Санкт-Петербургский Национальный

Исследовательский Университет

Информационных Технологий, Механики и Оптики

Лабораторная работа №3

«Многопетлевые полиалфавитные подстановки»

Дисциплина: Методы и ср-ва защиты комп-ой информации

Студент: Дидин Е.В.

Группа: Р3401

Вариант: 4

Санкт-Петербург

2016 год

1. **Задание**

Дешифровать криптограмму, зашифрованную многопетлевым шифром.

Определить период шифра предлагаемой криптограммы. Получить составной ключ, вычислить первичные ключи.

1. **Выполнение**

*Криптограмма:*

МЕЭЗЛМ ЖОЬЯАРОЫЙВКХСУСБЬЮФЩУБССАЭСЭЙЧЙЪЧОЫП ЬШМЩБСМХЕЯЖХЬАЭЩССКХВЕ ЭС ТЩНДСТЪЪ ЗВЫЫЬФБЭЦЫЭО ОРОРИЮШРЧЧОХБПЬРГВ ЙЭЩФЩБУМСЕКЬИПРСЯЭГКЕЧМЪЙНЬГЦТЦГЦФВЮЕЛЫЖЛЭФЭДСПФДЬИШ ШПЕЩУВРЦЧТХ К ЭЕКЪВУЗСЗЭКЭЮЭГ ЙЙЩЦРЛБШЩЕУОХМЯЦОХХТТЧЯФКОСЭРТСЯЩСДСАЭУФБЧЪДЩП ЭХКЗБЛСЕЙЪЧ ЬЪЫЙЮЛВДЕВВЫЧЯВРУАЛ ИЭЬЕОЕПНВОЯПЪХБГФВЕСВФ Х ВЖ УЦЭПЪЙОХАЬОБМХЪЮХУАБТЧФАЭВЮСП ОВРФБВЬЕФУОК ХЦА ВСЩЗОЫЩПРУЦЛ ИЗРБЩВЫГМНУАЭПДЩСКГХДЦАФЬАЪ ЦЯШГЭДАВЯЮУЦОЗТЙТУБСНЮГНВЬФВИЭЕТЗБШБЪОЮЮЗЮФНЯДЖКЬУСКЕ БПЫЫЪЯЙОЩСЗВЮЕОЫЧТЬЕЭШЛЖСДСАУЕВЪОЪЫАЛВЪХЕЙСКФЬЭНЮОЦЧВЧТОЛЖУНВШЯАЖЮАЕЛ ЛН КЬУОШЪУУИУРХСФФЧТПАПТМГЧКЧГЭМБЮ ЕЙУОУСШЛШ ЕГВ МФЛФВЗЛЛ ОШВТЖРОЬУУООЯТЪЬЭЛЕЦВЦЕРОХЪУФЛЩИЫЫЪЖ ЧОППЛЦКПУЯВТГБЮПЧПХТЩП ОЖЫБОПБШЮЮЭКЭИМЮПВКЫГЩТФ ПЖРЧМЪЗНЗЭЭЬЩОЬЯОЦЪНУЯВЖГЗАФВТ ЩРО ОЕВОРЭЭКОРЯЕЮПЗУСТИМ НЩХЪШДЯЕВЩЮДХСВФШЮУЮЕЭЕЗЩХСВ ЕЫЗЕПТКСНОПЕВДТИЧЙКНЧ ВЙЮЫ ПНЮГНДЪСАЖРО ГИЙРЮЭСУРЮПСММЫЦЪВТГЙЬЯЭОВЫБРАЧЫКП ЖОГПРЙ ЪСЪГЧОИЯЧЫХФ ЭЕЯУААХАРБШОЕФШЭТ ЪХРСТСХЩЬ РЖЫЖРРАЩЦИВЮЭАЮЩЩЧ ЬЙЬЛБГЗХЬАДЗОЧКГЙИСХМТ ЗЪЩУИСАЭТЪЬЧДИХ ХЧЭЪЫЛВАЙЛДРФНЭЮЖОШПМЧЧВЬГСМХЗОЧБЧ РХОЦЦЭРЯЕОЕФНЭСГДЭЛЭЛВЮЧЫЪФЪШАССИЛ ЮМСЕЦЖТЫБТМПЪПБГНГДЙЭФАЕТЩЕИУШВТХКБКЙУОПМЬЫРЮСМХЯУА ФЬЪЩТЕЩВЛБФЭАЩЩЬШ ИКЛКТНХЮЪЫВЕАЫЪБТОЮЕВНСОЛДОЫП ХШКЮСФЦЪУППФЧТЗСЕЕСХЛЕЯЕО ПШЯЫГД КФЮФГБЦАФЛЖ ЬЕДЯЦПРЮЭЭКОСЪАЩЙМРЖВНЗЕНЧЬРЫКСССКХМРСПЯЖЮУОСССЫЪТЗГХЙУГЪЯОЪНШИЛГАПЪЭЭКЯОХАРЫЦКФВКЦИ ПЧЖШГРХООЫНЧЯЛ КЧН КТХЪХТКГАЕЯРФЭЭКСЮИОЦИКСЕГШСНДВЧЬЪХБСЕЮЧРФСААЖРЩЖМЖКРЮЭ ЫФ Ф ВЖЖКВХСФВНАХЪШЗМРИХХМРГЛЫЛОДАОСЩИЬЮСХЕЭРФБПЮ УФ ЪВЭХФЕУЮЪНРАЙЧШКЬЛУЮЙНЗБТАЕСЕВЪХ УЧЖОЮФН ИЭПЪЫ ЖВЧШЕБЭОЭИВФРЖЯЭРЯЭСАУУЪ ВЙЯЫДЖСЯЧЯЖВЯАЗЛЕБЖАЭДЧНЖАЬЬШ ОЬИФСДГНДЦФЪФТЭЯЧТЪМКВРЭ КЭЮЭНТЙЙЩЦРЛБШЩХЕКТМАЛМКХЯРЭЩЖАЫЦОЯБЭЛЛЮЛВЮЯННЪЪЫЪУЕГЪЕКРЫЭ КФЫФ ЦКЕРЬСВШДЦЬЗОЪЫХУЕХХОФ НЭЕЭЧОБТБЗЙСДЮАШНВЦЯУУЦУАЛ ЭГ ИКРЭЪБ ДЬ ЬДВЛХИЬЪЩЧ ЩЬЖСЗХОБЯЕЫШСИ ТДЩЫИКЛПЮЧПХЕАЫИЮЖМФХЛЖЪКОЕПТОДБЭЮУЮВЦБЭЫРМПРУЩТИЭФЭМС ФИГАОССФКЮГЮПЮЧЯЖЪЬУЖЩЕСЧГГЗЯКЙДЧНЧЗСФЫЧЯБВЮЧРПЙЭЧЩЙОМФХКВСОФЫФЮЭ ФШЛЭ НВЮЧЛШВОЪЫ ЖДЛИЭПЪГЬЮТЬОЯБЭЛЛСЗЕИГМФЕЭДЗПТИЛЙРФ ОЕЧФФ ГШЮЩСПИЖЙОФШУШЪБШОКАЭУОЙОЙАУЬАСЫЪЮЬУИДВУБЭНЯВРФКЬИГВЭЮОЛЦШЧЙСОЭЩБВЕГЗЬЖХОЧЭЯЦАЛШЭ ХЛОЫЭЯАОИЧИФСФХЫДУФЧЙЗИХОЛФХКВСХЧИЭШБЮСОИЫ ЖЦХЖЮВЙЭЧВУЮУЙХМРСЗЯЩМНЮР ЩЫЬГЛВЭШ ЪАОБИУФРММЕДТ ЖЛМНЬАСЗЮКЪВЦКЕТУНБРЪЩНВФШЮАВЩОЫЬЦЦ ФШЪЭНПЦХДОФЕЭШЯЩУЕЩЮВБВЭУЖЯЬТОЫЙВПДЬИЯЧЦЬФУАЕЩУЫЛБЛТХРЪЩОХПТЧЦЪП УСЩШНЛЪЯШБРУЕЬГ П ВОЛЗУЪЬЧЙН ЗЛАШНЧФЫАКФЕАХХ БЦЛЪАЬАОГ ЪЮЩБСХХ НЩХЪОТЦЕВЛЧЮТТБОЭБЮОУЩФЫЙСЕИЕМЫУУОДКЯХАЛВЮБЬЛАЖЯЬШ ВЬИЙЭВФТГНЦП ДКЯЕПЪХИЗВПЬАДОЫ ЪЙДЫДХЮБЧЯГЗ ЭЫЭЕОЫИОМТИПЙКНЩ ХХЫНЯСМХЬЬДВТШЪ ФДЛКЙХБШЫАОЯАЕЯКЖУСЦВШМЬЩХОХЪТЖШЩУЭКС УИБСОСОЦЪЪ РБАЧДЖВОПМСЕКЬЫМРВПКШРИЪАСЩИЬГУСЫДОФБФТЯЬД УЦЦКГШОДЭЮУОБКЪШ ВЗАЦНВЦЭВИЮА ЪЗЭО НУЖЯООНТЙЛЛЮСПХЬУ ЪОПМЯЕБЖАЛБВЛЦЭПЫЧЕСОКРФРИЩЕНШВЬЧИАЖ ОГОФ ФЬУШНВОБЩИЬГВСЧЕЮВБЙТВВОЛФЫКВСМЭЙАЮЭЕЯЧХФСНСЩЬОФЧ Ю ХЕЗМХМРВИФЭЬЦЫ ВШШТ ПВАХТЭФЦУЙСКАЛШККЮЮАЮЪЙЬОСЫЕРЦЛОЮЧХХФЦЮИЪЕЗСБИЗЫЭ ЩБЮЭНТЙЮПЧВТЕЕТВ ХУЕЩЕЖФЗЩБЧАЭШ ЬЦДТЧВЙСРСХБОЯФРНЕЯЕИЛЖЭМТНЬЪЭ ЭМСТЪХТУРГИ ВАОФЫИУЯШЮЭЙДЯЭЫО ПКСТЪТЦИФСЧПЩЭАШЕМУОЭЗЩБ ОЪЩРЩП ЪЙЙЫЧЗГЗЭЩРЕАХИРФТРЦИРСЪАЛОППШЯЗЪОЭГЕЫЧТЗЙЭХЪЫФЛЗЛЮБЪЭАЮЮУЯЬСОИЦХЛИХЫЬЩПОШ РЩДСЕГКФЮЪАОХЪЫЧЙЛЮКИФЗЪОФГЭГЕЦЕСОГВЕ ЭСЖЦРЯАКПЗУРВЕХГЬДЩЭВЪБЖУЬГКБЯЮЖЮЪНФЕСЩИЦЧКРГАНЗФЬШЮЯЕБЖАЛБЮЮЪЖОЯЪУХЙЗЩСПРГЫЬФДПФИУЕКЪЗЛТМТОЕБФЬОСЛХЦ ВЗЫЗФХЖКТЭРЧТЬЦТЗСЕОЬЪОСН УЪРХСВЛЭЩРТОЭЫЫЕИЛШЭУГЮЯАЬАОБМХИКАУИЪЕ ЧДПДВВБ НЫАУГ ЭШЧХОМ ЪЯЩБГВКЕ УФФГЕЩЕБЖХМТ ПЧЫЬЦЩ ФЫТТОФФЧЫХЕААЕМРОЛЧВЙБЮ ЙБТФНСАМЩСТСДТ Х СЪТА ЮЦЖП ЭЮИЭЫЧКЯЭМЖСЕВТЙАФЬФЯЕОЕБМНКАСМЭЙЪАХИЭКЪММВРЫЖЮЪВУАЕЩТОХХМТЧАЯЩУЬШ ЦХЩКГИШХБ ВФЭФЖСУУЧХЯЖЪПФГКЫЭСГЕЪЧ УЖИВОФЭОК ЬФБЛЗЛННЗЭШАУЮЕБЕЪЬОПВДЕЫУ ОХЛОЕБСЭКВЦВХЕЭЯАЬСЩИЪМХНЮЧЯГЗ ДВВБСКХ ПЪДОЕПНСИЦЭЪЮСПРГЮУЕЖСУЪЯРОЩХЕБУБЧКФЩКНМЯЪН УСЗЧЦФЩПЩ РЛСЧЮЭГМЭЭЕОЭЯОЦПЕЛЭВ ЗЕНЧЕФТКСИНЪХЛПСКФШБЕФЛСЛХКЦГОЫБЬФГЭТПЯЦОГГЭРЖНПЕНУЫОЫЙЯЩБСЖЫЧТХЫФТСЦЦНЖЫЭФЧКЧШЦОЪЕХБВРСЖОИЩЬЯВОДЫЭЕКЯЪЮБЯВОЭЭЯАИХКЕЩСНУЦИЫВЪОЪЫАЛВЪХКЗСЙЭЬЪЦОБМЙЛЪББХЦЙЙФЪТАЪЯШ ОЮБАКЕГШСНАЕЮЧИЭЧВСЕБЬЧФЬАЪЕФТКХОСДОЩШЮЮФДВЬЫНЭБОЖЦНВЖЕУЩЮУЫШХЕБУВЦЕПТФЖЯДЖКЧЖСХЯОЩХЕУЪТАЛМХАРБЮЦЭЭНАРДОЗРЧВРЫЧПЪЫПДЦРО Э НЭФЮАФ МОН ЙЭЩЫХЛХЪНЧВЯАМСЕВЛГБКЯЛЕЮ СЕСЦХЬЭЛВЫЫЬФВРВЫВОЛФЖЩБЬЭЩЖЪЙДУСЧИКФВРЮМНБЪОФХЬФ ЯЖМРЬЛФЕЧМОТ ХЦХ ВЦЬШЯФЭОАЙСЧНЪЖПЮСЗПВО ЭЛНФИК РВГБОЬХЪГЩРУАЛШЕЖДЭБШТЬЯЫСШЮШРВФШЭЮЯХСК ЪЕДМАВМ ЭСЗФЮФДЪЙИШСТСВЦЩФЛААЪЮФШМХВЕ ЭЧ ЫУЬИЭКЛЖССНЦЯОЧМЧГЦРИБЧЮДКСЛАШЭСЯОЮЧХ СТИМЭЧФШУШЪУЕГЧИЯРЬЛШШУЮФВЯШЛЭЪВСВЕНЦПЪАЪУАКЪШЮП ЭЩЖЪЙДОСЩКУ ДУЫВЬФВТВИЭУУЙХОКЭРОЙАОЪОСЛИЦЧИВЖЪЦДЪЮНЖРО ЩЫМРЬЛЯЕЙЪОП ЫЕЮЙРЮБЧЩЭМКТЖЯЙУВЫЖБФЛЪЮОВЭТРЙЛЗЮВРЫЧЫХЩФЮЪЫФЛЗЛЛБ КЭШСЦ ЕЭШЪШТВЩЫЖЦФЗО ФФ ЩЦЭЪЧВОЖЬН Т ИЪТЦИФСЧДЗЧ ДЭЯИАЧХЗВЬЭЭЕЭНБВЧХВБЪЕГЫЙЯУФЯУЛИОРКЫПУРЭЦЩЩААЫФКЩКФВСЧПЦДББРЪВЛНЗХОВЮЛТЖОЯФБРЙБЦ ЕИОШМФЗТВИШЖ ОЖПВФЮЪЩОЫПДСЫМРЯГПЮЧЪВДУАКСЕОЩХДПТИОПАЬОТЧЩ ЫНВТЫЗУЩФЬЫЖРСИГСЭЖФЮОЗБ Ч ФШБПЧУЙЦЙЙЕУОАМРОСЫГИЮЩЛСЩЬЦН ЬШЕЖЗГВКЕ УФЭ ИРЗУРЫПБЮРЕААУЪЬЯШЪУВНЦНШ РФФЦИРОЛФХЛГЛЬСААЙОЕХШЪЬФСЛБЧПДВ ЫЭРИЫУГ БВЕЪЮОДАОСЫВПЪХВШЧ ЪАЬАГРРРСДЛУГЕО ПНУОЭТЗЩЫВХЫДУЮФЩАЕМЬОЛЮОМДХПГЭНФГ ЙЙЩЦХГМ РХУОШЮЯЕВЪАЫБЪЭЯЩЦАЫ

*Открытый текст:*

ЖЕСТОКОЙ ГРУБОЙ И ГОРЬКОЙ КАЗАЛАСЬ ЗЕМЛЯ НА КОТОРОЙ ОСТАНОВИЛСЯ ЕГО ВЗГЛЯД И ПОД ЕГО НОГАМИ ВЫСОЧАЙШИЙ ХРЕБЕТ ЭФЕЛ ДУАТА КРУТО БОЛЬШИМИ УСТУПАМИ ОПУСКАЛСЯ В ТЕМНЫЙ ЖЕЛОБ НА ДАЛЬНЕМ КОНЦЕ КОТОРОГО ПОДНИМАЛСЯ ВТОРОЙ ХРЕБЕТ ГОРАЗДО БОЛЕЕ НИЗКИЙ С НЕРОВНЫМИ КРАЯМИ ПОХОЖИМИ НА КЛЫКИ НА ФОНЕ КРАСНОГО СВЕТА ЗА НИМ ЭТО БЫЛ УГРЮМЫЙ МОРГАЙ ВНУТРЕННЕЕ КОЛЬЦО ОГРАЖДАЮЩЕЕ ЭТУ ЗЕМЛЮ ДАЛЕКО ЗА НИМ НО ПРЯМО ВПЕРЕДИ ЗА ШИРОКИМ ОЗЕРОМ ТЬМЫ ИСПЕЩРЕННЫМ КРОХОТНЫМИ ОГОНЬКАМИ ВИДНЕЛОСЬ БОЛЬШОЕ ЗАРЕВО ИЗ НЕГО ПОДНИМАЛИСЬ ОГРОМНЫЕ КОЛОННЫ КЛУБЯЩЕГОСЯ ДЫМА ТУСКЛО КРАСНЫЕ У ОСНОВАНИЯ ЧЕРНЫЕ ВВЕРХУ ГДЕ ОНИ СЛИВАЛИСЬ В ВОЛНУЮЩИЙСЯ БАЛДАХИН ПОКРЫВАВШИЙ ВСЮ ЭТУ ПРОКЛЯТУЮ ЗЕМЛЮ СЭМ СМОТРЕЛ НА ОРОДРУИН ГОРУ ОГНЯ И ВРЕМЯ ОТ ВРЕМЕНИ ПЕЧИ ДАЛЕКО ВНИЗУ ЕЕ ПЕПЕЛЬНОГО КОНУСА РАЗОГРЕВАЛИСЬ И С ГРОМКИМ РЕВОМ И ШУМОМ ВЫБРАСЫВАЛИ ПОТОКИ РАСКАЛЕННОЙ ЛАВЫ ИЗ ЩЕЛЕЙ НА СКЛОНАХ ГОРЫ НЕКОТОРЫЕ ПО БОЛЬШИМ КАНАЛАМ ТЕКЛИ К БАРАД ДУРУ ДРУГИЕ ПРОКЛАДЫВАЛИ СЕБЕ ИЗВИЛИСТЫЙ ПУТЬ ПО КАМЕНИСТОЙ РАВНИНЕ ПОКА ОНИ НЕ ОСТЫВАЛИ И НЕ ЛЕЖАЛИ КАК ИЗОГНУТЫЕ ДРАКОНЬИ ТУШИ ИЗВЕРГНУТЫЕ ПЫТАЕМОЙ ЗЕМЛЕЙ ИМЕННО В ТАКОЙ ЧАС АКТИВНОСТИ СМОТРЕЛ СЭМ НА ГОРУ СУДЬБЫ И НА ЕЕ ОГНИ ЗАКРЫТЫЕ ВЫСОКИМ ЭФЕЛ ДУАТОМ ОТ ГЛАЗ ТЕХ КТО ВЗБИРАЛСЯ ПО ТРОПЕ С ЗАПАДА ТЕПЕРЬ ЭТИ ОГНИ ОТРАЖАЯСЬ В ЗАСТЫВШЕЙ ПОВЕРХНОСТИ СКАЛ КАЗАЛОСЬ ОКРАШИВАЛИ ИХ В ЦВЕТ КРОВИ В ЭТОМ УЖАСНОМ СВЕТЕ СЭМ СТОЯЛ МАЛЕНЬКИЙ ПОТОМУ ЧТО ПОСМОТРЕВ НАЛЕВО ОН УВИДЕЛ БАШНЮ КИРИТ УНГОЛА ВО ВСЕЙ ЕЕ СИЛЕ РОГ БАШНИ КОТОРЫЙ ОН ВИДЕЛ С ДРУГОЙ СТОРОНЫ БЫЛ ВЕРШИНОЙ ЭТОЙ БАШНИ ЕЕ ВОСТОЧНАЯ СТОРОНА ПОДНИМАЛАСЬ ТРЕМЯ БОЛЬШИМИ ЯРУСАМИ ИЗ ЩЕЛИ В ГОРНОЙ СТЕНЕ ДАЛЕКО ВНИЗУ ЗАДНЕЙ СТОРОНОЙ БАШНЯ БЫЛА ОБРАЩЕНА К БОЛЬШОМУ УТЕСУ И СОЕДИНЯЛАСЬ С НИМ ВЫСТУПАЮЩИМИ БАСТИОНАМИ ОДИН НАД ДРУГИМ УМЕНЬШАЮЩИМИСЯ К ВЕРХУ С КРУТЫМИ СТЕНАМИ СЛОЖЕННЫМИ ИЗ КАМНЯ И ВЫХОДЯЩИМИ НА СЕВЕРО ВОСТОК И ЮГО ЗАПАД У НИЖНЕГО ЯРУСА ДВУМЯ СОТНЯМИ ФУТОВ НИЖЕ ТОГО МЕСТА ГДЕ СТОЯЛ СЭМ СТЕНА С УКРЕПЛЕНИЯМИ ОКРУЖАЛА УЗКИЙ ДВОР ВОРОТА ДВОРА В ЮГО ВОСТОЧНОЙ СТЕНЕ ВЫХОДИЛИ НА ШИРОКУЮ ДОРОГУ ПРОХОДИВШУЮ ПО КРАЮ ПРОПАСТИ ЗАТЕМ ПОВОРАЧИВАВШУЮ НА ЮГ И УХОДЯЩУЮ ИЗВИВАЯСЬ ВНИЗ ВО ТЬМУ НА СОЕДИНЕНИЕ С ДОРОГОЙ ИДУЩЕЙ ИЗ ДОЛИНЫ МОРГУЛА ЗАТЕМ ДОРОГА ЧЕРЕЗ НЕРОВНОЕ УЩЕЛЬЕ УХОДИЛА В МОРГ АЙ В ДОЛИНУ ГОРГОРОТ И ДАЛЬШЕ В БАРАД ДУР УЗКАЯ ВЕРХНЯЯ ТРОПА НА КОТОРОЙ СТОЯЛ СЭМ БЫСТРО ПО ЛЕСТНИЦАМ И КРУТЫМ СПУСКАМ ОПУСКАЛАСЬ К ГЛАВНОЙ ДОРОГЕ ПОД ХМУРЫМИ СТЕНАМИ У ВХОДА В БАШНЮ И ВДРУГ СЭМ ПОНЯЛ ЧТО ЭТА КРЕПОСТЬ БЫЛА ПОСТРОЕНА НЕ ДЛЯ ЗАЩИТЫ МОРДОРА НО ДЛЯ ОБОРОНЫ ОТ МОРДОРА НА САМОМ ДЕЛЕ ЭТО БЫЛО СОЗДАНИЕ ДРЕВНЕГО ГОНДОРА ВОСТОЧНЫЙ ФОРПОСТ ОБОРОНЫ ИТИЛИЕНА ПОСТРОЕННЫЙ КОГДА ВСЛЕД ЗА ПОСЛЕДНИМ СОЮЗОМ ЛЮДИ ЗАПАДА ВНИМАТЕЛЬНО СЛЕДИЛИ ЗА ЗЛОЙ ЗЕМЛЕЙ САУРОНА ГДЕ ПРОДОЛЖАЛИ ЖИТЬ ЕГО СОЗДАНИЯ НО КАК БЫЛО И С КАРНБОТОМ И КАРНОСТОМ БАШНЯМИ ЗУБОВ ТАК И ЗДЕСЬ БДИТЕЛЬНОСТЬ ОСЛАБЛА И ПРЕДАТЕЛЬСТВО ОТДАЛО ЭТУ БАШНЮ ГЛАВЕ ДУХОВ КОЛЬЦА И ТЕПЕРЬ ДОЛГИЕ ГОДЫ ЕЕ УДЕРЖИВАЛИ ЗЛЫЕ СУЩЕСТВА ПОСЛЕ СВОЕГО ВОЗВРАЩЕНИЯ В МОРДОР САУРОН НАШЕЛ ЕЕ ПОЛЕЗНОЙ У НЕГО БЫЛО МАЛО СЛУГ НО МНОГО РАБОВ КОТОРЫХ НУЖНО БЫЛО ДЕРЖАТЬ В СТРАХЕ И ГЛАВНОЙ ЕГО ЦЕЛЬЮ КАК И В СТАРИНУ БЫЛО ПРЕДОТВРАТИТЬ БЕГСТВО ИЗ МОРДОРА ХОТЯ ЕСЛИ БЫ ПРОТИВНИК ОКАЗАЛСЯ НАСТОЛЬКО БЕЗРАССУДЕН ЧТО ПОПЫТАЛСЯ БЫ ТАЙНО ПРОНИКНУТЬ В ЭТУ ЗЕМЛЮ БАШНЯ ПОСЛУЖИЛА БЫ НЕПРЕОДОЛИМОЙ ПРЕГРАДОЙ ДЛЯ ТЕХ КТО ОБМАНУЛ БДИТЕЛЬНОСТЬ МОРГУЛА И ШЕЛОБ ТОЛЬКО ТЕПЕРЬ СЭМ ПОНЯЛ ВСЮ БЕЗНАДЕЖНОСТЬ ПОПЫТКИ СПУСТИТЬСЯ ВНИЗ НА ВИДУ У МНОЖЕСТВА ОКОН И БДИТЕЛЬНЫХ ВОРОТ И ДАЖЕ ЕСЛИ БЫ ОН ПРОДЕЛАЛ ЭТО ВСЕ РАВНО ОН НЕ УШЕЛ БЫ ДАЛЕКО ПО ХОРОШО ОХРАНЯЕМОЙ ДОРОГЕ ДАЖЕ ЧЕРНЫЕ ТЕНИ ЗАЛЕГШИЕ ГЛУБОКО ТАМ КУДА НЕ ДОСТИГАЛО КРАСНОЕ ЗАРЕВО НЕ МОГЛИ БЫ СПРЯТАТЬ ЕГО ОТ ВИДЯЩИХ В ТЕМНОТЕ ОРКОВ НО ХОТЯ СПУСК ПРЕДСТАВЛЯЛСЯ ОТЧАЯННЫМ И БЕЗНАДЕЖНЫМ ЕГО ЗАДАЧА БЫЛА ГОРАЗДО ТРУДНЕЕ НЕ БЕЖАТЬ И СКРЫВАТЬСЯ НО ВОЙТИ В ВОРОТА В ОДИНОЧЕСТВЕ МЫСЛИ ЕГО ОБРАТИЛИСЬ К КОЛЬЦУ НО В НИХ НЕ БЫЛО УСПОКОЕНИЯ ТОЛЬКО УЖАС И ОПАСНОСТЬ КАК ТОЛЬКО ОН ОКАЗАЛСЯ НА ВИДУ У ГОРЫ ОГНЯ СВЕРКАВШЕЙ ДАЛЕКО ВПЕРЕДИ ОН ПОНЯЛ ЧТО НОША ЕГО ИЗМЕНИЛАСЬ ОКАЗАВШИСЬ ВБЛИЗИ ОТ ОГРОМНЫХ ПЕЧЕЙ ГДЕ В ГЛУБОКОЙ ДРЕВНОСТИ ОНО БЫЛО ВЫКОВАНО КОЛЬЦО ПРИОБРЕЛО ОГРОМНУЮ СИЛУ СТАЛО БОЛЕЕ СВИРЕПЫМ И НЕПОКОРНЫМ ПОСЛУШНЫМ ЛИШЬ МОГУЧЕЙ ВОЛЕ ХОТЯ СЭМ НЕ НАДЕЛ КОЛЬЦО ОНО ВИСЕЛО НА ЦЕПИ У НЕГО НА ШЕЕ ОН СТОЯ ЗДЕСЬ ЧУВСТВОВАЛ КАК ОНО УВЕЛИЧИВАЕТСЯ РАСШИРЯЕТСЯ ЗАКУТЫВАЯ В ОБШИРНУЮ ТЕНЬ САМОГО СЕБЯ ЗЛОВЕЩАЯ УГРОЗА ВСТАВАЛА НАД СТЕНАМИ МОРДОРА ОН ЗНАЛ ЧТО ТЕПЕРЬ ПЕРЕД НИМ ЛИШЬ ДВА ПУТИ ВОЗДЕРЖАТЬСЯ ОТ ИСПОЛЬЗОВАНИЯ КОЛЬЦА ХОТЯ ОНО БУДЕТ МУЧИТЕЛЬНО ИСКУШАТЬ ЕГО ИЛИ ОБЪЯВИТЬ ЕГО СВОИМ БРОСИВ ВЫЗОВ СИЛЕ ЧТО СИДИТ В ТЕМНОЙ КРЕПОСТИ ЗА ДОЛИНОЙ ТЕНЕЙ КОЛЬЦО ИСКУШАЛО ЕГО ПОДТАЧИВАЯ ЕГО ВОЛЮ И РАЗУМ

*Составной ключ:*

ЖАМЦЮВТЮПЩПОПАТКЫЛТГГЦШОХХПУЫС

*Протокол анализа:*

Индекс соответствия данного текста равен 0.0171, следовательно, необходимо воспользоваться подходом Ф. Казиски. Период равный 30 имеет наибольший вес, который равен 31. Возьмём ключ размером 30 символов. Далее для каждой группы заменяем наиболее часто встречающийся символ на пробел. В итоге мы получили ключ и расшифрованный текст. Далее найдём первичные ключи.

*Поиск первичных ключей*.

Скорее всего мы имеем слова размером 5 и 6 букв. Составим необходимые уравнения в соответствии с составным ключом.

K11+K21=6 K12+K25=27

K12+K22=0 K13+K26=11

K13+K23=0 K14+K21=18

**K14+K24=22** K15+K22=3

K15+K25=30 K11+K23=3

K11+K26=2 **K12+K24=22**

K12+K21=18 K13+K25=24

K13+K22=30 K14+K26=14

K14+K23=15 K15+K21=21

K15+K24=25 K11+K22=21

K11+K25=15 K12+K23=15

K12+K25=14 K13+K24=19

K13+K21=15 K14+K25=27

K14+K22=0 K15+K26=17

K15+K23=18

K11+K24=10

Как видно из выделенных уравнений, K12=K14. В русском языке не много букв можно подставить на эти позиции. Перебирая по алфавиту, выбрав букву «О», мы нашли второе слово (К21…К26):

К21=18-14=4(«Д»)

К22=33-14=19(«У»)

К23=15-14=1(«Б»)

К24=22-14=8(«И»)

К25=27-14=13(«Н»)

К26=14-14=0(«А»)

Получили слово «ДУБИНА», подставим готовые значения и найдём второе слово «ВОЛОС».

1. **Вывод**

В ходе выполнения лабораторной работы был изучен метод дешифрации текста, зашифрованного многопетлевым шрифтом. Был получен и расшифрован составной ключ, в результате чего были получены первичные ключи.