto iter = alf.find(a);
        y1 = iter->second;
        iter = alf.find(b);
        y2 = iter->second;
        Y1_Y2_Y3_Y4_Y5.push_back(y1 * 31 + y2);
        if (counter == 5) { break; }
    }
    // ЗАПОЛНИЛИ ЧИСЛАМИ Y1 Y2 Y3 Y4 Y5

    multimap < int, int> pari_X_Y_25;
    int X; int Y; int i = 0;
    for (int i = 0; i <= 4; i++) {
        X = X1_X2_X3_X4_X5[i];
        for (int y = 0; y <= 4; y++)
        {
            Y = Y1_Y2_Y3_Y4_Y5[y];
            pari_X_Y_25.insert(pair<int, int>(X, Y));
        }
    }
    //int count = 0; int w = 0;
    int X1, X2, Y1, Y2, Z, XX;
    shifro_text_12.close();
    ifstream shifro_text2_12("D:\\VISUAL STUDIO 4\\laba 3\\12.txt");
    map <int, char> alf2{ { 0, 'a'},{1, '6'},{2, 'В'},{3, 'Г'},{4, 'д'},{5, 'е'},{6, 'ж'},{7,
'з'},{8, 'и'},{9, 'й'},{10, 'к'},{11, 'л'},{12, 'м'},{13, 'н'},{14, 'о'},{15, 'п'},{16, 'р'},{17,
'с'},{18, 'т'},{19, 'у'},{20, 'ф'},{21, 'х'},{22, 'ц'},{23, 'ч'},{24, 'ш'},{25, 'щ'},{26, 'ь'},{27,
'ы'},{28, 'э'},{29, 'ю'},{30, 'я' } };
    vector <string> VT;
    string vt;
    bool gcd_31;
    vector <int> gcd_31_a;
    vector <int> gcd_31_b;
    for (auto it = pari_X_Y_25.begin(); it != pari_X_Y_25.end(); ++it)
    {

        for (auto iter = pari_X_Y_25.begin(); iter != pari_X_Y_25.end(); ++iter)
        {
            if (it->first == 572) { break; }
            //if (it->first == 417 && iter->first == 572) { break; }
            cout << it->first << " " << iter->first << endl;
            gcd_31 = false;

```

```

gcd_31_b);
ab(it->second, iter->second, it->first, iter->first, 961, A, B, gcd_31, gcd_31_a,
if (gcd_31)
{
    for (int i = 0; i < 31; i++) {

        gcd(gcd_31_a[i], 31, x, y);
        if (x < 0) while (x < 0) x += 31;
        if (x > 0) while (x > 31) x -= 31;
        while (!shifro_text2_12.eof())
        {
            shifro_text2_12.get(ch1);
            shifro_text2_12.get(ch2);
            auto it1 = alf.find(ch1);

            auto it2 = alf.find(ch2);
            int Z = it1->second * 31 + it2->second;
            int XX = (Z - gcd_31_b[i]) * x;
            if (XX > 0) { while (XX > 31) XX = XX - 31; }
            if (XX < 0) { while (XX < 0) XX = XX + 31; }
            int x2 = XX % 31;
            int x1 = (XX - x2) / 31;
            auto it_x1 = alf2.find(x1);
            if (it_x1 == alf2.end()) { cout << "it_x1" << endl; }
            auto it_x2 = alf2.find(x2);
            if (it_x2 == alf2.end()) { cout << "it_x2" << endl; }
            vt.push_back(it_x1->second);
            vt.push_back(it_x2->second);
            //VT[i].push_back(it_x1->second);
            //VT[i].push_back(it_x2->second);

        }
        VT.push_back(vt);
        vt.clear();
        //shifro_text2_12.close();
        shifro_text2_12.clear();
        shifro_text2_12.seekg(0, ios_base::beg);

        /*
        cout << "Папа " << endl;
        cout << " X: " << it->first;
        cout << " Y: " << it->second;
        cout << endl;
        cout << "и napa" << endl;
        cout << "X: " << iter->first;
        cout << "Y: " << iter->second;
        cout << endl;
        cout << endl;
        */
        //count++;
    }
    gcd_31_a.clear();
    gcd_31_b.clear();
    gcd_31 = false;
}
else
{
    gcd(A, 961, x, y);
    if (x < 0) while (x < 0) x += 961;
    if (x > 0) while (x > 961) x -= 961;
    while (!shifro_text2_12.eof())
    {
        shifro_text2_12.get(ch1);
        shifro_text2_12.get(ch2);
        auto it1 = alf.find(ch1);

        auto it2 = alf.find(ch2);
        int Z = it1->second * 31 + it2->second;
        int XX = (Z - B) * x;
    }
}

```

```

        if (XX > 0) { while (XX > 961) XX = XX - 961; }
        if (XX < 0) { while (XX < 0) XX = XX + 961; }
        int x2 = XX % 31;
        int x1 = (XX - x2) / 31;
        auto it_x1 = alf2.find(x1);
        auto it_x2 = alf2.find(x2);
        vt.push_back(it_x1->second);
        vt.push_back(it_x2->second);
        //VT[i].push_back(it_x1->second);
        //VT[i].push_back(it_x2->second);

    }

    VT.push_back(vt);
    vt.clear();
    //shifro_text2_12.close();
    shifro_text2_12.clear();
    shifro_text2_12.seekg(0, ios_base::beg);
}

}

}

//cout << count << endl;
for (auto x : VT)
{
    if (x[0] != 'a' && x[1] != 'a' && x[2] != 'a')
    {
        bool boo = true;
        for (int i = 0; i < x.size(); i++)
        {
            ch1 = x[i];
            ch2 = x[i + 1];
            ch1ch2.push_back(ch1);
            ch1ch2.push_back(ch2);
            if (ch1ch2 == "аы" || ch1ch2 == "оы" || ch1ch2 == "еы" || ch1ch2 ==
"уы" || ch1ch2 == "оь" || ch1ch2 == "аь" || ch1ch2 == "оь" || ch1ch2 == "еь" || ch1ch2 == "иь" ||
ch1ch2 == "уь")
            {
                boo = false;
                ch1ch2.clear();
                break;
            }
            ch1ch2.clear();
        }
        if (boo)
        {
            for (int i = 0; i < x.size(); i++)
            {
                cout << x[i];
            }
            break;
        }
    }
}

//shifro_text2_12.close();
/*
char ch1, ch2;
map <char, int> alf{
{'a',0},{'б',1},{'в',2},{'г',3},{'д',4},{'е',5},{'ж',6},{'з',7},{'и',8},{'й',9},{'к',10},{'л',11},{'м',
12},{'н',13},{'о',14},{'п',15},{'р',16},{'с',17},{'т',18},{'у',19},{'ф',20},{'х',21},{'ц',22},{'ч',23
},{'ш',24},{'щ',25},{'ы',26},{'ь',27},{'э',28},{'ю',29},{'я',30} };
map <int, char> alf2{ { 0, 'a'},{1, 'б'},{2, 'в'},{3, 'г'},{4, 'д'},{5, 'е'},{6, 'ж'},{7,
'з'},{8, 'и'},{9, 'й'},{10, 'к'},{11, 'л'},{12, 'м'},{13, 'н'},{14, 'о'},{15, 'п'},{16, 'р'},{17,
'с'},{18, 'т'},{19, 'у'},{20, 'ф'},{21, 'х'},{22, 'ц'},{23, 'ч'},{24, 'ш'},{25, 'щ'},{26, 'ы'},{27,
'ь'},{28, 'э'},{29, 'ю'},{30, 'я'} };
vector <string> VT;

```

```

string vt;
ifstream shifro_text2_12("D:\\VISUAL STUDIO 4\\laba 3\\12.txt");
ab(165, 478, 545, 417, 961, A, B);
cout << "a=" << A << endl;
cout << "b=" << B << endl;
gcd(A, 961, x, y);
if (x < 0) while (x < 0) x += 961;
if (x > 0) while (x > 961) x -= 961;
while (!shifro_text2_12.eof())
{
    shifro_text2_12.get(ch1);
    shifro_text2_12.get(ch2);
    auto it1 = alf.find(ch1);
    auto it2 = alf.find(ch2);
    int Z = it1->second * 31 + it2->second;
    int XX = (Z - B) * x;
    if (XX > 0) { while (XX > 961) XX = XX - 961; }
    if (XX < 0) { while (XX < 0) XX = XX + 961; }
    int x2 = XX % 31;
    int x1 = (XX - x2) / 31;
    auto it_x1 = alf2.find(x1);
    auto it_x2 = alf2.find(x2);
    vt.push_back(it_x1->second);
    vt.push_back(it_x2->second);
    //VT[i].push_back(it_x1->second);
    //VT[i].push_back(it_x2->second);

}
VT.push_back(vt);
vt.clear();

int Z = 444; // первые две буквы ШТ
cout << "a_obratnoe=" << x << endl;
int XX = (Z - B) * x;
cout << "X=" << XX << endl;
if (XX > 0) { while (XX > 961) XX = XX - 961; }
if (XX < 0) { while (XX < 0) XX = XX + 961; }
cout << "X=" << XX << endl;
int x2 = XX % 31;
int x1 = (XX - x2) / 31;
cout << "x1=" << x1 << endl;
cout << "x2=" << x2 << endl;
*/

}

void ab(int Y1, int Y2, int X1, int X2, int m, int& a, int& b, bool& gcd_31, vector<int>& gcd_31_a,
vector<int>& gcd_31_b)
{
    int g = gcd(X1 - X2, m, x, y);
    //cout << "d=" << g << endl;
    if (g == 1){
        x = (x % m + m) % m;
        //cout << "Обратное:" << x << endl;

        a = (Y1 - Y2) * x;
        if (a > 0)
            while (a > m) a = a - m;
        if (a < 0)
            while (a < 0) a = a + m;

        b = Y1 - a * X1;
        if (b < 0)
            while (b < 0) b = b + m;

        if (b > m)
            while (b > m) b = b - m;
    }
    ///*
    if(g>1)

```

```

{
    gcd_31 = true;
    a=(Y1 - Y2)* x / 31;
    m = m / 31;
    if (a > 0)
        while (a > m) a = a - m;
    if (a < 0)
        while (a < 0) a = a + m;
    gcd_31_a.push_back(a);
    for (int i = 1; i < 31; i++)
    {
        a = a + i * 31;
        gcd_31_a.push_back(a);
    }

    for (int i = 0; i < 31; i++)
    {
        gcd_31_b.push_back(Y1 - gcd_31_a[i] * X1);
    }
}
//*/
}

```

ВИСНОВКИ

В ході практикума ми засвоїли принцип криптоаналізу шифру афінної біграмної підстановки, набули практичних навичок у частотному аналізі на прикладі розкриття моноалфавітної підстановки та опанували прийоми роботи в модулярній арифметиці.