Университет ИТМО

Факультет программной инженерии и компьютерной техники

Кафедра вычислительной техники

Лабораторная работа № 3 по дисциплине ”Методы и средства защиты компьютерной информации”

Вариант 12

Выполнил:

Чебыкин И. Б.

Группа: P3401

Проверяющий: Ожиганов А. А.

Санкт-Петербург, 2018

Цель работы.

Дешифровать криптограмму, зашифрованную многопетлевым шифром.

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

Выполнение

Криптограмма

КГЖОЬХМСЮЬНЧЬЧЮВПОЧШЖУЕШОРДВЮХСЬЗРЧЭ ИПЩИЗЬЯРПЭБРЯ ТК ЯПАВДЫЬ ЛО ИГХДЭША ЗАКЗЯ
РЩЩДЦАКЫЬВЮАЮЙУБЙЦШЩСАЯПЮАЪАТРАГЖЖЫЖВМЛПКДЬОЦИЯМУФЮУА ХЮВВЯЕЭИ
КЗОЪЙУЭЬХЖУЪЙФЬШГЪФВЫЩЕИЫФИЭФЪФМЗННЗНВССЕ
ХЭУЗШЪЮИОАВЙЬЦФЬПИШЧЛЬПЩРНКБРЬЬЪБИФЪАФЮЕЫГВЧЯШАДЬЙНЬРРКЧХ
АЫСЗХЮЕЬХНАЗПЦООКФБДТШБЯВВСЫБГТРПЫЦ ВДТДПТОНШМОККЖАЪ
ЦЮЫПЗНЭПЗВАЪБЫГХБЭНБКККЗКЦЛПЪ РЕНВНПЗВЯАЭЮДВЩО ЗЕББЗЕЩЯС
ЮТФЪАЗЭЯЕАЪКЗЕАМРРЬШГБФШЫТДХПВДМВНЬБОЬЖШЫЗВЮ ЕЦДЩЬЩЖТЪТЭОДУЙАЪ
ШФЬУХГМФТФЭЕДШБЩВЯМЧХХЬБГТТ ЗЕЬШКДЧЦЫЯЩЩККПЯЩБСНЭЪШУДАЪЮЙСДХЩН
ФОЭИУТЕБЗАРПАБХЭО ТУНЮЛЫЖЬЙШДХАШГНК ЦГЯБААШПЦЪФИЩГСЮРСЫДЪЮСВЮН ЬЭЩЬ
ТХДПЕИТЩЯЪОГХТАВПЩЧЭЬТЙИРШВН ЖВБУАШЗЭЪВЕГЕЕЭФХТНШРУЬКШБ МВФХЯЦ
ВХЩЫЬНЖГЧЖЫОЗЙУКЙРЪГГЬФТЯБЕЦЦЫЗФЬХГЬЪВСЧИЧЧЩНТГЩБУТПЯЩЛ ЕПЬГ ЮИЬЧГТАНЕЗУУИШЮД
ЛВ ФЕЫЩЛЩРЙХДЫДЪМ Ф ЧЛЗРШЦВОФЧРУЛХЦХЭСЫЦЬАГЗМСМЕХЮЬЙУЬН ДРЧЧИХИ БЕЬЗШЫИФЮПЙ
СКНЦЪЯИ ЕБЮЯЦЭЦПЖГЕГЛГВВЮКЭКДШБЛЖРМЕГ
ЮШНЯИЭЖСЯГЬГЧБТЯВПКШЙЦЬЯЯИФАББЕОТЮЩЕЙЖЛЙГЭЪПК ОККЙИЛБА ЮАПЪЭИЪЩНИЮ ЬЧШСФЭЪ
ЫЯИЕСЯСЖ РАВИИПЬВМЦИЙГФФПТЪЕЭЧКЩОШЕАПЬЩЛДНПЬГ ЮИЫЖЪЯЯЛЪНБЬЧИЩМЯ
ПСЩБТТЮДИЭЦЙГАФЙАЛЙДШККУЪЯМЭ ПВИДЦЬМВТЗКЫФЖЫООЕЗРМ ЩЬНСРПАУ ЦЦПЙС
ЮЙЙАФЯФМЭХЖЬХЩХН ЦКЫБЪХЩХЩТЙВЫНУФП ВЧУЬИВЙЬЗТРПЮШЗУОФФВЯАЭЮДПЦО ЗЕБЬЧИЩМЕЕПХ
НТФЮКНЙШНЕ ЪМТЮЯКЭЧЗЫСГИАПЯЩМВЦТБЪЫДМЙОЪШОЕМДЬККЙЦЛ ЭЭК
ВТЛЫЪКЬБДЫДЪМАЮБДХЭТШТЪВХЫЮУБУШРЖИАХГЖЕЦЪЭЭ МПБКЩПРЬФ
ВДЛЭИОЩУАШКЖХКХНЭЖКЫБТАХЪВХЫРДЦТКПЬИИЩМГХФПОАЭХЧЭХАОЯВФШБФЕЫЕПЭГВЫОИТЪМ
ПЗУХДЗЪЛКИФЭРДХЛНЭФВ
ЫМВЕЕЯКЫЧШНБШЮЮМОЕБЛСЪАЧББПГЭИЙГФЭЭОИНЙЬШЩШГАЧЫХАЗУЖПЬСДВКДЧДНЦБ
ХЛБФЩПЯМЪЦФБНГЦСБЩАЯЬВШДНЬВЭДЪКМЮЬДНБРОУЖШОФМВЮЫЗГБЭЩЧЭЬКЫВИЫСЛИФСХГ ДЗ МНЙШК
ИЖПЭЭГНЫККЖЪЯПВЫШЕВЭЦЩЩФНЦЙЙЪЭЯ ЬЧИЫКПЕЯИ ЕШЫБГТЦЭЩРЬМДИШ
МЮЛДНЧЭЪФРАУЩЭШКЗАНПКТЙ КДИЖПЧВЧЧЩЯИИЩШЕЮПТУЛШШКОВРЦЗЬЙХБОЛДНКГХЩЬЗ ЯРЪБ
ТМХДСЫЖААВХЪЭЭЕТУЬЧЖА БВБРЯВТРДЩФКГЖЙАЕЯСЕЭДНБТЖУНЕФБОЪ ЮЦ
МНЙЫЬНЦЫТЪЛДУОКНШЭМОШЮФЖЖ ЦХЩЕЦЪБЛЮХШЭЭЖГЭШЗЙВНЛЪБШЭЪУЗВ
ВЯГНКЕЩХОФЭИЩЬЪЖЬЫКВПЭЩЪФВЫЗВМЗМЬДБННЭ ДЩНЦЪЦМНХОПЬЛДЦ
ББЫЕПМИЯЫТЛЧТЛМЦЭСЯРЗААЮИЦЦПЭСМИАЬЗЕЯСЮЧУОМЦДЮЪЕФШПА
АЬЮЙПЖЫЙИТЪМЧБЭНКЮШЖХЮТФТПА ЯЗШАВМЗКЖЭЖХНЭЪДЬОЦГЦСИЪПШШ ЫЗЬБУЙШКЯЕФПФИ
ЬУЫЗАРОРХТФЬЭАСП ЛВВДЫЕЕ ЗВИЧНЗЖЦВРЯФЭХХХХИЫФИЫЮЬ ЭДФЩЕЭДШЭЯАЮ НЭОПЮИДЦ
ФИЫЖИОРХКАЭЭЗЫКЧЮЪРКЭЩП
ВВЗШЩИЮЕККШФЮЭЭИЧЫЭЭЖЭЯИФЭХЧИЧЦТЪРГЫИЫЪШНБТЗЛБЪЙПЯВФМББЪХЦАЛСТВКАЧЛ УЕРККДЗЙЬ

БВХПЬЪЯЦУМЪАЫЬИ НТФЭ ДШБР ЭДРЭЫЮУЬАЛРЛСАХМЙЮЩНМЦЭККДПШВДМБКДУЗШМ
ЩФЮГДРЧКТЪШЭДТЭШЮУ ЧАХК ЮЦТЯЪАЖЖГМФХУВАДУЬПЩЭЪС ЮТУВТХРГСИЫТЫЗВЮ ЕЦДУИНЕЮН
ДЮАДВСЗШАДГЕЭАЙФЪЭ ТОКЙРВЦЛ БШЪБЮЧИПЖИЫДМЙЩВППКД ФЬЧЛВЫ ЭПАУЙШШТФШЫЬБЫПХРЭ ЧЦЦЧ
ЕСЯЕЪПЯБЛДЫЯХВКГЬЗ Д ОМЕТЙОХЖРЦТВПАУМУТШЕЛЫБЧМВУЩЧЭЪЕПДФЛРОЕЖ
ЮЦВЙЫПЫЮЖГЬЮИЪМЯЮЪТЩЬТЩЫЗЕФБР
ЪЦШОАРЦЫЬЛКЛИЧЭЯЕККТЕСЛИФУЮАЩДЗЯЗВОАДСЭФЩПНЙУННТАЪЯСБХУУВТЙ
ЯЗАЗЬОЫДКЫШАДУЬХЮХНВВЫЛАХЬЗАЗЕАЗНЕ ЮМ ИКЛЛХРБРР
АХЗЮИЯЗФДБЫДМЙЬЗЧАЛЪДУЬОЮБСЯБЪЮЭЪЧУОЩНАЕКМ БНОДШДЬЛРЕЯИ ЧП
ФЛЭРАСЛРХЮЬПАНЩЮМДТЭЩЮХ ТРПТУИЧХЮВВГЭЬЭЭЕГЧОВКШЙВНРЙО ЫХЧВЬЗСФОЙХЯМЭФЭП
ДУКЖИВЯИ ШЫЮЕЫДГПКЦКХНЫБХЧЧЙ
ДЫЧЙФЩЛИФУЫФБЭИЬБВАБПЫДЪМАВЗФРЗЦЙМЯПВАЪБКШНПКГЗГИОЧБНЕЮЙАКЛЦЭБНБ
ОБПЪХЦЪЙЦЯХЩНЕШЫОБЭРЛЬЫВА ИБРПБСЫАРДГМСЬЙЙФЬФПВВЫКККОЦБ БХФФЭ
ЦПЫЮЖХЯВЦЖМЩНШЦШКСШСПМЭХЩУ ЭИБЯУГВКМВХПОМЭЧЦЪШЩРДЩЪПЕЩЙЮЖЫКБЫЭЭЫЩЪШБЫЧЫРМТЖУЫ
БЮПБМДЫФЪВАЩКЫДХЧЭКЭЫКЯВЪЩКИФШПБЗТЩПЗФНЦОЕШАМЩРЗКШБСШГЧЕ
ПЧФЪЦШРЖЛСИЬЮЧШНЪЕННИЬКЗЦПЕЩШПАЫГЪВИГЩОДРЧЧЫШОБДХМИЙЮНЙФР
ВЫЗЪЪХГАНЪЧМХЯЛБНФЬКЩЬЯПХ БЬБУХАГЛРХЯЙИЕЯПК ОКДЭША ЗАРДУМВЫФЖСЫДК ЬХППИИГКПЯЮВТ
ЭП ЖДАКЮЮФНШПЫЕБХО
ИФЕСРЫСКИФЪРЮЪБЦЦЪУЦХЛЙЧЕТЬЮГДУЬКЖЬНСЖОЬУКУПФБУЬЫИЦГФУФОЙУХКСШТ-
НРРСЮЭЪЯИЫЗКАББЖУБЫТЛЧПЫБЩКМЮНЕБТФЪГЗЪЙИК
ДЗЧЯ ЪЮОКЬОКЖЭЯИФБХУВТМ МЖГЫЬЮТЕЯП ВГЦДЗЖВПЯЩКПДТЫЙРЬЫГЫНЪЧЕЫО ИКФЬЖИЯРТРНПЮИ
ХКЯВГХЛАПЭТО ЧПЫККЩУЪХФСШЕЭУЭПИСЮЖЪ КФДЬШЗГЦДЗДСРКЭ
ВТЛОЗШЩТЛГЯЙНЭЭБЬЧЧЛЕХУЦЯАШХЭЕХТЧХЛОЩЕКЮИЯХФЭЬКШДТАЮРКЭХПЬЪБЦЫХФЕЮБЫ
ФТЗВЧЖЩЗНЮРСЕАЭКИЪЫЗАГУЦЗЙЦМФЫЯАШТУГИОЩИ ЕЮТЩМГТРШВЮАЭМЙРМРШВЕКЛЦШФНРВФР
ЪЧИПИСЫБЭЯ
ЕЯЯЮВГЧЬОЮЬДЗБКДУЯАШЮЭВЬХГЬЧБХЫЕЧЗКНЪЖАННППЭФЪБЦЫЯХЫЖЙЬЗУСПЭИД-
ММЦЕЦООЪЧФФЪФЫЗЯЕЬАЭЫЪВЦЬЮЧЗЛАРДРОЕЖ
ЮЦВЙЗЯЗООМДЖЧБНЩЛДКАЬМЖЬВОФЮЦЬЯУНЬЗИЫВЭВДХГФК ККЯЗРВ
БФЪВГЛУХБКНЙЯЬЭЗЭРПБТДОАНШЫНМЭААФКАФПЫЮЖХУОЫХЦО
ЧЦРМНЭЩМЕФЬРГМУЗТФТГЖЭЖИУМЧДЧИЩНЧАВ ЛУПХМ ТЧ
БШЛЦИЦЪХКЗЕАДЬЬЧЩЬНЧЯЮЩУВТЧЮЯШЬАЬЮЧЯХФ ЧЗКНКЖОЯЧХАБПЪАЪЪЗОЙШФЬЦЕЛОЛЙДЛОИДСМАФУ
ЬЮАШЛЯЕЬХЮЬДЩНОДЭРРЙЦЬЯЯГДЮЬТЪГНЫХФЙШБНТФХОЛМУЭЫЩФРЖАФЪЮ ЖЕХШКХЬБДЫЖВС
ЗШПУЯИГСЯНХПАБМ ЖДЩХЬМЭИЕЯМЩЭИЕЧКФЛРЙИЪТВУЙЮИЭЩОГ ЯГЬХВЧЕЧБЭКСШТ НЩКПХХЮЗ
ЪКЛЦЮЙЙХЪООЧШБЭЩКЩДМФ ЮМВ ИПЬВУЗЭЭЭФЪПНБУЧЯЦЮЮ ЕШЫУЬНУЮЩРАБЙЙЫВМЫЮЗПЩИКЖЦМ ЗЪ
ФВ ВПЫЮАКЭЖЧЭФОЗ КНЭЗЕСЯПХ ЮИИЧНПРХЙЧЧЫЗЗЧЭ ЕЙУОГШЯОЕДРЕЬ
ЬЗЭЪВЗЫННЭФСЬВЖХКЮВГРДЩЪПЗЬКАТПИГЛГСЙЬФДЪВЖЕЦЬТЖЬДСХЬШУЙАЗОКРЙЯЬЮЕЩТО
ЕМЧПАЩЦЛОЮПЫЬТОЗЫЯРГШЧЗ ФПЭБЕЗЩМЦКСЛИ

Открытый текст

ПОКУДА ВАДИМ ПЕТРОВИЧ ЛЕЖАЛ В ХАРЬКОВСКОМ ГОСПИТАЛЕ ВРЕМЕНИ ДЛЯ ВСЯКИХ
РАЗМЫШЛЕНИЙ БЫЛО ДОСТАТОЧНО ИТАК ОН ОКАЗАЛСЯ ПО ЭТУ СТОРОНУ ОГНЕННОЙ ГРАНИЦЫ
ЭТОТ НОВЫЙ МИР БЫЛ ВНЕШНЕ НЕПРИВЛЕКАТЕЛЕН НЕТОПЛЕННАЯ ПАЛАТА ЗА ОКНАМИ ПАДАЮЩИЙ
МОКРЫЙ СНЕГ СКВЕРНАЯ ЕДВА СЕРЫЙ СУПЧИК С ВОБЛОЙ И БУДНИЧНЫЕ РАЗГОВОРЫ БОЛЬНЫХ О
ЕДЕ МАХОРКЕ О ТЕМПЕРАТУРЕ О ГЛАВНОМ ВРАЧЕ НИ СЛОВА О НЕВЕДОМОМ БУДУЩЕМ КУДА
УСТРЕМИЛАСЬ РОССИЯ О СОБЫТИЯХ ПОТРЯСАЮЩИХ ЕЕ О НЕСКОНЧАЕМОЙ КРОВАВОЙ БОРЬБЕ

УЧАСТНИКИ КОТОРОЙ ЭТИ БОЛЬНЫЕ И РАНЕНЫЕ ЛЮДИ С ОБРИТЫМИ ГОЛОВАМИ В БАЙКОВЫХ НЕСВЕЖИХ ХАЛАТАХ ТО СПАЛИ ЦЕЛЫМИ ДНЯМИ ТО ТУТ ЖЕ НА КОЙКЕ ИГРАЛИ В САМОДЕЛЬНЫЕ ШАШКИ ТО КТО НИБУДЬ ВПОЛГОЛОСА ЗАВОДИЛ ТОСКЛИВУЮ ПЕСНЮ ВАДИМА ПЕТРОВИЧА НЕ ЧУРАЛИСЬ НО И НЕ СЧИТАЛИ ЕГО ЗА СВОЕГО А ЕМУ ВПОРУ БЫЛО РАЗГОВАРИВАТЬ С САМИМ СОБОЙ СТОЛЬКО НАКОПИЛОСЬ У НЕГО НЕПРОДУМАННОГО И НЕРЕШЕННОГО И СТОЛЬКО ВОСПОМИНАНИЙ ОБРЫВАЛОСЬ КАК КНИГА ГДЕ ВЫРВАНА СТРАНИЦА В САМОМ ЗАХВАТЫВАЮЩЕМ МЕСТЕ ВАДИМ ПЕТРОВИЧ ПРИНЯЛ БЕЗ КОЛЕБАНИЙ ЭТОТ НОВЫЙ МИР ПОТОМУ ЧТО ЭТО СОВЕРШАЛОСЬ С ЕГО РОДИНОЙ ТЕПЕРЬ НАДО БЫЛО ВСЕ ПОНЯТЬ ВСЕ ОСМЫСЛИТЬ ОДНАЖДЫ ГЛАВНЫЙ ВРАЧ ПРИНЕС ЕМУ МОСКОВСКИЕ ГАЗЕТЫ ВАДИМ ПЕТРОВИЧ ПРОЧЕЛ ИХ СОВСЕМ ИНЫМИ ГЛАЗАМИ НЕ ТАК КАК БЫВАЛО ЗАРАНЕЕ ЗЛОБНО ИЗДЕВАЯСЬ РУССКАЯ РЕВОЛЮЦИЯ ПЕРЕКИДЫВАЛАСЬ В ВЕНГРИЮ В ГЕРМАНИЮ В ИТАЛИЮ ГАЗЕТНЫЕ СТРОКИ БЫЛИ НАСЫЩЕНЫ ДЕРЗОСТЬЮ УВЕРЕННОСТЬЮ ОПТИМИЗМОМ РОССИЯ РАЗДАВЛЕННАЯ ВОЙНОЙ РАЗДИРАЕМАЯ МЕЖДОУСОБИЦЕЙ ЗАРАНЕЕ ПОДЕЛЕННАЯ МЕЖДУ ВЕЛИКИМИ ДЕРЖАВАМИ БЕРЕТ РУКОВОДСТВО МИРОВОЙ ПОЛИТИКОЙ СТАНОВИТСЯ ГРОЗНОЙ СИЛОЙ ОН НАЧИНАЛ ПОНИМАТЬ БУДНИЧНОЕ СПОКОЙСТВИЕ ТОВАРИЩЕЙ В СЕРЫХ ХАЛАТАХ ОНИ ЗНАЛИ КАКОЕ ДЕЛО СДЕЛАНО ОНИ ПОРАБОТАЛИ ИХ СПОКОЙСТВИЕ ВЕКОВОЕ ТЯЖЕЛОРУКОЕ ТЯЖЕЛОНОГОЕ МНОГОДУМНОЕ ВЫДЕРЖАЛО ПЯТЬ СТОЛЕТИЙ А УЖ ГОСПОДИ ЧЕГО ТОЛЬКО НЕ БЫЛО СТРАННАЯ И ОСОБЕННАЯ ИСТОРИЯ РУССКОГО НАРОДА РУССКОГО ГОСУДАРСТВА ОГРОМНЫЕ И НЕОФОРМЛЕННЫЕ ИДЕИ БРОДЯТ В НЕМ ИЗ СТОЛЕТИЯ В СТОЛЕТИЕ ИДЕИ МИРОВОГО ВЕЛИЧИЯ И ПРАВДИВОЙ ЖИЗНИ ОСУЩЕСТВЛЯЮТСЯ НЕБЫВАЛЫЕ И ДЕРЗКИЕ НАЧИНАНИЯ КОТОРЫЕ СМУЩАЮТ ЕВРОПЕЙСКИЙ МИР И ЕВРОПА СО СТРАХОМ И НЕГОДОВАНИЕМ ВГЛЯДЫВАЕТСЯ В ЭТО ВОСТОЧНОЕ ЧУДИЩЕ И СЛАБОЕ И МОГУЧЕЕ НИЩЕЕ И НЕИЗМЕРИМО БОГАТОЕ РОЖДАЮЩЕЕ ИЗ ТЕМНЫХ НЕДР СВОИХ ЦЕЛЫЕ ЗАРЕВА ВСЕЧЕЛОВЕЧЕСКИХ ИДЕЙ И ЗАМЫСЛОВ И НАКОНЕЦ РОССИЯ ИМЕННО РОССИЯ ИЗБИРАЕТ НОВЫЙ НИКЕМ НИКОГДА НЕ ПРОБОВАННЫЙ ПУТЬ И С ПЕРВЫХ ЖЕ ШАГОВ СЛЫШНА ЕЕ ПОСТУПЬ ПО МИРУ ПОНЯТНО ЧТО С ТАКИМИ МЫСЛЯМИ ВАДИМУ ПЕТРОВИЧУ БЫЛО ВСЕ РАВНО КАКИЕ ТАМ ГРЯЗНЫЕ РУЧЬИ ЗА ОКНАМИ ГОНЯТ ПО УЛИЦЕ МАРТОВСКИЙ СНЕГ И БРЕДЕТ УГРЮМЫЙ И НЕДОВОЛЬНЫЙ СОВЕТСКИЙ СЛУЖАЩИЙ С МЕШКОМ ДЛЯ ПРОДУКТОВ И ЖЕСТЯНКОЙ ДЛЯ КЕРОСИНА ЗА СПИНОЙ В РАСКИСШИХ БАШМАКАХ ЗАСЕДАТЬ В ОДНОЙ ИЗ БЕСЧИСЛЕННЫХ КОЛЛЕГИЙ БЫЛО ВСЕ РАВНО КАКОЙ ГЛОТАТЬ СУП С КАКИМИ РЫБЬИМИ ГЛАЗКАМИ ЕМУ НЕ ТЕРПЕЛОСЬ ПОСКОРЕЕ САМОМУ НАЧАТЬ ПОДСОБЛЯТЬ ВОКРУГ ЭТОГО ДЕЛА УКРАИНА ОЧИЩАЛАСЬ ОТ ПЕТЛЮРОВЦЕВ НЕДАВНО БЫЛ ВЗЯТ КРАСНОЙ АРМИЕЙ ЕКАТЕРИНОСЛАВ ПЕТЛЮРА ЕЩЕ ЦЕПЛЯЛСЯ ЗА БЕЛУЮ ЦЕРКОВЬ НО ОТТУДА ЕГО НАКОНЕЦ ВЫБИЛИ И ОН С ОСТАТКАМ КУРЕНЕЙ УШЕЛ ЗА ГРАНИЦУ В ГАЛИЦИЮ ВПЕРЕДИ НАСТУПАЮЩИХ ВОЙСК КРАСНОЙ АРМИИ КАТИЛСЯ ШИРОКИЙ ВАЛ ПАРТИЗАНСКИХ ВОССТАНИЙ ИХ РАЗМАХ ТРУДНО ПОДДАВАЛСЯ УЧЕТУ И РУКОВОДСТВУ ОНИ ВСПЫХИВАЛИ КАК ПОЖАРЫ ПО СЕЛАМ И ВОЛОСТЯМ РАЗДИРАЕМЫМ ЖЕСТОКОЙ БОРЬБОЙ МАЛОЗЕМЕЛЬНОГО КРЕСТЬЯНСТВА С КРЕПКИМ КУЛАЧЕСТВОМ И ТЕ И ДРУГИЕ ВЫСТАВЛЯЛИ ОТРЯДЫ СШИБАВШИЕСЯ СО ВСЕЙ ЯРОСТЬЮ КОННЫЕ И ПЕШИЕ В КРОВАВЫХ БИТВАХ ПОВСЮДУ ШНЫРЯЛИ МАСКИРУЯСЬ И ПРОВОЦИРУЯ ТАЙНЫЕ АГЕНТЫ ПЕТЛЮРОВСКИЕ ДЕНИКИНСКИЕ И ПОЛЬСКИЕ И ЕЩЕ БОЛЕЕ ТЕМНЫХ И СКРЫТНЫХ ОРГАНИЗАЦИЙ СОВЕТСКАЯ ВЛАСТЬ БЫЛА ПО ГОРОДАМ ДА ПО МАГИСТРАЛЯМ ЖЕЛЕЗНЫХ ДОРОГ А ЗА НИМИ В СТОРОНЫ НА ПОЛЕТ СНАРЯДА С БРОНЕПОЕЗДА БУШЕВАЛА ВОЙНА ВАДИМ ПЕТРОВИЧ ПОЛУЧИЛ НАКОНЕЦ ДОЛГО ОЖИДАЕМОЕ НАЗНАЧЕНИЕ В ШТАБ КУРСАНТСКОЙ БРИГАДЫ ГДЕ КОМИССАРОМ БЫЛ ЧУГАЙ В СЕРЕДИНЕ МАРТА ВЫПИСАЛСЯ ИЗ ГОСПИТАЛЯ ЕЩЕ ПРИХРАМЫВАЮЩИЙ С ПАЛОЧКОЙ И ПОЕХАЛ В КИЕВ В СВОЮ ЧАСТЬ ОТКОЛОВШАЯСЯ ОТ АТАМАНА ГРИГОРЬЕВА БАНДА ЗЕЛЕНОГО ГРОМЯ СЕЛЬСОВЕТЫ И ОХОТЯСЬ ЗА КОММУНИСТАМИ ПОДСКАКИВАЛА НА СОТНЯХ ТАЧАНОК К САМОМУ КИЕВУ ПЛАН ЛИКВИДАЦИИ ЭТОЙ БАНДЫ БЫЛ РАЗРАБОТАН С УЧАСТИЕМ РОЩИНА В ШТАБЕ НАРКОМВОЕНА СИЛ БЫЛО НЕМНОГО НАРКОМВОЕН УКРАИНЫ ВЫЕХАЛ ИЗ КИЕВА НА ПАРОХОДЕ ЧТОБЫ РУКОВОДИТЬ ОПЕРАЦИЕЙ НА

МЕСТЕ ДНЕПР БЫЛ ЕЩЕ ШИРОК ПАРОХОД ШЛЕПАЛ КОЛЕСАМИ ПО ЯСНОЙ ВОДЕ ВОЗМУЩАЕМОЙ
ЛИШЬ ЛЕНИВЫМИ ВОДОВОРОТАМИ

Составной ключ

ЬЦЭЬШХНПЮШЕЛЭИЩС АХРРФЫУИРЪГ

Краткий протокол криптоанализа

Сначала определяем период ключа с помощью методов ИС и Казиски.

В результате период равен 28.

Далее делаем замены в тексте согласно совпадению частот символов в группе с частотами русского языка, корректируем ошибки и получаем составной ключ.

Далее раскладываем его на первичные ключи.

Длина составного ключа равна 28 символам. Будем считать, что в шифре использовались 2 ключа. Тогда их длины могут равняться 4 и 7.

Пусть составной ключ $K = K_1K_2...K_{28}$

Первый первичный ключ $K_1 = K_{1,1} + K_{1,2} + ... + K_{1,4}$

Второй первичный ключ $K_2 = K_{2,1} + K_{2,2} + ... + K_{2,7}$

Составим уравнения, из которых сможем найти значения первичных ключей.

$K_{1,1} + K_{2,1} = 28$ “Ь”

$K_{1,2} + K_{2,2} = 22$ “Ц”

$K_{1,3} + K_{2,3} = 29$ “Э”

$K_{1,4} + K_{2,4} = 28$ “Ь”

$K_{1,1} + K_{2,5} = 24$ “Ш”

$K_{1,2} + K_{2,6} = 21$ “Х”

$K_{1,3} + K_{2,7} = 13$ “Н”

$K_{1,4} + K_{2,1} = 15$ “П”

$K_{1,1} + K_{2,2} = 30$ “Ю”

$K_{1,2} + K_{2,3} = 24$ “Ш”

$K_{1,3} + K_{2,4} = 5$ “Е”

$K_{1,4} + K_{2,5} = 11$ “Л”

$K_{1,1} + K_{2,6} = 29$ “Э”

$K_{1,2} + K_{2,7} = 8$ “И”

$K_{1,3} + K_{2,1} = 25$ “Щ”

$K_{1,4} + K_{2,2} = 17$ “С”

$K_{1,1} + K_{2,3} = 32$ ” ”

$K_{1,2} + K_{2,4} = 0$ “А”

$K_{1,3} + K_{2,5} = 21$ “Х”

$K_{1,4} + K_{2,6} = 16$ “Р”

$K_{1,1} + K_{2,7} = 16$ “Р”

$K_{1,2} + K_{2,1} = 20$ “Ф”

$K_{1,3} + K_{2,2} = 27$ “Ы”

$K_{1,4} + K_{2,3} = 19$ “У”

$K_{1,1} + K_{2,4} = 8$ “И”

$K_{1,2} + K_{2,5} = 16$ “Р”

$K_{1,3} + K_{2,6} = 26$ “Ъ”

$K_{1,4} + K_{2,7} = 3$ “Г”

Имеем 11 неизвестных и 10 линейно независимых уравнений. Выразим все переменные через одну, например, через $K_{2,1}$.

$K_{1,1} = 28 - K_{2,1}$

$K_{1,2} = 20 - K_{2,1}$

$K_{1,3} = 25 - K_{2,1}$

$K_{1,4} = 15 - K_{2,1}$

Эта переменная является числовым эквивалентом символа русского алфавита и, следовательно, может принимать целочисленные значения от 0 до 31. Первичные ключи являются словами русского языка, поэтому, перебрав все возможные значения $K_{2,1}$, получим истинные значения первичных ключей.

Первичные ключи: «РИНГ» и «МОРЩИНА».