ГУАП

КАФЕДРА 33

ОТЧЕТ   
ЗАЩИЩЕН С ОЦЕНКОЙ

ПРЕПОДАВАТЕЛЬ

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| доцент |  |  |  | А.В.Окатов |
| должность, уч. степень, звание |  | подпись, дата |  | инициалы, фамилия |

|  |
| --- |
| ОТЧЕТ О ЛАБОРАТОРНОЙ РАБОТЕ |
| ШИФР ОДНОАЛФАВИТНОЙ ЗАМЕНЫ |
| по курсу: ЗАЩИТА ИНФОРМАЦИИ |
|  |
|  |

РАБОТУ ВЫПОЛНИЛ

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| СТУДЕНТ ГР. № | 4941 |  |  |  | Н.С. Горбунов |
|  |  |  | подпись, дата |  | инициалы, фамилия |

Санкт-Петербург 2022

**Цель работы:** на практикеизучить шифр одноалфавитной замены

**Ход работы**

**Часть 1**

Для зашифровывания исходного текста выбрал шифр, основанный на квадрате Полибиля.

Иходный текст:

Лето – чудесное время года. Долгие солнечные дни сменяют короткие теплые ночи. Чаще всего стоит ясная погода, и бескрайнее синее небо простирается над головой. Деревья пышно убраны в яркие зеленые одежды. Под ними всюду густо растет трава, усеянная цветастыми огоньками летних цветов – маков, колокольчиков, клевера, пижмы, ромашки, ноготков… А над ними порхают бабочки и жужжат всякие мурашки. Лето украшает сады и огороды. Спеют сочные вишни, за ними спешат абрикосы и персики. Большие красные ягоды клубники клонятся низко к земле. Постепенно “загорают” в лучах летнего солнца еще недавно зеленые помидорчики. То тут, то там на арках завязываются огурцы. Цепкие колючие ветви ежевики сплошь усеяны сладкими темно-фиолетовыми, почти черными ягодами. И так повсюду – буйство цвета, праздник плодородия, приятное ощущение тепла и уюта. У лета чудесный звонкий голос – это поют высоко в небе или скрытые в ветвях деревьев птицы – маэстро-соловей, утренний жаворонок, веселый болтун-воробей. А ближе к вечеру музыка лета меняется – вступает хор сверчков, который не смолкает до утра. И даже дождь летом – теплый и ласковый. Под шатром низких туч воздух становится горячим. Прохладные капли дождя смывают пыль с дорог и листвы, благодаря чему после она заиграет еще более чистым изумрудным сиянием. Лето – яркое, разноцветное… Июнь не похож на август, и у июля есть чем порадовать глаз. Высокое чистое небо, теплая прозрачная вода речек, спелые фрукты, насыщенные цвета вокруг… Нет на свете человека, который не любил бы лета!

Секретный ключ: *ЭТОФИНАЛВСЕМЯПРУДЮШКЫБГЖЗХЦЧЩЬ*

Написал программу для шифрования, на выходе получил зашифрованный текст:

енюпгшиндяпноунмьфпиэипефвндпеянгяхниявдмняьщюспупюсвнюнрехняпгвгэзноднфпдюпвюьдяэьрпфпиэвтндсуэвянндвяннянтпрупдювуэнюдьяэифпепопвинуноцьрхжяпштуэяхоьусвнлненяхнпинаихрпиявмводщишфшдюпуэдюнююуэоэшдньяяэьбонюэдюхмвпфпяцсэмвенюявыбонюпомэспоспепспецгвспосенонуэрвамхупмэжсвяпфпюспоэяэиявмврпуыэщютэтпгсввашааэюодьсвнмшуэжсвенюпшсуэжэнюдэихвпфпупихдрнщюдпгяхновжявлэявмвдрнжэюэтувспдхврнудвсвтпецжвнсуэдяхньфпихсештявсвсепяьюдьявлспслнменрпдюнрняяплэфпуэщюоешгэыенюянфпдпеябэнзняниэояплненяхнрпмвипугвсвюпюшююпюэмяээусэылэоьлхоэщюдьпфшубхбнрсвнспещгвнонюовнановсвдрепжцшдньяхдеэисвмвюнмяпквпенюпохмврпгювгнуяхмвьфпиэмввюэсрподщиштшвдюопбонюэруэлиявсрепипупивьрувьюяпнпзшзнявнюнреэвшщюэшенюэгшиндяхвлопясввфпепдчюпрпщюохдпспоянтнвевдсухюхноонюоьыинуноцнорювбхмэчдюупдпепонвшюуняявваэопупяпсонднехвтпеюшяопуптнвэтевансонгнушмшлхсэенюэмняьнюдьодюшрэнюыпудонугспоспюпухвяндмпесэнюипшюуэвиэанипаиценюпмюнрехввеэдспохврпижэюупмявлсвыюшгоплишыдюэяповюдьфпуьгвмрупыеэияхнсэревипаиьдмхоэщюрхецдипупфвевдюохтеэфпиэуьгнмшрпденпяэлэвфуэнюнзнтпеннгвдюхмвлшмушияхмдвьявнменюпьуспнуэляпбонюяпнвщяцянрпыпаяээофшдювшвщеьндюцгнмрпуэипоэюцфеэлохдпспнгвдюпнянтпюнреэьруплуэгяэьопиэунгнсдрнехнкушсюхяэдхзняяхнбонюэопсушфянюяэдонюнгнепонсэспюпухвянещтветхенюэ

Для проверки работоспособности с помощью своей программы и расшифровал полученный текст:

ЛЕТОЧУДЕСНОЕВРЕМЯГОДАДОЛГИЕСОЛНЕЧНЫЕДНИСМЕНЯЮТКОРОТКИЕТЕПЛЫЕНОЧИЧАЩЕВСЕГОСТОИТЯСНАЯПОГОДАИБЕСКРАИНЕЕСИНЕЕНЕБОПРОСТИРАЕТСЯНАДГОЛОВОИДЕРЕВЬЯПЫШНОУБРАНЫВЯРКИЕЗЕЛЕНЫЕОДЕЖДЫПОДНИМИВСЮДУГУСТОРАСТЕТТРАВАУСЕЯННАЯЦВЕТАСТЫМИОГОНЬКАМИЛЕТНИХЦВЕТОВМАКОВКОЛОКОЛЬЧИКОВКЛЕВЕРАПИЖМЫРОМАШКИНОГОТКОВАНАДНИМИПОРХАЮТБАБОЧКИИЖУЖЖАТВСЯКИЕМУРАШКИЛЕТОУКРАШАЕТСАДЫИОГОРОДЫСПЕЮТСОЧНЫЕВИШНИЗАНИМИСПЕШАТАБРИКОСЫИПЕРСИКИБОЛЬШИЕКРАСНЫЕЯГОДЫКЛУБНИКИКЛОНЯТСЯНИЗКОКЗЕМЛЕПОСТЕПЕННОЗАГОРАЮТВЛУЧАХЛЕТНЕГОСОЛНЦАЕЩЕНЕДАВНОЗЕЛЕНЫЕПОМИДОРЧИКИТОТУТТОТАМНААРКАХЗАВЯЗЫВАЮТСЯОГУРЦЫЦЕПКИЕКОЛЮЧИЕВЕТВИЕЖЕВИКИСПЛОШЬУСЕЯНЫСЛАДКИМИТЕМНОФИОЛЕТОВЫМИПОЧТИЧЕРНЫМИЯГОДАМИИТАКПОВСЮДУБУИСТВОЦВЕТАПРАЗДНИКПЛОДОРОДИЯПРИЯТНОЕОЩУЩЕНИЕТЕПЛАИУЮТАУЛЕТАЧУДЕСНЫИЗВОНКИИГОЛОСЭТОПОЮТВЫСОКОВНЕБЕИЛИСКРЫТЫЕВВЕТВЯХДЕРЕВЬЕВПТИЦЫМАЭСТРОСОЛОВЕИУТРЕННИИЖАВОРОНОКВЕСЕЛЫИБОЛТУНВОРОБЕИАБЛИЖЕКВЕЧЕРУМУЗЫКАЛЕТАМЕНЯЕТСЯВСТУПАЕТХОРСВЕРЧКОВКОТОРЫИНЕСМОЛКАЕТДОУТРАИДАЖЕДОЖДЬЛЕТОМТЕПЛЫИИЛАСКОВЫИПОДШАТРОМНИЗКИХТУЧВОЗДУХСТАНОВИТСЯГОРЯЧИМПРОХЛАДНЫЕКАПЛИДОЖДЯСМЫВАЮТПЫЛЬСДОРОГИЛИСТВЫБЛАГОДАРЯЧЕМУПОСЛЕОНАЗАИГРАЕТЕЩЕБОЛЕЕЧИСТЫМИЗУМРУДНЫМСИЯНИЕМЛЕТОЯРКОЕРАЗНОЦВЕТНОЕИЮНЬНЕПОХОЖНААВГУСТИУИЮЛЯЕСТЬЧЕМПОРАДОВАТЬГЛАЗВЫСОКОЕЧИСТОЕНЕБОТЕПЛАЯПРОЗРАЧНАЯВОДАРЕЧЕКСПЕЛЫЕФРУКТЫНАСЫЩЕННЫЕЦВЕТАВОКРУГНЕТНАСВЕТЕЧЕЛОВЕКАКОТОРЫИНЕЛЮБИЛБЫЛЕТА

**Часть 2**

От Осташова А.С. перехватил шифровку:

овзхздфдщяогокмдебзььцоюзебеозяьжхемьксдллдуваэьлкхкелдзебсофсдвкооувоикдвуозоемкдэмыекдбефьмдозвуеогколмеьяозьзьвфдзхфпвззоскеукьфдькопвбефеьзвщбефдкокдьмозвсомьфеяаюьиуозуоьлдбоудозекдбовкаьрсевдозвщгспмхакдвдшыьмяьккыьвдшыьевзсыьжьбьуелуыждщвхкдмковфдлдккеьшпфеьздфбеозпшьсдщюзечзеьяьфпаноьбовкобелдуьмеудяьрыьэдуесекефьвеяеуоьомьквзуоккдщковсдукоккдщбовкхьмевздозвщекдцокеаэьлкькеуовхшьслдшьсдозбсьвяпжьудщвхьвдшрегпяырдозвщукоровдиьреувояпюжообефпбдозвщяьжхцокеауояьфегевзсдмдкьщбефсдькоьшосоздфгеуесьзяогокмдбзьцдвжьбешзоскеукьфдугспмьбеуькпозвщкобсояеэкешплдфекпбсьсемыекдвдшдкоуомдозюзелдвьядлдвздуящозоофькпзхвщкдевзсьоьпшосозхвбовкоьузезшьгфегмджьббсеклдозоовосмцоекдкомпшдозеряьлфеьвшосзьекдбсевзебеозбеозмезоибесбефдкоьввщфкозгеяевькоересуозвщмыидкьокешыфегмдрсевдошвщгспмхакдзоскььшылкдошшыбекьшдошьувосдукегспмхакдзоскььздфрпмозувогмд

Начал расшифровку на основе статистики встречаемости букв в русском языке.

Таблица 1. Частота встречаемости букв

|  |  |  |
| --- | --- | --- |
| Буква, другой символ | Частота встречаемости в тексте | Частота встречаемости в русском языке |
| **А** | 10 | **62** |
| **Б** | 36 | **14** |
| **В** | 64 | **38** |
| **Г** | 17 | **13** |
| **Д** | 89 | **25** |
| **Е, Ё** | 91 | **72** |
| **Ж** | 9 | **7** |
| **3** | 66 | **16** |
| **И, Й** | 5 | **72** |
| **К** | 80 | **28** |
| **Л** | 19 | **35** |
| **М** | 33 | **26** |
| **Н** | 1 | **53** |
| **О** | 110 | **90** |
| **П** | 23 | **23** |
| **Р** | 11 | **40** |
| **С** | 43 | **45** |
| **Т** | 0 | **53** |
| **У** | 37 | **21** |
| **Ф** | 31 | **2** |
| **Х** | 16 | **9** |
| **Ц** | 5 | **4** |
| **Ч** | 1 | **4** |
| **Ш** | 25 | **6** |
| **Щ** | 21 | **3** |
| **Ы** | 15 | **16** |
| **Ь, Ъ** | 87 | **14** |
| **Э** | 5 | **3** |
| **Ю** | 5 | **16** |
| **Я** | 33 | **18** |

Начал замены, предполагая, что наиболее встречаемся буква в тексте есть наиболее встречаемая буква в русском языке. Однако в первой же замене необходимо было менять «о» на «о». А затем «е» на «е». Так как это маловероятно, я решил поменять замены местами и продолжить.

Таблица 2. Замены, основанные на частоте встречаемости букв

|  |  |
| --- | --- |
| Старая буква | Новая буква |
| О | Е |
| Е | О |
| Д | А |
| Ь | И |
| К | Н |
| З | Т |
| В | С |
| С | Р |

После 8 первых замен получился текст:

**ЕСТх**ТАфАщяЕгЕНмАОбТИцЕюТОбОЕТяИжхОмИНРАллАуСаэИлНхНОлАТОбРЕфРАСНЕЕуСЕиНАСуЕТЕОмНАэмыОНАбОфИмАЕТСуОЕгНЕлмОИяЕТИТИСфАТхфпСТТЕРНОуНИфАИНЕпСбОфОИТСщбОфАНЕНАИмЕТСРЕмИфОяаюИиуЕТуЕИлАбЕуАЕТОНАбЕСНаИ**рРОСАЕТСщ**гРпмхаНАСАшыИмяИННыИСАшыИ**ОСТРыИ**жИбИуОлуыжАщСхНАмНЕСфАлАННОИшпфОИТАфбОЕТпшИРАщюТОчТОИяИфпанЕИбЕСНЕбОлАуИмОуАяИрыИэАуОРОНОфИСОяОуЕИЕмИНСТуЕННАщНЕСРАуНЕННАщбЕСНхИмОСТАЕТСщОНАцЕНОаэИлНИНОуЕСхшИРлАшИРАЕТбРИСяпжИуАщСхИСАшрОгпяырАЕТСщуНЕрЕСАиИрОуСЕяпюжЕЕбОфпбАЕТСщяИжхцЕНОауЕяИфОгОСТРАмАНИщбОфРАИНЕИшЕРЕТАфгОуОРИТяЕгЕНмАбТИцАСжИбОшТЕРНОуНИфАугРпмИбОуИНпЕТСщНЕбРЕяОэНОшплАфОНпбРИРОмыОНАСАшАНЕуЕмАЕТюТОлАСИяАлАСТАуящЕТЕЕфИНпТхСщНАОСТРИЕИпшЕРЕТхСбЕСНЕИуТОТшИгфОгмАжИббРОНлАЕТЕЕСЕРмцЕОНАНЕмпшАЕТОряИлфОИСшЕРТИОНАбРОСТОбОЕТбОЕТмОТЕибОРбОфАНЕИССщфНЕТгОяОСИНЕОрОРуЕТСщмыиАНИЕНОшыфОгмАрРОСАЕшСщгРпмхаНАТЕРНИИшылНАЕшшыбОНИшАЕшИуСЕРАуНОгРпмхаНАТЕРНИИТАфрпмЕТуСЕгмА

Со сложностями, но можно угадать некоторые слова, и по ним уже выполнить замену. К примеру, первые 4 символа очень похожи на слово «есть», а значит можно заменить «х» на «ь».

Таблица 2. Замены, основанные распозновании слов

|  |  |
| --- | --- |
| Старая буква | Новая буква |
| Х | Ь |
| У | В |
| Ф | К |
| Б | П |
| Щ | Я |
| Ш | М |
| М | Д |
| Ю | Ч |
| Л | З |
| Э | Ж |
| А | Ю |
| Ж | Ш |
| Я | Л |
| П | У |
| Р | Б |
| И | Э |
| Н | Щ |
| Г | Г |
| Ц | Ц |
| Ы | Ы |

Получившийся текст:

ЕСТЬТАКАЯЛЕГЕНДАОПТИЦЕЧТОПОЕТЛИШЬОДИНРАЗЗАВСЮЖИЗНЬНОЗАТОПРЕКРАСНЕЕВСЕХНАСВЕТЕОДНАЖДЫОНАПОКИДАЕТСВОЕГНЕЗДОИЛЕТИТИСКАТЬКУСТТЕРНОВНИКАИНЕУСПОКОИТСЯПОКАНЕНАИДЕТСРЕДИКОЛЮЧИХВЕТВЕИЗАПЕВАЕТОНАПЕСНЮИБРОСАЕТСЯГРУДЬЮНАСАМЫИДЛИННЫИСАМЫИОСТРЫИШИПИВОЗВЫШАЯСЬНАДНЕСКАЗАННОИМУКОИТАКПОЕТУМИРАЯЧТОЭТОИЛИКУЮЩЕИПЕСНЕПОЗАВИДОВАЛИБЫИЖАВОРОНОКИСОЛОВЕИЕДИНСТВЕННАЯНЕСРАВНЕННАЯПЕСНЬИДОСТАЕТСЯОНАЦЕНОЮЖИЗНИНОВЕСЬМИРЗАМИРАЕТПРИСЛУШИВАЯСЬИСАМБОГУЛЫБАЕТСЯВНЕБЕСАХИБОВСЕЛУЧШЕЕПОКУПАЕТСЯЛИШЬЦЕНОЮВЕЛИКОГОСТРАДАНИЯПОКРАИНЕИМЕРЕТАКГОВОРИТЛЕГЕНДАПТИЦАСШИПОМТЕРНОВНИКАВГРУДИПОВИНУЕТСЯНЕПРЕЛОЖНОМУЗАКОНУПРИРОДЫОНАСАМАНЕВЕДАЕТЧТОЗАСИЛАЗАСТАВЛЯЕТЕЕКИНУТЬСЯНАОСТРИЕИУМЕРЕТЬСПЕСНЕИВТОТМИГКОГДАШИППРОНЗАЕТЕЕСЕРДЦЕОНАНЕДУМАЕТОБЛИЗКОИСМЕРТИОНАПРОСТОПОЕТПОЕТДОТЕХПОРПОКАНЕИССЯКНЕТГОЛОСИНЕОБОРВЕТСЯДЫХАНИЕНОМЫКОГДАБРОСАЕМСЯГРУДЬЮНАТЕРНИИМЫЗНАЕММЫПОНИМАЕМИВСЕРАВНОГРУДЬЮНАТЕРНИИТАКБУДЕТВСЕГДА

**Вывод:**

1. Был изучен и реализован на языке C# шифр одноалфавитной замены на базе квадрата Полибиля.
2. Был перехвачен шифртекст и удачно расшифрован с помощью таблицы частоты встречаемости букв в русском языке.
3. Удачная расшифровка была возможна благодаря тому, что был перехвачен довольной большой текст. В случаях, когда перехватывается маленький шифротекст, удачное расшифрование невозможно т. к. частоты букв не соотносятся с частотами встречаемости букв в русском языке.