МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНО-ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ЮУрГГПУ»)

ФИЗИКО-МАТЕМАТИЧЕКИЙ ФАКУЛЬТЕТ

КАФЕДРА ИНФОРМАТИКИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И МЕТОДИКИ ОБУЧЕНИЯ ИНФОРМАТИКЕ

Изучение основ криптографии на уроках информатики в школе

Выпускная квалификационная работа
по направлению 44.03.05, Педагогическое образование (с двумя профилями подготовки)
Направленность программы бакалавриата

«Информатика. Математика»

Проверка на объем заимствований:
75 % авторского текста

Работа рекомендована к защите
рекомендована/не рекомендована
«11» мая 2017 г.
и.о. зав. кафедрой И, ИТ и МОИ
_____ Рузаков А.А.

Выполнил:
Студент группы ЗФ-513-111-5-1
Гачковский Виталий Валерьевич

Научный руководитель:
кандидат педагогических наук,
кафедры ИИТиМОИ
_____ Гилязева Наталья Вита

Челябинск
2017

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНО-ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ЮУрГГПУ»)

ФИЗИКО-МАТЕМАТИЧЕКИЙ ФАКУЛЬТЕТ

КАФЕДРА ИНФОРМАТИКИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И МЕТОДИКИ ОБУЧЕНИЯ ИНФОРМАТИКЕ

Изучение основ криптографии на уроках информатики в школе

Выпускная квалификационная работа
по направлению 44.03.05, Педагогическое образование (с двумя профилями подготовки)
Направленность программы бакалавриата

«Информатика. Математика»

Проверка на объем заимствований:
_____% авторского текста

Работа _____ к защите
рекомендована/не рекомендована

« ___ » _____ 20__ г.
и.о. зав. кафедрой И, ИТ и МОИ

_____ Рузаков А.А.

Выполнил:
Студент группы ЗФ-513-111-5-1
Гачковский Виталий Валерьевич

Научный руководитель:
кандидат педагогических наук, доцент кафедры ИИТиМОИ
_____ Гилязева Наталья Витальевна

Челябинск
2017

Оглавление

ВВЕДЕНИЕ

В современном обществе информация играет большую роль в различных сферах жизнедеятельности человека. Информация становится товаром, у которого есть автор, гарантии качества, цена. Информация может представлять коммерческую, личную, военную или государственную тайну, поэтому важным становится не только обработка постоянно возрастающих объемов информации, но и ее защита. Возможность несанкционированного использования информации возникает из-за ее уязвимости, что связано с незаконными действиями лиц, имеющих доступ к программным и информационным ресурсам вычислительных сетей. Данные, обрабатываемые с помощью электронных средств, должны быть защищены от несанкционированного доступа. Рассматриваемая проблема может быть решена с помощью шифрования информации, которое является одним из разделов криптографии.

Криптография позволяет обеспечить безопасность информации. В наше время использование криптографических методов получило широкое распространение в результате развития электронного обмена данными. Такой обмен данными широко используется в различных организациях и учреждениях. Для обеспечения защиты данных, передаваемых по сети и обладающих высокой секретностью, применяется шифрование сообщений. В настоящее время разработано множество алгоритмов защиты информации, основанных на применении различных схем и методов шифрования, однако такие алгоритмы понятны лишь узкому кругу специалистов в этой области.

Для понимания важности вопросов, связанных с защитой информации возникает необходимость введения в школьный курс информатики элементов криптографии. Проведение такого курса обеспечит для школьников понимание тем, связанных с ценностью информации и ее защитой, предоставит возможность учащимся познакомиться и практически

поработать с некоторыми алгоритмами шифрования, являющимися основой криптографии.

Данные положения определяют **цель исследования**: изучить литературу по проблеме исследования, разработать демонстрационную программу, иллюстрирующую работу некоторых алгоритмов шифрования, разработать элективный курс и методические рекомендации к нему.

Объектом исследования квалификационной работы является процесс обучения основам криптографической защиты информации в старших классах школы.

Предметом исследования является формирование навыков защиты информации на занятиях элективного курса «Основы криптографии».

В соответствии с целью работы были поставлены следующие **задачи**:

1. Изучить теоретические положения по проблеме исследования.
2. Разработать демонстрационную программу, иллюстрирующую некоторые алгоритмы шифрования информации.
3. Разработать и адаптировать школьный элективный курс по изучению криптографических основ защиты информации в школе для 10-11 классов.
4. Разработать программно-методическую поддержку элективного курса в виде электронного пособия.

Гипотеза: если включить в школьный курс вопросы, связанные с изучением криптографической защиты информации, то это обеспечит понимание учащимися важности вопросов защиты информации, а также сформирует стойкий интерес к серьезному обучению более сложных алгоритмов криптографии в будущем.

Для подтверждения этой гипотезы были использованы следующие **методы исследования**:

1. Анализ теоретических источников.
2. Наблюдение за реальным педагогическим процессом.

3. Анализ результатов тестирований и выполнений индивидуальных заданий.

Практическая значимость данной работы заключается в создании сайта, содержащего основные теоретические положения по данной теме, а также демонстрационной программы, иллюстрирующей некоторые алгоритмы шифрования информации.

ГЛАВА 1. КРИПТОГРАФИЯ С ДРЕВНЕЙШИХ ВРЕМЕН И ДО НАШИХ ДНЕЙ

1.1.Основные понятия криптографии

Криптография – это греческое слово, обозначающее в переводе «тайнопись». В общем смысле, криптография – это наука, которая изучает математические методы преобразования информации. Наряду с понятием криптография часто используют термины «криптоанализ» и «криптология». Криптоанализ – это наука о способах вскрытия шифров, в то время как криптология используется для обозначения всей области секретной связи [1, 11].

Криптографические алгоритмы широко применяются в современном обществе для хранения и обработки паролей пользователей в сети, при передаче бухгалтерских отчетов через удаленные каналы связи, в случаях обслуживания банковских пластиковых карт и т.п.

Все задачи, которые решаются с помощью криптографии существенно зависят от уровня развития техники и технологии, от применяемых средств связи и способов передачи информации. Кроме этого, криптография использует достижения фундаментальных наук, и прежде всего, математики.

Для рассмотрения примеров методов шифрования необходимо ввести основные понятия криптографии.

Исходное сообщение, которое требуется защитить при передаче по каналам связи, обычно называют **открытым текстом** или сообщением.

Совокупность заранее оговоренных способов преобразования открытого сообщения с целью его защиты называют **шифром.**

Сообщение, полученное после преобразования с использованием любого шифра, называется **шифрованным сообщением** (закрытым текстом, криптограммой).

Процесс преобразования открытого текста в шифрованное сообщение называется **шифрованием.**

Шифрование – это способ защит информации ценного характера от организованной преступности. Несмотря на то, что шифрование изначально должно было использоваться только в военных целях, в информационном обществе оно стало одним из главных способов обеспечения безопасности доступа к ресурсам, электронным платежам, деловой переписке и т.п.

Обратный процесс, заключающийся в процессе преобразования закрытого текста в исходное сообщение, называется **расшифрованием.**

Осуществить процессы шифрования и расшифрования сообщений можно только с использованием специальной информации, которая называется **ключом.**

В **криптоанализе** как науке о методах и способах вскрытия шифров основными понятиями являются стойкость шифра и атака на шифр.

Стойкость шифра – это характеристика шифра, определяющая его стойкость к дешифрованию без знания ключа.

Атака на шифр – это попытка вскрытия шифра какими-либо методами.

Вскрытием (взламыванием) шифра является процесс получения защищаемой информации из шифрованного сообщения без знания примененного шифра.

«Любой шифр может быть вскрыт, если только в этом есть настоятельная необходимость и информация, которую предполагается получить, стоит затраченных средств, усилий и времени…» – Норберт Винер.

Получение строгих доказуемых оценок стойкости для каждого конкретного шифра – проблема нерешенная. Это объясняется тем, что до сих пор нет необходимых для решения такой проблемы математических результатов. Поэтому стойкость конкретного шифра оценивается только путем всевозможных попыток его вскрытия и зависит от квалификации криптоаналитиков, атакующих шифр. Такая процедура называется проверкой стойкости шифра.

Задачей криптоаналитика является получение открытого текста и ключа на основе анализа шифротекста.

Обычно считается, что противник, то есть человек или организация, стремящаяся вскрыть какой-то текст, знает шифр и имеет возможности для его предварительного изучения. Противник также знает некоторые характеристики открытых текстов, например, общую тематику сообщений.

Можно выделить несколько возможностей для противника:

- противник может перехватить все шифрованные сообщения, но не имеет соответствующих им открытых текстов;
- противник может перехватить все шифрованные сообщения и добывать соответствующие им открытые тексты;
- противник имеет доступ к шифру, но не к ключам, поэтому может шифровать и дешифровать любую информацию.

Кроме перехвата и вскрытия шифра противник может пытаться получить защищаемую информацию многими другими способами. Например, известен агентурный метод, когда противник каким-либо путем склоняет одного из законных пользователей к сотрудничеству и с помощью этого агента получает доступ к защищаемой информации. В такой ситуации криптография бессильна. Также противник может пытаться не получить, а уничтожить или модифицировать информацию в процессе ее передачи. Для защиты от таких угроз разрабатываются свои специфические методы. Таким образом, передаваемая информация может защищаться различными способами.

Основная классификация криптографических методов делит их на две большие части:

- методы шифрования с закрытым ключом (симметричное шифрование);
- методы шифрования с открытым ключом (асимметричное шифрование).

При шифровании с закрытым ключом используется один и тот же ключ как для шифрования, так и для расшифрования сообщения, который обе стороны стараются хранить в секрете от противника.

Методы шифрования с открытым ключом начали разрабатываться относительно недавно во второй половине XX в. В эту группу относятся методы, в которых для шифрования и расшифрования данных используются два разных ключа. При этом открытый ключ может передаваться по незащищенному каналу связи.

В зависимости от характера воздействий, производимых над данными, алгоритмы делятся на следующие виды:

- перестановочные, в которых блоки информации (биты, байты и т.п.) не изменяются сами по себе, но изменяется их порядок следования, что делает информацию недоступной стороннему наблюдателю;
- подстановочные, в которых изменяются по определенным правилам непосредственно блоки информации.

В зависимости от размера блока информации криптоалгоритмы могут делиться на следующие группы:

- потоковые шифры, в которых единицей шифрования является один бит. Результат кодирования в таких шифрах не зависит от прошедшего ранее входного потока. Схема применяется в системах передачи потоков информации, то есть в тех случаях, когда передача информации начинается и заканчивается в произвольные моменты времени и может случайно прерываться;
- блочные шифры, в которых единицей шифрования является блок байтов. Результат шифрования в этом случае зависит от всех исходных байтов блока. Схема применяется при пакетной передаче информации.

1.2.История развития криптографии

Различные методы шифрования применялись и в древности. До наших дней дошли зашифрованные записи египетского вельможи, высеченные на его гробнице.

Развитию шифрования способствовали войны. Письменные приказы и донесения обязательно шифровались, чтобы захват гонцов не позволил противнику получать важную информацию.

Ряд систем шифрования появились примерно в 4 тысячелетии до нашей эры одновременно с письменностью. Методы секретной переписки были изобретены независимо во многих древних странах, таких как Египет, Шумер и Китай. Один из древних методов шифрования назывался атбаш, представляющий собой шифр замены – вместо первой буквы алфавита писалась последняя, вместо второй – предпоследняя и так далее.

В качестве примера шифра замены, изобретенного в древние времена, может выступать шифр Юлия Цезаря. В шифрованном сообщении Цезаря каждая буква заменялась четвертой по счету от нее буквой в алфавите. Тогда знаменитая фраза этого полководца: «VENI, VIDI, VICI» («Пришел, увидел, победил») в зашифрованном виде будет иметь вид: «XFOJ, XJEF, XJDJ».

Принципиально иной шифр, более древний, связан с перестановкой букв сообщения по определенному правилу, известному и отправителю и получателю. Этот шифр назывался скитала, по названию стержня, на который наматывались свитки папируса. Свиток наматывали на палочку по спирали и вдоль палочки писали текст. После снятия полоски, буквы на ней располагались хаотично. Для прочтения такой шифровки требовалось знать не только способ засекречивания, но и обладать ключом в виде палочки определенного диаметра. Этот шифр был популярен в Спарте и совершенствовался в более поздние времена.

Греческий писатель и историк Полибий за два века до нашей эры изобрел полибианский квадрат. Квадрат размером 5х5 заполнялся буквами алфавита случайным образом. Для шифрования на квадрате находили букву текста и заменяли ее буквой, стоящей в квадрате снизу. Если буква находилась в нижней строке, то ее заменяли буквой первой строки того же столбца.

С древних времен существовали и приборы для шифрования. Спарта, наиболее воинственная из греческих государств, имела хорошо проработанную систему секретной связи еще в 5 веке до нашей эры. С помощью скиталы, первого известного криптографического устройства, члены спартанского коллегиального правительства шифровали послания, используя метод перестановки.

Римляне в качестве криптографических устройств использовали шифрующие диски. Каждый из двух дисков, помещенных на общую ось, содержал на ободе алфавит в случайной последовательности. Найдя на одном диске букву текста, с другого диска считывали соответствующую ей букву шифра. Такие приборы, порождающие шифр простой замены, использовались до эпохи Возрождения.

Для связи греки и римляне использовали код на основе полибианского квадрата с естественным заполнением алфавитом. Буквы кодировались номером строки и номером столбца, соответствующим ей в квадрате. Сигнал передавался ночью факелами, а днем флагами.

После падения Римской империи в Европе пошли столетия упадка, в течение которых все лучшие достижения цивилизации, а вместе с тем и криптология, были утрачены. Возрождение криптографии относится к концу средневековья.

Ученые средневековья применяли шифр, основанный на использовании магических квадратов – это квадратные таблицы со вписанными в их клетки последовательными натуральными числами с 1, в которых сумма по всем строкам, столбцам и диагоналям одинакова. Текст сообщения вписывался в таблицу в соответствии с приведенной в ней нумерацией. Затем текст выписывался по строкам. Надежность данного шифра определялась большим количеством магических квадратов. Существует один квадрат 3x3, квадратов 4x4 всего 880, а 5x5 уже около 250000. Ручной перебор всех вариантов был чрезвычайно затруднителен.

Увлечение теорией магических квадратов привело к открытию нового класса шифров перестановок, которые получили название решетки или трафареты. Трафареты представляют собой квадратные таблицы, четверть ячеек которых вырезана, причем таким образом, что при четырех поворотах они скрывают весь квадрат. Вписывание в прорезанные ячейки текста и повороты решеток повторяется до тех пор, пока весь квадрат не будет заполнен. Число решеток очень быстро растет с увеличением их размера. Решеток 2х2 существует всего одна, решеток 4х4 уже 256, а 6х6 уже более ста тысяч. Однако шифры типа решеток довольно просто вскрываются и не могут быть использованы в качестве самостоятельного шифра.

Шифр Вижинера является модификацией шифра Цезаря. Замена символов сообщения производится в соответствии с ключевой фразой и используемой таблицей замены.

Композиторы использовали методы тайнописи для включения своего имени в музыкальные произведения. Так, Иоганн Себастьян Бах кодировал свою фамилию нотами, которые составляли основную тему произведения. Несколько органных фуг Баха представляют вариации относительно такой темы.

На Руси в Новгороде с XIV века использовались коды простой замены, так как наряду с буквами использовался и ряд специальных символов. В это время начинает складываться тарабарский язык, заключающийся в следующем: все сообщение разбивалось на слоги и между каждым слогом вставлялись попеременно слоги ТАРА и БАРА. Этот способ шифрования применялся в нашей стране до начала 18 века.

19 век принес в криптографию новые достижения. Постоянно расширяющееся применение шифров выдвигало и новые требования к ним – легкость массового использования и устойчивость к взлому. В 1854 году Чарльз Уитстон разработал новую систему шифрования биграммами, которую называют двойной квадрат. Этот шифр использует сразу две таблицы, расположенные по горизонтали, а шифрование идет биграммами по

простому правилу. Сообщение разбивается на биграммы и шифруется. Если обе буквы исходного текста принадлежат одной колонке, то буквами шифра считаются буквы, которые в таблице расположены под ними. Если буква открытого текста находилась в нижнем ряду, то бралась буква того же столбца, но в первой строке. Если обе буквы биграммы исходного текста принадлежали одной строке, то буквами шифра считались те, которые лежали справа от них. Если обе буквы биграммы исходного текста лежали в разных строках и разных столбцах, то брались такие две буквы, чтобы все четыре буквы образовывали прямоугольник. Шифрование биграммами дает весьма устойчивый к вскрытию и простой шифр.

Прибором шифрования в этот период выступал цилиндр Базери. Этот прибор состоял из 20 дисков со случайно нанесенным по ободу алфавитом. Перед началом шифрования диски помещались на общую ось в порядке, определяемом ключом. После набора первых 20 букв текста в ряд на цилиндрах их поворачивали вместе и считывали в другом ряду шифрованное сообщение. Процесс повторялся до тех пор, пока не было зашифровано все сообщение.

Однако первая практически используемая криптографическая машина была предложена Жильбером Вернамом только в 1917 году. Предшественницей современных шифровальных устройств была роторная машина, изобретенная в 1917 году Эдвардом Хеберном и названная в дальнейшем Энигмой.

1.3.Алгоритмы шифрования с закрытым ключом

Процессы шифрования и расшифрования в методах шифрования информации с закрытым ключом осуществляются с использованием одного и того же ключа. Именно поэтому закрытый ключ следует хранить в тайне от противника.

Рассмотрим общий принцип симметричного шифрования информации и классификацию этих методов.

Допустим, пользователю А необходимо отправить пользователю Б некоторое сообщение, при этом исключается ситуация чтения этого сообщения третьим лицом. Поэтому перед отправкой сообщения пользователю А необходимо это сообщение зашифровать, при этом для шифрования и расшифрования сообщения будет использоваться один и тот же закрытый ключ.

Пользователь А, изображенный на рисунке 1, формирует некоторое сообщение, шифрует его с использованием выбранного ключа, затем пересылает его пользователю Б по открытому каналу связи.

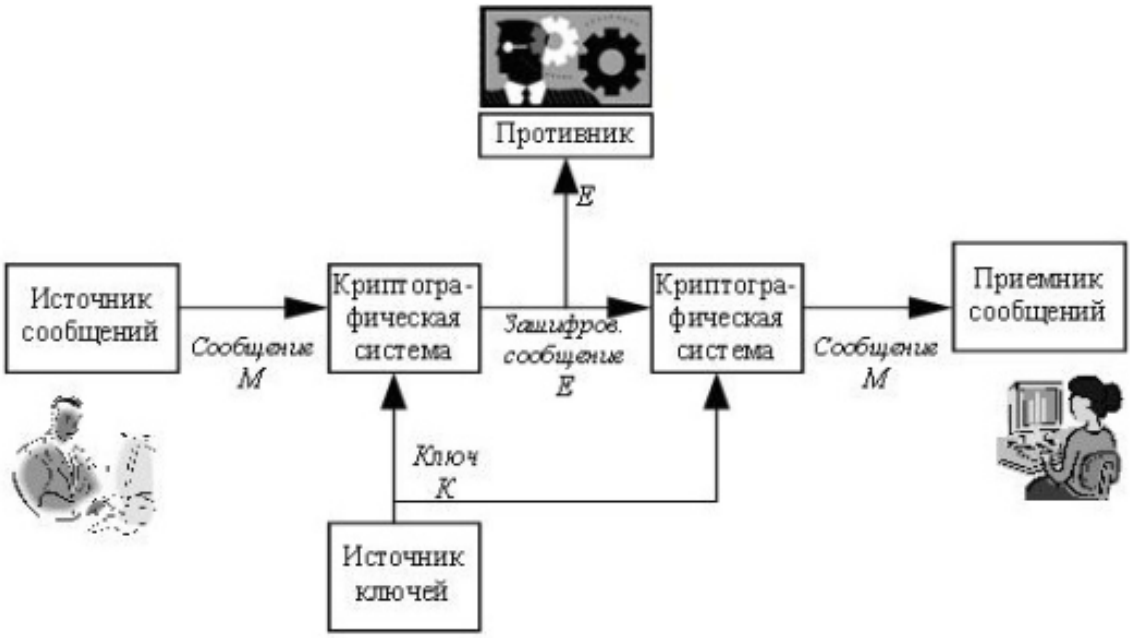


Рис. 1. Общая схема симметричного шифрования

Пользователь Б, получив криптограмму, расшифровывает ее с помощью ключа, который предварительно был передан пользователем А по защищенному каналу связи, и получает исходное сообщение.

К настоящему времени накоплено уже достаточно большое количество методов шифрования с закрытым ключом, которые можно разделить на следующие группы:

− методы замены (одноалфавитная замена, многоалфавитная замена);

- методы перестановки (перестановка с фиксированным периодом, табличная перестановка);
- блочные алгоритмы;
- поточные алгоритмы.

Рассмотрим примеры использования этих алгоритмов более подробно.

1.3.1. Методы замены и перестановки

Основная идея методов шифрования заменой заключается в том, что символы исходного текста заменяются одним или несколькими символами другого алфавита в соответствии с принятым правилом преобразования.

Методы замены, в свою очередь, представлены следующими видами:

- одноалфавитная замена (шифр Юлия Цезаря, простая замена, пропорциональные шифры);
- многоалфавитная замена (шифр Вижинера).

Наиболее ярким примером метода одноалфавитной замены является шифр знаменитого римского императора Юлия Цезаря, жившего в 1 в. до н.э. Исторически установлено, что великий полководец использовал этот шифр в своей переписке.

Алгоритм шифра Юлия Цезаря применительно к русскому алфавиту заключается в том, что каждая буква сообщения заменяется на другую букву, которая в русском алфавите отстоит от исходной на три позиции дальше. Таким образом, буква А заменяется на Г, буква Б на Д и так далее, затем для букв Э, Ю, Я начинается просмотр алфавита с первого символа.

Например, слово Информатика после шифрования методом Юлия Цезаря превратится в слово Лрчсупгхлнг. Чтобы расшифровать полученную криптограмму необходимо знать только алгоритм шифрования.

В случае сдвига букв не на три знака вправо, а на n, где n не может быть больше количества символов в алфавите, можно усложнить алгоритм метода шифрования Юлия Цезаря. В этом случае параметр сдвига n будет

являться ключом шифрования. Так как значение ключа нужно держать в секрете, то отправитель и получатель могут каким-либо образом договариваться о значении ключа.

Для реализации метода простой замены может быть использована таблица, например, приведенная на рисунке 2.

Откр. текст	Шифр 1	Шифр 2		Откр. текст	Шифр 1	Шифр 2		Откр. текст	Шифр 1	Шифр 2
А	В	^		М	Т	№		Ч	М	Σ
Б	И	@		Н	Ц	#		Ш	У	∇
В	О	)		О	.	-		Щ	Д	ϒ
Г	А	+		П	Ж	=		Ъ	Э	ℵ
Д	Щ	<		Р	Г	(		Ы	Н	⊕
Е	П	>		С	Л	?		Ь	Ю	×
Ж	К	∀		Т	Х	%		Э	Ы	⌀
З	Б	♦		У	С	⊗		Ю	Ш	$
И	Ъ	*		Ф	Ь	!		Я	Е	Δ
К	пробел	♥		Х	Ч	№		пробел	Ф	∞
Л	Р	♠		Ц	З	®		.	Я	♣

Рис. 2. Таблица для выполнения шифрования методом замены

С помощью таблицы замен, приведенной на рисунке 2, можно привести пример шифрования слова ВСТРЕЧА, которое примет следующий вид: ОЛХГПМВ. Однако зашифрованный текст имеет сравнительно низкий уровень защиты, так как может быть вскрыт с помощью частотного криптоанализа.

Частотный криптоанализ использует статистические данные языка, на котором написано сообщение. Известно, что в текстах на русском языке наиболее часто встречаются символы О, И. Реже встречаются буквы Е и А. Из согласных к наиболее часто встречающимся символам относятся Т, Н, Р и С.

Специалист по расшифровке информации без знания ключа, то есть криптоаналитик, внимательно изучает полученную криптограмму, подсчитывая частоту встречи символов, входящих в сообщение. Далее наиболее часто встречаемые знаки зашифрованного сообщения заменяются, например, буквами О. Затем производится попытка определить места для

букв И, Е, А и часто встречаемых согласных. Однако, если ничего не известно заранее о содержании перехваченного сообщения малой длины, дешифровать его однозначно не получится. Достаточно длинное сообщение, зашифрованное методом простой замены, в большинстве случаев обычно удается успешно дешифровать.

Если попытаться замаскировать статистические характеристики открытого текста, то задача вскрытия шифра простой замены значительно усложнится. Например, можно использовать программы-архиваторы перед шифрованием для сжатия открытого текста.

Пропорциональные шифры являются одним из видов метода шифрования с помощью одноалфавитной замены, в которых для знаков, встречающихся часто, используется относительно большое число возможных эквивалентов, а для менее используемых исходных знаков может оказаться достаточным одного или двух эквивалентов. Например, в качестве замен для пропорционального шифра может быть использована следующая таблица 1.

В этом случае сообщение ВЗРЫВ может быть зашифровано следующим образом: 210753134136106.

Пропорциональные шифры обладают большей надежностью относительно шифров простой одноалфавитной замены. Однако если имеется хотя бы одна пара «открытый текст – шифротекст», то дешифрование производится достаточно просто.

В целях повышения надежности шифрования методы замены естественным образом усложнялись путем маскирования естественной частотной статистики исходного языка. В многоалфавитных подстановках для замены символов исходного текста используется не один, а несколько алфавитов, либо алфавиты для замены образуются из символов одного алфавита, записанных в другом порядке.

Таблица 1

Таблица замен для пропорционального шифра

Символ	Варианты замены					Символ	Варианты замены					
А	760	128	350	201		С	800	767	105			
Б	101					Т	759	135	214			
В	210	106				У	544					
Г	351					Ф	560					
Д	129					Х	768					
Е	761	130	802	352		Ц	545					
Ж	102					Ч	215					
З	753					Ш	103					
И	762	211	131			Щ	752					
К	754	764				Ъ	561					
Л	132	354				Ы	136					
М	755	742				Ь	562					
Н	763	756	212			Э	750					
О	757	213	765	133	353	Ю	570					
П	743	766				Я	216	104				
Р	134	532				Пробел	751	769	758	801	849	035...

Шифр Вижинера – это пример шифрования методом многоалфавитной замены. Данный метод был изобретен в XVI веке французским ученым Блезом Вижинером. Для применения шифра Вижинера необходимо использовать таблицу (матрицу), изображенную на рисунке 3.

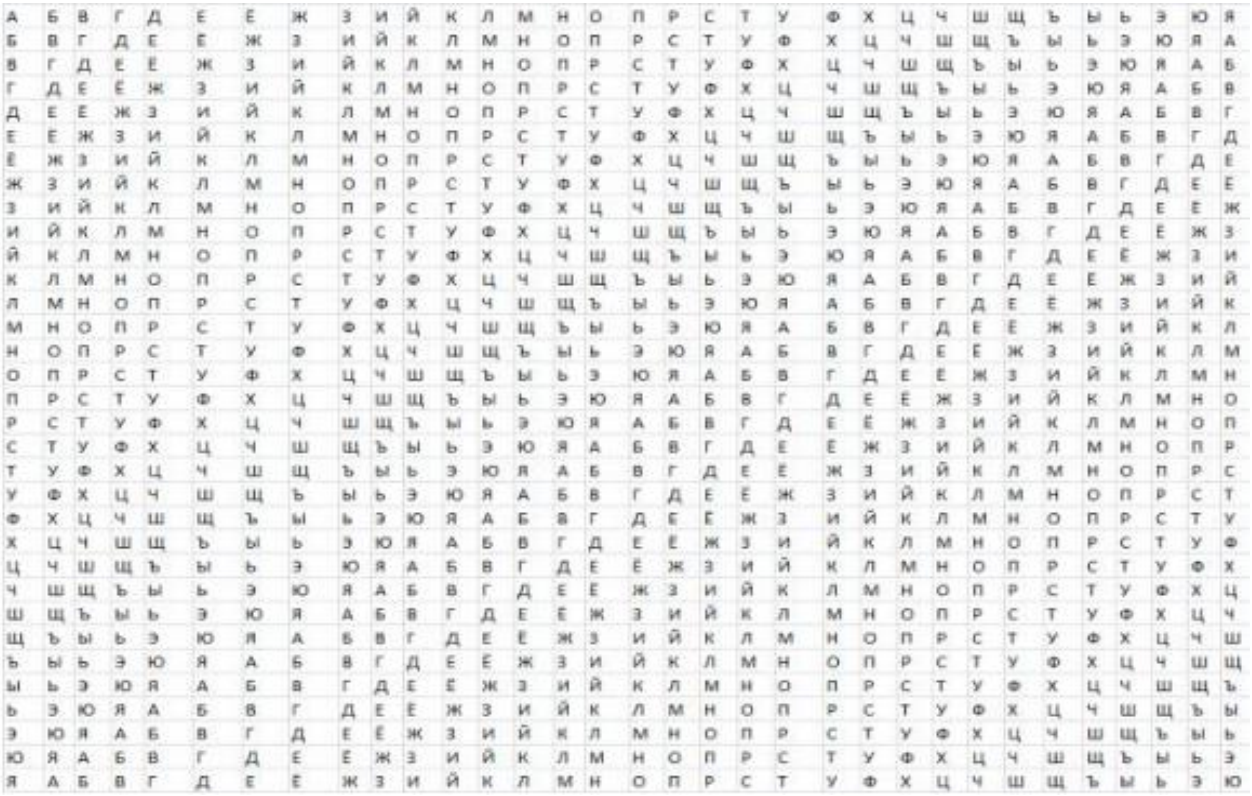


Рис. 3. Таблица Вижинера

Таблица Вижинера устроена следующим образом: в первой строке таблицы располагаются буквы в исходном алфавитном порядке, во второй строке записывается та же последовательность букв, циклически сдвинутая влево на одну позицию, в третьей строке – сдвинутая на две позиции и т. д. Однако рассматриваемая таблица лишь помогает сформировать таблицу, непосредственно используемую для шифрования.

Для формирования подматрицы шифрования необходимо выбрать ключ, представляющий собой некоторое слово или набор символов исходного алфавита, затем из полной матрицы выписывают подматрицу шифрования, включающую первую строку и строки матрицы, начальными буквами которых являются последовательно буквы ключа. Например, если выбрать ключ ГРОМ, то подматрица шифрования будет иметь вид, изображенный на рисунке 4.

А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В
М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л
О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н
Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П

Рис.4. Подматрица шифрования в методе Вижинера

Пусть необходимо зашифровать методом Вижинера с использованием ключа ГРОМ сообщение «НАЧАЛО ОПЕРАЦИИ». Для этого сначала выписывают символы исходного сообщения, затем под каждой буквой шифруемого текста подписывают символы ключа, повторяя их требуемое число раз (рисунок 5).

Н	А	Ч	А	Л	О	О	П	Е	Р	А	Ц	И	И
Г	Р	О	М	Г	Р	О	М	Г	Р	О	М	Г	Р

Рис. 5. Алгоритм шифрования методом Вижинера

Далее шифруемый текст по подматрице шифрования заменяют символами, расположенными на пересечениях линий, соединяющих символы ключа, находящейся под ней и символа текста первой строки таблицы (рисунок 6).

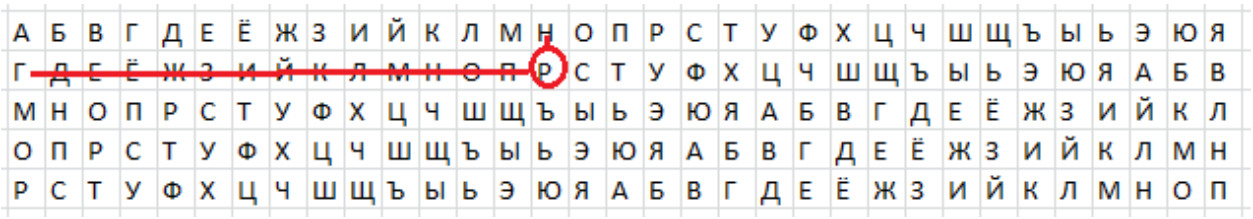


Рис. 6. Принцип замены в алгоритме шифрования методом Вижинера

Применяя аналогичную замену для следующих символов исходного сообщения получают следующую криптограмму, изображенную на рисунке 7.

Н	А	Ч	А	Л	О	О	П	Е	Р	А	Ц	И	И
Г	Р	О	М	Г	Р	О	М	Г	Р	О	М	Г	Р
Р	**Р**	**Ё**	**М**	**О**	**Я**	**Э**	**Ь**	**З**	**Б**	**О**	**Г**	**Л**	**Щ**

Рис. 7. Криптограмма, полученная в результате применения алгоритма шифрования методом Вижинера

С целью повышения надежности шифрования текста можно использовать подряд два или более шифрования по методу Вижинера с разными ключами.

Методы многоалфавитной подстановки являются достаточно надежными в случае «ручного» криптоанализа. В случае применения вычислительной техники скорости проводимых расчетов повышаются, следовательно, вскрытие метода многоалфавитной подстановки возможно достаточно быстро.

Наряду с методами замены к простейшим методам шифрования относятся методы перестановки. Основная идея шифров перестановки заключается в том, что исходный текст делится на блоки, в каждом из которых выполняется перестановка символов.

К основным видам методов замены относят:

- перестановка с фиксированным периодом;
- табличная перестановка.

При перестановке с фиксированным периодом P сообщение делится на блоки по P символов и в каждом блоке производится одна и та же операция перестановки. Ключом в данном случае является правило, по которому производится перестановка. В результате сами буквы сообщения не изменяются, но передаются в другом порядке.

Например, необходимо зашифровать методом перестановки с фиксированным периодом текст: МЕСТО_ВСТРЕЧИ_ИЗМЕНИТЬ_НЕЛЬЗЯ. В качестве периода перестановки взять d=6, а в качестве ключа перестановки взять 436215.

Для выполнения шифрования в каждом блоке из 6 символов четвертый символ становится на первое место, третий – на второе, шестой – на третье и т.д. То есть результатом шифрования для ключа 436215 будет следующее сообщение: ТС_ЕМОРТЧСВЕЗИЕ_ИМЬТНИН_ЗЬ_ЛЕЯ.

Следующим видом методов перестановки является перестановка по таблице. Основная идея этого метода заключается в том, что исходный текст

записывается по строкам некоторой таблицы. Последовательность заполнения строк и чтения столбцов может быть любой и задается ключом.

Например, необходимо зашифровать методом перестановки по таблице 5*6 сообщение: МЕСТО_ВСТРЕЧИ_ИЗМЕНИТЬ_НЕЛЬЗЯ.

Записываем исходное сообщение по строчкам таблицы 5*6 как показано на рисунке 8.

М	Е	С	Т	О	_
В	С	Т	Р	Е	Ч
И	_	И	З	М	Е
Н	И	Т	Ь	_	Н
Е	Л	Ь	З	Я	_

Рис. 8. Таблица для метода табличной перестановки

Если размер сообщения не кратен размеру блока, можно дополнить сообщение какими-либо символами, не влияющими на смысл, например, пробелами.

Затем считываем из таблицы каждый блок последовательно по столбцам, получая зашифрованное сообщение: МВИНЕЕС_ИЛСТИТЬТРЗЬЗ_ЧЕН_.

В этом методе в качестве ключа можно использовать порядок считывания столбцов.

Таким образом, шифрование как вид кодирования является одним из способов обработки информации. На практике часто используются алгоритмы шифрования методами замены, перестановки, а также комбинированные методы.

В предыдущем параграфе примеры шифрования приводились на основе символов русского алфавита. Однако, вся информация, которая поступает в компьютер, переводится в двоичный вид, следовательно, при шифровании с закрытым ключом обрабатываются только двоичные данные. Вполне естественно, что в процессе шифрования кроме обычных операций

замены и перестановки применяются другие специфичные для символов нулей и единиц операции.

Рассмотрим операции, применяемые к двоичным данным и используемые в большинстве современных алгоритмов шифрования с закрытым ключом.

Операция побитового (поразрядного) сложения по модулю 2, обозначаемая XOR или $\oplus$, является одной из часто используемых операций при шифровании.

Операция побитового сложения по модулю 2 представляет собой сложение двоичных чисел без переноса переполнения суммы в следующий разряд. В примере, изображенном на рисунке 9, в первом и пятом разряде сумма двух единиц в двоичной системе счисления дает 10_2, следовательно, в первом и пятом разряде необходимо записать символ нуля, а единицу перенести в следующий разряд, но в случае поразрядного сложения по модулю 2 такого переноса не происходит.

Номер разряда	7	6	5	4	3	2	1	0
Операнд 1	**1**	**0**	**1**	**0**	**1**	**0**	**1**	**0**
Операнд 2	**0**	**0**	**1**	**1**	**0**	**0**	**1**	**1**
Сумма по модулю 2	1	0	0	1	1	0	0	1

Рис.9. Операция XOR – побитовое сложение по модулю 2

Операция сложения по модулю 2^{32} или по модулю 2^{16} также является наиболее часто используемой операцией в шифровании. Эта операция выполняется как обычное сложение двоичных чисел, но при этом исключается перенос переполнения в 32-й или 16-й разряд результата. Операция сложения по модулю 2^{16} изображена на рисунке 10.

Номер разряда	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
Операнд 1	**1**	**0**	**1**	**0**	**1**	**0**	**1**	**0**	**1**	**0**	**1**	**0**	**1**	**0**	**1**	**0**
Операнд 2	**0**	**1**	**1**	**1**	**0**	**0**	**1**	**1**	**0**	**0**	**1**	**1**	**0**	**0**	**1**	**1**
Сумма по модулю 2	0	0	0	1	1	1	0	1	1	1	0	1	1	1	0	1

Рис. 10. Операция побитового сложения по модулю 2^{16}

Следующая операция циклического сдвига, наиболее распространенная при шифровании, передвигает биты на заданное число разрядов влево или вправо. В примере, приведенном на рисунке 11, демонстрируется, что при циклическом сдвиге вправо на три разряда, три крайних правых разряда переносятся и дописываются слева. Аналогично выполняется циклический сдвиг влево.

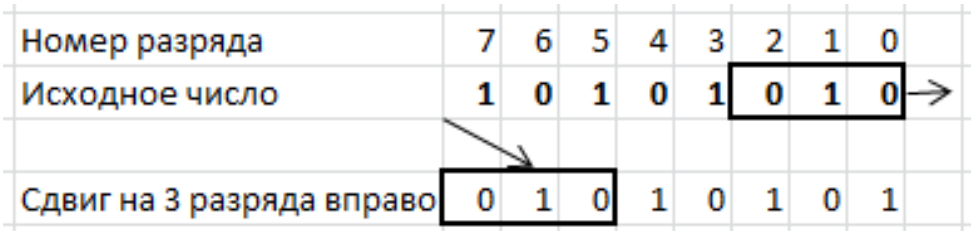


Рис. 11. Схема циклического сдвига на три разряда вправо

Таким образом, в алгоритмах симметричного шифрования часто используются операции циклического сдвига, поразрядного сложения по модулю 2, поразрядного сложения по модулю 2^{16} или 2^{32}, также операции перестановки и замены.

Вышеперечисленные операции являются простейшими и в алгоритме их принято циклически повторять, образовывая так называемые раунды. Также для удобства работы вся последовательность бит обычно делится на блоки фиксированной длины с характерным размером в пределах от 64 до 256 бит. Разновидность шифра фиксированной длины называется блочным шифром.

Одним из методов формирования блочного шифра является сеть Фейштеля, лежащая в основе известных алгоритмов DES и ГОСТ 28147-89. Процесс шифрования в сети Фейштеля легко реализуется как на программном уровне, так и на аппаратном, что обеспечивает широкие возможности применения.

Алгоритм шифрования с использованием сети Фейштеля изображен на рисунке 12.

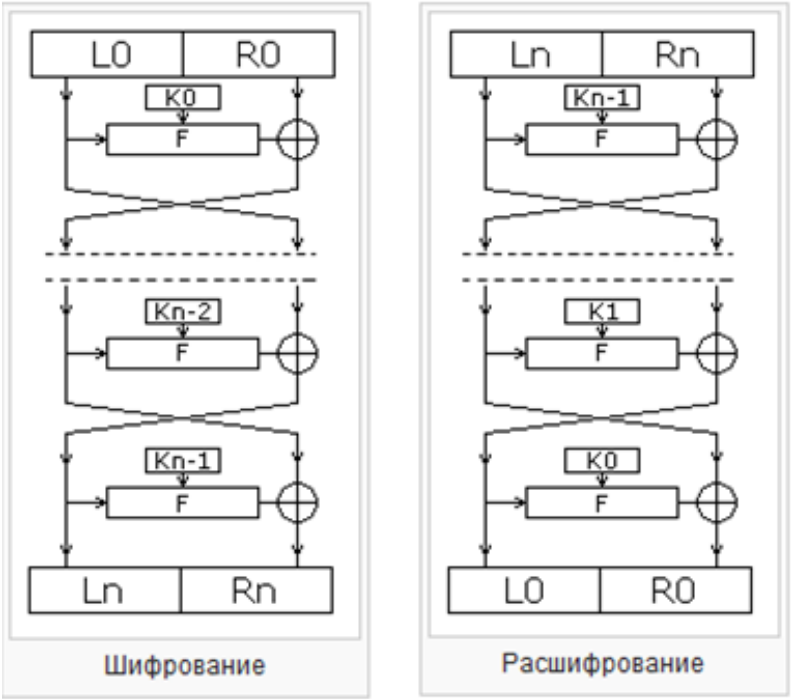


Рис. 12. Схема алгоритма сети Фейштеля

Разберем алгоритм сети Фейштеля на примере. Пусть необходимо зашифровать с использованием сети Фейштеля числа L=100 и R=200, используя формулу:

$$F(L, n) = (L+n) \% 256 \quad (1)$$

При выполнении первого раунда n=1, исходные числа равны L=100 и R=200. Вычисляем значение функции F(L, n) = (L+n) % 256 и полученный результат поразрядно складываем со значением переменной R:

$((100+1) \% 256) \oplus 200 = 173.$

Далее значения переменных меняются и становятся соответственно равными L=173, R=100.

При выполнении второго раунда n=2 значения переменных равны L=173, R=100. Вычисляем значение функции F(L, n) = (L+n) % 256 и полученный результат поразрядно складываем со значением переменной R:

$((173+2) \% 256) \oplus 100 = 203.$

В конце второго раунда значения переменных меняются и становятся соответственно равными L=203, R=173.

При выполнении третьего раунда n=3 значения переменных равны L=203, R=173. Вновь вычисляем значение функции F(L, n) = (L+n) % 256 и полученный результат поразрядно складываем со значением переменной R:

((203+3) % 256) ⊕173 = 99.

На последнем раунде значения переменных менять не нужно, то есть зашифрованные значения равны L=203, R=99.

Для проверки вычислений выполним процесс расшифровки чисел L=203, R=99.

На третьем раунде n=3, используя значения переменных L=203, R=99 вычисляем значение функции F(L, n) = (L+n) % 256 и полученный результат складываем со значением переменной R:

((203 + 3) % 256) ⊕99=173.

Далее значения переменных меняются и становятся соответственно равными L=173, R=203.

На втором раунде при n=2 и L = 173, R = 203 проводим аналогичные вычисления:

((173 + 2) % 256)⊕203 = 100.

Далее значения переменных меняются и становятся соответственно равными L = 100, R = 173.

На первом раунде при n=3 и L = 100, R = 173 также проводим аналогичные вычисления:

((100+1) % 256) ⊕ 173= 200.

Так как на последнем раунде значения переменных не меняются, то полученные значения L = 100, R = 173 равны первоначальным, следовательно, процесс шифрования и расшифрования проведен правильно.

1.3.2. Поточные шифры

При шифровании с закрытым ключом обрабатываются двоичные данные, разделенные на блоки. Однако шифрование блоками не

единственная возможность преобразования данных. Рассмотрим еще одну возможность шифрования данных по символам.

Обработка входного сообщения по одному биту (или байту) за операцию выполняется при использовании поточного шифра. Благодаря этому свойству поточный алгоритм может работать в реальном времени, то есть каждый поступающий символ может шифроваться и передаваться сразу.

Схема работы поточного шифра изображена на рисунке 13 и заключается в следующем: биты символов исходного текста складываются поразрядно по модулю 2 с битами соответствующего ключа из последовательности ключей, в результате чего получаются биты зашифрованного сообщения. Зашифрованное сообщение передается по открытому каналу связи, затем расшифровывается с использованием этой же последовательности ключей.

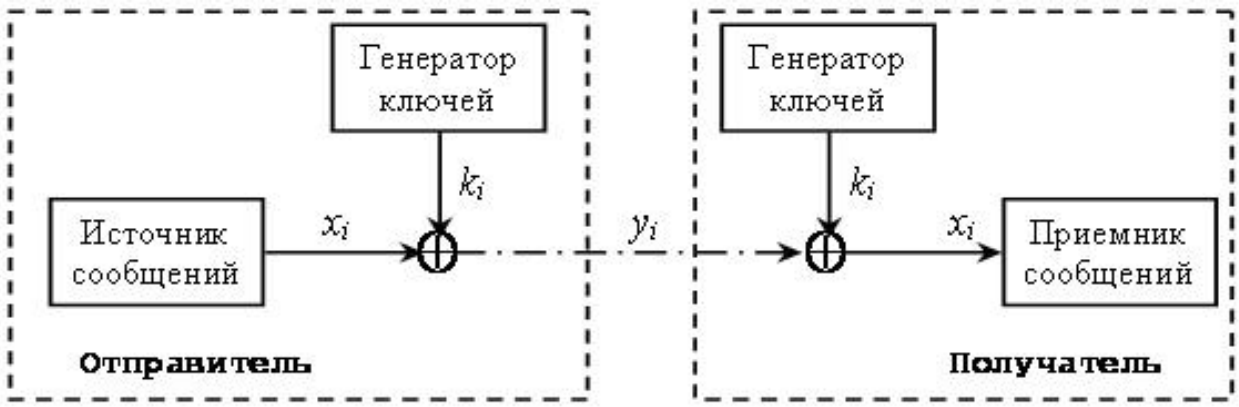


Рис. 13. Схема работы поточного шифра

Так как операции шифрования и расшифрования для всех поточных шифров одни и те же, то такие преобразования должны различаться только способом создания последовательности ключей, следовательно, надежность шифрования зависит от свойств генератора ключей.

Основное назначение генератора псевдослучайных чисел заключается в создании последовательности битов, похожей на случайную последовательность. Числа таких последовательностей вычисляются по определенным правилам, поэтому они не являются случайными и могут быть

абсолютно точно воспроизведены как на стороне отправителя сообщения, так и на стороне приемника.

Для обеспечения надежности шифрования генератору псевдослучайных чисел в криптографии предъявляются следующие требования:

- период последовательности псевдослучайных чисел должен быть очень большой;
- создаваемая последовательность псевдослучайных чисел должна быть практически неотличима от действительно случайной;
- вычисление последующего числа в псевдослучайной последовательности по известным предыдущим элементам без знания ключа должно быть трудной задачей.

В основе генераторов псевдослучайных чисел могут лежать разные алгоритмы создания псевдослучайных последовательностей, например, линейный конгруэнтный генератор, метод Фибоначчи с запаздыванием.

Линейный конгруэнтный генератор вычисляет очередное число по следующей формуле:

$$k_i = (a*k_{i-1}+b) \bmod c, \quad (2)$$

где a, b, c − некоторые константы,

k_{i-1} − предыдущее псевдослучайное число.

Начальное значение k_0 должно быть задано заранее для получения k_1.

Пример: Пусть требуется вычислить несколько элементов последовательности псевдослучайных чисел с помощью линейного конгруэнтного генератора, при этом заданы следующие начальные значения a=5, b=3, c=11, k_0= 1.

По приведенной выше формуле вычислим несколько элементов последовательности:

$k_1 = (5 * 1 + 3) \bmod 11 = 8;$

$k_2 = (5 * 8 + 3) \bmod 11 = 10;$

$k_3 = (5 * 10 + 3) \bmod 11 = 9;$

$k_4 = (5 * 9 + 3) \bmod 11 = 4;$

$k_5 = (5 * 4 + 3) \bmod 11 = 1;$

$k_6 = (5 * 1 + 3) \bmod 11 = 8,$

$k_7 = (5 * 8 + 3) \bmod 11 = 10;$

$k_8 = (5 * 10 + 3) \bmod 11 = 9.$

Можно заметить, что со значения k_6 псевдослучайные числа начинают повторяться, то есть 8, 10, 9, 4, 1 – это период псевдослучайной последовательности.

Линейный конгруэнтный генератор прост для понимания работы генератора псевдослучайных чисел, однако в криптографических целях он не используется, так как криптоаналитики научились вычислять всю последовательность чисел по нескольким значениям.

Более надежен по отношению к вскрытию противника метод Фибоначчи с запаздыванием.

Базовая формула этого метода имеет следующий вид:

$$k_i = \begin{cases} k_{i-a} - k_{i-b}, & если\ k_{i-a} \geq k_{i-b} \\ k_{i-a} - k_{i-b} + 1, & если\ k_{i-a} < k_{i-b} \end{cases} \qquad (3)$$

где k_i − вещественные числа из диапазона [0,1],

a, b − целые положительные числа.

Пример:

Пусть требуется вычислить несколько элементов последовательности псевдослучайных чисел с помощью метода Фибоначчи с запаздыванием, при этом заданы следующие начальные значения

a = 4, b = 1, k_0=0.1; k_1=0.7; k_2=0.3; k_3=0.9; k_4=0.5:

$k_5 = k_1 - k_4 = 0.7 - 0.5 = 0.2;$

$k_6 = k_2 - k_5 = 0.3 - 0.2 = 0.1;$

$k_7 = k_3 - k_6 = 0.9 - 0.1 = 0.8;$

$k_8 = k_4 - k_7 + 1 = 0.5 - 0.8 + 1 = 0.7;$

$k_9 = k_5 - k_8 + 1 = 0.2 - 0.7 + 1 = 0.5;$

$k_{10} = k_6 - k_9 + 1 = 0.1 - 0.5 + 1 = 0.6;$

$k_{11} = k_7 - k_{10} = 0.8 - 0.6 = 0.2;$

$k_{12} = k_8 - k_{11} = 0.7 - 0.2 = 0.5;$

$k_{13} = k_9 - k_{12} + 1 = 0.5 - 0.5 + 1 = 1;$

$k_{14} = k_{10} - k_{13} + 1 = 0.6 - 1 + 1 = 0.6.$

1.3.3. Примеры современных алгоритмов с закрытым ключом

Наиболее известными алгоритмами шифрования с открытым ключом на сегодняшний день являются OTP, DES, IDEA, Российский стандарт шифрования.

OTP (one-time pad) – единственный шифр, который считается безоговорочно безопасным, то есть вероятность его взлома практически равна нулю. Это также доказывает, что любой безусловно стойкий шифр должен использовать только один круг шифрования.

IDEA (international decryption-encryption algorithm) разработан в 1990-1991 годах в Цюрихе в Швейцарии. Запатентован в США, Европе и Японии.

В данном шифре используются 64-битовые блоки, размер ключа составляет 128 бит, число раундов – 8. В шифре IDEA используется относительно сложная структура раунда при небольшом их количестве. Шифрование данных осуществляется с помощью аддитивных и мультипликативных операций.

В качестве американского стандарта шифрования данных в середине 70х годов XX века Национальным Институтом Стандартов и Технологий была принята система шифрования DES. DES – это блочный шифр. Размер блока составляет 64 бита. В системе используется 16 раундов. Шифр достаточно устойчив к атакам хакеров, но легко поддается вскрытию с использованием специального аппаратного обеспечения. Поэтому данная система становится слишком слабой и не используется в новых прикладных программах.

Вариант DES – 3 DES основан на использовании того же стандарта шифрования данных, но шифрование исходного текста проводится три раза.

Этот способ шифрования является более сильным и устойчивым, однако, довольно медленным по сравнению с некоторыми новыми блочными шифрами.

DES – это первый блочный шифр, который широко применялся в общественном секторе, что сыграло важную роль в создании систем шифрования.

1.4. Алгоритмы шифрования с открытым ключом. Алгоритм RSA

При шифровании с закрытым ключом может возникнуть проблема безопасной передачи секретного ключа получателям сообщения. Для решения этой проблемы были разработаны так называемые асимметричные криптографические алгоритмы, в которых шифрование и расшифрование выполняется на различных ключах.

При ассиметричном шифровании один из двух ключей, применяющийся при шифровании, является открытым и может быть объявлен всем, а второй ключ, использующийся при расшифровании, называется закрытым и должен держаться в секрете.

В то время как алгоритмы симметричного шифрования используют в основном операции замены, перестановки, поразрядного суммирования по модулю 2, циклического сдвига, основная особенность асимметричных криптографических алгоритмов заключается в том, что они основаны на свойствах так называемых односторонних функций.

Односторонней функцией называется математическая функция, которую относительно легко вычислить, но трудно найти по значению функции соответствующее значение аргумента. Под выражением «трудно вычислить» понимают, что для вычисления этого значения потребуется не один год расчетов с использованием ЭВМ.

Одним из первых в конце 70-х гг. XX в. был предложен алгоритм шифрования с открытым ключом RSA, кроме того, этот алгоритм является

одним из широко применяемых и наиболее популярных асимметричных алгоритмов. Шифрование с использованием алгоритма RSA применяется в операционной системе Windows, в популярном пакете шифрования PGP, в различных Интернет-браузерах, в банковских компьютерных системах.

Название RSA является аббревиатурой, в частности, составлено из первых букв фамилий авторов: Р.Ривест, А.Шамир и Л.Адлеман. Алгоритм основан на использовании того факта, что задача разложения большого числа на простые сомножители является трудной.

Перед тем как описать основные шаги алгоритма шифрования RSA, рассмотрим некоторые положения теории чисел, применяемые в данном алгоритме.

Если делителями числа является единица и само число, то оно называется простым, в противном случае, если у числа есть еще делители, то такое число называется составным. Например, простые числа 7, 29; составные числа 10, 225.

Не для каждого числа можно сразу определить, простое оно или составное. Проверка на простоту оказывается сложной для больших чисел, например, для числа 20000017? В таких случаях для работы с большими целыми числами требуются специальные компьютерные программы.

Простые числа могут быть своеобразным решением задачи факторизации, заключающейся в нахождении двух или более чисел, дающих при перемножении заданное число. Решение задачи факторизации базируется на основной теореме арифметики, доказывающей, что любое составное число можно составить из некоторого количества простых чисел с помощью умножения.

Решение задачи факторизации требует значительных затрат времени даже в том случае, когда известно, что оно является произведением двух больших простых чисел. Сложность задачи факторизации применяется в некоторых криптографических алгоритмах, в частности, в системе шифрования RSA.

Для использования алгоритма шифрования RSA может понадобиться следующее определение. Два числа называются взаимно простыми, если они не имеют ни одного общего делителя кроме единицы. Например, числа 11 и 12 взаимно просты, так как у них нет общих делителей кроме единицы, а числа 30 и 35 не являются взаимно простыми, так как у них есть общий делитель 5.

Деление по модулю (деление с остатком) – это арифметическая операция, означающая нахождение таких целых чисел q и r для деления по модулю a на b, что выполняется равенство:

$$a = b * q + r \quad (4)$$

Таким образом, результатом операции деления по модулю a mod b будет являться число r. Например, 78 mod 33 = 12 или (-78) mod 33 = 21.

Рассмотрим принцип шифрования информации по алгоритму RSA. Пусть первый абонент желает передать зашифрованное сообщение второму абоненту. Первоначально второй абонент должен подготовить пару, состоящую из открытого и закрытого ключа, далее отправить свой открытый ключ первому пользователю.

Для подготовки открытого и закрытого ключей выбираются два больших простых числа P и Q. Затем вычисляется их произведение

$$N = P*Q. \quad (5)$$

Следующим шагом рассчитывается вспомогательное число

$$f = (P - 1)*(Q - 1) \quad (6)$$

Для проведения шифрования далее случайным образом выбирается число $d < f$ и взаимно простое с f.

Следующим шагом необходимо найти число e такое, что

$$e*d \bmod f = 1 \quad (7)$$

Найденные числа d и N будут являться открытым ключом пользователя, а значение e – закрытым ключом.

Второй пользователь желает получить зашифрованное сообщение от первого пользователя, следовательно, второй пользователь должен отправить открытый ключ (d, N) первому пользователю.

Выбранные первоначально числа P и Q далее не будут использоваться больше в вычислениях, однако для обеспечения безопасности их нельзя никому сообщать.

Описанные действия являются своего рода подготовительными для выполнения алгоритма шифрования RSA.

Если первый абонент желает передать некоторое сообщение второму абоненту, он должен представить сообщение в цифровом виде и разбить его на блоки m_1, m_2, m_3, ... , где $m_i < N$.

Первый абонент каждый блок сообщения шифрует по следующей формуле, используя открытые параметры второго пользователя

$$c_i = m_i \text{^d mod } N \quad (8)$$

Зашифрованное сообщение состоит из частей c1, c2, c3, и т.д. и готово для передачи по открытой линии.

Второй абонент, получив зашифрованное сообщение, расшифровывает все его блоки по формуле:

$$m_i = c \text{^e mod } N \quad (9)$$

В случае перехвата третьим лицом зашифрованного сообщения, противник, знающий открытый ключ, не сможет найти исходное сообщение при больших значениях P и Q, следовательно, надежность к взлому алгоритма шифрования RSA достаточно высокая.

Выводы по главе 1

В данной главе были рассмотрены основные понятия, касающиеся криптографической защиты информации. К таким понятиям относятся: криптография, криптоанализ, шифр, шифрование, открытый текст, криптограмма, закрытый текст, ключ, открытый ключ, закрытый ключ, стойкость шифра, атаки на шифр.

В процессе изучения литературы был прослежен процесс становления криптографии как науки и выделены следующие этапы ее развития:

1. Криптография в древности – использовались следующие алгоритмы и устройства шифрования: атбаш, шифр Цезаря, скитала, полибианский квадрат, магический квадрат, шифры перестановки и замены.
2. Криптография средних веков – использовались следующие методы и устройства шифрования: шифр Вижинера, шифр Гронсфельда, тарабарская грамота, биграммные шифры, цилиндр Базери, Энигма.
3. Современная криптография – использовались следующие методы и устройства шифрования: OTP, DES, IDEA, Российский стандарт шифрования, RSA.

Таким образом, в первой главе квалификационной работы рассмотрены основные теоретические положения по криптографической защите информации. Перейдем к обоснованию того, что изучение этих вопросов обеспечит понимание учащимися важности защиты информации, а также сформирует стойкий интерес к серьезному обучению более сложных алгоритмов криптографии в будущем.

ГЛАВА 2. РАЗРАБОТКА ЭЛЕКТИВНОГО КУРСА «ОСНОВЫ КРИПТОГРАФИИ»

2.1. Анализ нормативных документов

Федеральные государственные образовательные стандарты (ФГОС) представляют собой совокупность требований, обязательных при реализации основных образовательных программ начального общего, основного общего, среднего (полного) общего, начального профессионального, среднего профессионального и высшего профессионального образования образовательными учреждениями, имеющими государственную аккредитацию.

ФГОС обеспечивают:

1) единство образовательного пространства Российской Федерации;
2) преемственность основных образовательных программ начального общего, основного общего, среднего (полного) общего, начального профессионального, среднего профессионального и высшего профессионального образования.

Был проанализирован ФГОС основного общего образования (ФГОС ООО) и среднего (полного) общего образования (ФГОС С(П)ОО).

ФГОС ООО устанавливает требования к результатам освоения основной образовательной программы основного общего образования.

Метапредметные результаты:

- формирование и развитие компетентности в области использования информационно-коммуникационных технологий (далее ИКТ-компетенции).

Предметные результаты:

Изучение предметной области «Математика и информатика» должно обеспечить:

- осознание значения математики и информатики в повседневной жизни человека;

– понимание роли информационных процессов в современном мире.

В результате изучения предметной области «Математика и информатика» обучающиеся получают представление об основных информационных процессах в реальных ситуациях.

Предметные результаты изучения предметной области «Математика и информатика» должны отражать:

– формирование информационной и алгоритмической культуры; формирование представления о компьютере как универсальном устройстве обработки информации; развитие основных навыков и умений использования компьютерных устройств;
– формирование умений формализации и структурирования информации, умения выбирать способ представления данных в соответствии с поставленной задачей — таблицы, схемы, графики, диаграммы, с использованием соответствующих программных средств обработки данных;
– формирование навыков и умений безопасного и целесообразного поведения при работе с компьютерными программами и в Интернете, умения соблюдать нормы информационной этики и права.

ФГОС С(П)ОО устанавливает требования к результатам освоения основной образовательной программы основного общего образования:

Личностные результаты:

– осознанный выбор будущей профессии и возможностей реализации собственных жизненных планов; отношение к профессиональной деятельности как возможности участия в решении личных, общественных, государственных, общенациональных проблем.

Метапредметные результаты:

– умение использовать средства информационных и коммуникационных технологий (далее – ИКТ) в решении когнитивных, коммуникативных и организационных задач с соблюдением требований эргономики,

техники безопасности, гигиены, ресурсосбережения, правовых и этических норм, норм информационной безопасности;

Предметные результаты:

Область «Математика и информатика»:

Изучение предметной области «Математика и информатика» должно обеспечить:

- сформированность умений применять полученные знания при решении различных задач;
- сформированность представлений о роли информатики и ИКТ в современном обществе, понимание основ правовых аспектов использования компьютерных программ и работы в Интернете;
- сформированность представлений о влиянии информационных технологий на жизнь человека в обществе; понимание социального, экономического, политического, культурного, юридического, природного, эргономического, медицинского и физиологического контекстов информационных технологий;
- принятие этических аспектов информационных технологий; осознание ответственности людей, вовлечённых в создание и использование информационных систем, распространение информации [18].

Предметные результаты изучения предметной области «Математика и информатика» включают предметные результаты изучения учебных предметов:

«Информатика» (базовый уровень) – требования к предметным результатам освоения базового курса информатики должны отражать:

- сформированность представлений о роли информации и связанных с ней процессов в окружающем мире;
- сформированность базовых навыков и умений по соблюдению требований техники безопасности, гигиены и ресурсосбережения при работе со средствами информатизации; понимание основ правовых

аспектов использования компьютерных программ и работы в Интернете [18].

«Информатика» (углубленный уровень) – требования к предметным результатам освоения углубленного курса информатики должны включать требования к результатам освоения базового курса и дополнительно отражать:

- владение системой базовых знаний, отражающих вклад информатики в формирование современной научной картины мира;
- сформированность представлений об устройстве современных компьютеров, о тенденциях развития компьютерных технологий; об общих принципах разработки и функционирования интернет-приложений;
- сформированность умения работать с библиотеками программ.

Из анализа ФГОС следует вывод о том, что тема «Основы криптографии» не представлена.

В учебнике «Информатика. 10 класс. Углубленный уровень» Полякова К.Ю., Еремина Е.А. представлены такие дидактические единицы: информационная безопасность, защита информации, средства защиты информации, понятие криптографии, понятие криптоанализа, понятие шифрования, ключ, виды ключей: открытый ключ, закрытый ключ, шифр Юлия Цезаря, шифр Вижинера, понятие о хэшировании, алгоритм RSA [6].

В учебнике «Информатика. 11 класс. Углубленный уровень в 2 частях» Полякова К.Ю., Еремина Е.А. сведений по криптографическим основам защиты информации не представлено [8].

В учебнике «Информатика. 10-11 класс» Семакина И.Г., Хеннера Е.К. представлены такие дидактические единицы: защищаемая информации, несанкционированное воздействие, понятие о криптографии, понятие ключа, шифр Юлия Цезаря [17].

В учебнике «Информатика. 7 класс ФГОС» Босовой Л.Л. представлены такие дидактические единицы: понятие кодирования информации, виды кодирования информации [2].

В учебнике «Информатика и ИКТ. 11 класс» Гейна А.Г. представлены такие дидактические единицы: понятие кодирования информации, виды кодирования информации [4].

В учебнике «Информатика и информационные технологии. 10-11 класс» Угриновича Н.Д. представлены такие дидактические единицы: кодирование информации, декодирование информации, кодирование текстовой, числовой и графической информации [12].

На основе анализа учебников можно сделать вывод о том, что криптографические основы защиты информации представлены только в учебниках Полякова К.Ю. и Семакина И.Г.. В этих учебниках рассматриваемая тема раскрывается достаточно поверхностно и недостаточно.

В программе по курсу «Информатика» для 7-9 классов (105 часов) Угриновича Н.Д. тема информационная безопасность раскрывается посредством изложения информации о правовой охране программ и данных, также о лицензионных, условно бесплатных и свободно распространяемых программах в объеме 3 часа для изучения в 7 и 9 классах [15].

В программе по курсу «Информатика» для 10-11 классов Угриновича Н.Д. тема информационная безопасность раскрывается посредством изложения информации о правовой охране программ и данных, международном праве в области информационной безопасности, средствах защиты информации в автоматизированных информационных системах, компьютерных сетях и компьютерах. На изучение данной темы выделено 5 часов в 10-11 классах [16].

В программе по курсу «Информатика» для 10-11 классов Семакина И.Г. представлена тема «Информационное право и безопасность» в объеме 2 часа [17].

На основе анализа рабочих программ, можно сделать вывод о том, что тема «Основы криптографии» предоставлено недостаточно и очень поверхностно.

2.2. Элективный курс «Основы криптографии»

Информационные технологии помогают человеку решать самые сложные проблемы. Но вместе с бурным развитием телекоммуникационных систем все острее встает вопрос о сохранности передаваемых с их помощью данных. Этим обуславливается широкое распространение криптографии и формирование такой отрасли как информационная безопасность. Поэтому появляется необходимость введения в школьный курс информатики элементов криптографии.

В настоящее время для защиты конфиденциальной информации применяются электронные шифровальные устройства. Для создания и обеспечения грамотной эксплуатации такой техники широко используются достижения современной криптографии, в основе которой лежат математика, информатика, электроника и другие науки.

На уроках предлагаемого элективного курса учащиеся будут знакомиться с основными понятиями криптографии и криптоанализа, решать занимательные задачи и знакомиться с простыми алгоритмами и способами шифрования. Такой подход позволит сформировать у учащихся стойкий интерес к предмету, приобрести навыки и умения в использовании криптографических алгоритмов.

Курс предложен для учащихся 10-11 классов продолжительностью 19 часов по 1 часу в неделю.

Цель курса – знакомство учащихся с основными понятиями криптографии и некоторыми методами шифрования.

Задачи курса:

Образовательные:

- получить общее представление о криптографии как науке;
- познакомиться с основными понятиями криптографии;
- познакомиться с историей развития криптографии;
- получить практические навыки использования некоторых алгоритмов шифрования с закрытым и открытым ключом.

Воспитательные:

- оценивать свои умения применять полученные знания при шифровании и расшифровке информации;
- принимать участие в обсуждении результатов деятельности других обучающихся по шифрованию и расшифровке информации;

Развивающие:

- развить творческие способности;
- анализировать работу других учащихся;
- развить мыслительные способности;
- обобщать и систематизировать полученные знания о криптографической защите информации;
- анализировать криптостойкость шифров.

Основная методическая установка курса – обучение школьников навыкам самостоятельной индивидуальной и групповой работы по криптографической защите информации. В задачи учителя входит создание условий для реализации ведущей подростковой деятельности – авторского действия, выраженного в проектных формах работы. На определенных этапах обучения учащиеся объединяются в группы, т.е. используется проектный метод обучения. В процессе работы предполагаются лекционные занятия, практические занятия, коллективные обсуждения, самостоятельная работа, работа в творческих группах. Выполнение проектов завершается публичной защитой результатов и рефлексией.

До изучения курса учащийся **должен**

Знать

- основные функции компьютера;
- технику безопасности работы за компьютером;
- понятия информации, кодирование информации, системы счисления;
- основы работы с текстовым редактором;

Уметь

- иметь базовый набор навыков работы с текстовым редактором;
- иметь базовые навыки по работе с простейшими арифметическими операциями над натуральными числами;
- иметь базовые навыки работы с двоичными числами.

По окончании курса учащиеся **должны**

Знать

- что такое криптография;
- история развития криптографии с древнейших времен;
- основные понятия криптографии и криптоанализа;
- математические основы шифрования с закрытым ключом;
- математические основы шифрования с открытым ключом;
- основные алгоритмы шифрования, использовавшиеся до XX века;
- основные современные алгоритмы шифрования;

Уметь

- применять основные алгоритмы шифрования с закрытым ключом;
- узнавать тип шифра;
- отличать виды использованных алгоритмов, примененных для шифрования определенного текста;
- развить коммуникативные качества в процессе групповой работы;
- чувствовать ответственность за выполненную работу;
- уметь самостоятельно работать над индивидуальным заданием;
- уметь увидеть свою работу глазами коллег по учебе за счет коллективной оценки каждой работы.

Курс завершается проведением итогового тестирования и презентацией проекта. Итоговый проект является формой текущего и итогового контроля, предполагающей выполнение учащимися индивидуальных и групповых заданий. Проект связан с созданием собственного шифра. В таблице 2 представлено тематическое планирование курса.

Таблица 2

Тематическое планирование курса

№ урока	Тема урока	Всего	Теория	Практика
1	Основные понятия криптографии	1	1	-
2	История развития криптографии	1	1	-
3	Методы шифрования с закрытым ключом	1	1	-
4	Шифр Юлия Цезаря	1	-	1
5	Пропорциональные шифры	1	-	1
6	Шифр Вижинера	1	-	1
7	Методы гаммирования	1	-	1
8	Методы перестановки с фиксированным периодом	1	-	1
9	Методы перестановки по таблице	1	-	1
10	Блочные шифры с закрытым ключом	1	1	-
11-12	Сеть Фейштеля	2	-	2
13-14	Методы шифрования с открытым ключом	2	2	-
15-16	Алгоритм RSA	2	-	2
17	Понятие о цифровой подписи	1	1	-
Итого:		17	7	10

Ниже представлено поурочное планирование.

Урок №1. Основные понятия криптографии (1 час).

Тип урока по ФГОС: урок усвоения новых знаний.

Вид урока: лекция.

Цели урока:

Знать

- Предмет и задачи криптографии.
- Применение криптографии в современном обществе.
- Основные определения.
- Реализация криптографических методов.
- Понятие о криптографических атаках.
- Пример простейшего шифра.

Уметь

- Использовать понятийный аппарат по данной теме.
- Приводить примеры применения криптографии в современном обществе.
- Приводить примеры реализации криптографических методов.

Основные понятия: криптография, криптоанализ, криптология, стеганография, шифр, шифрование, расшифрование, дешифрование, ключ, шифрование с закрытым ключом, шифрование с открытым ключом, механические шифровальные машины, аппаратные шифраторы, криптографические атаки.

Методические рекомендации: Учитель посредством презентации рассказывает об основных понятиях криптографии и ведет беседу с учениками, задавая им различные вопросы по теме.

Вопросы для контроля:

- Что такое криптография?
- Что такое шифрование?
- Что такое ключ?
- Что представляет собой процесс шифрования?

- Чем расшифровка отличается от дешифровки?
- Что представляла собой первая механическая шифровальная машина?
- Что такое аппаратные шифраторы?
- Кем могут проводиться криптографические атаки?

Урок №2. История развития криптографии (1 час).

Тип урока по ФГОС: урок усвоения новых знаний.

Вид урока: лекция.

Цели урока:

Знать

- Криптографические алгоритмы и устройства шифрования, применяемые в древности.
- Криптографические алгоритмы и устройства шифрования, применяемые в средние века.
- Современные криптографические алгоритмы и устройства шифрования.

Уметь

- Использовать понятийный аппарат по данной теме.
- Приводить примеры применения криптографии в древности, в средние века и в современное время.

Основные понятия: атбаш, шифр Цезаря, скитала, полибианский квадрат, магический квадрат, шифры перестановки и замены, шифр Вижинера, шифр Гронсфельда, тарабарская грамота, биграммные шифры, цилиндр Базери, Энигма, DES, IDEA.

Методические рекомендации: Учитель посредством презентации рассказывает об основных этапах развития криптографии и ведет беседу с учениками, задавая им различные вопросы по теме.

Вопросы для контроля:

- Какие криптографические алгоритмы и устройства шифрования были изобретены и применялись в древности?
- Какие криптографические алгоритмы и устройства шифрования были изобретены и применялись в средние века?
- Какие современные криптографические алгоритмы Вы знаете?

Урок №3. Методы шифрования с закрытым ключом (1 час).

Тип урока по ФГОС: урок усвоения новых знаний.

Вид урока: лекция.

Цели урока:

Знать

- Общий принцип работы методов шифрования с закрытым ключом.
- Виды методов шифрования с закрытым ключом.
- Понятие о методах замены.
- Понятие о методах перестановки.
- Примеры алгоритмов шифрования как методов замены.
- Примеры алгоритмов шифрования как методов перестановки.

Уметь

- Использовать понятийный аппарат по данной теме.
- Приводить примеры алгоритмов шифрования как методов замены.
- Приводить примеры алгоритмов шифрования как методов перестановки.

Основные понятия: шифрование с закрытым ключом, симметричное шифрование, методы замены, методы перестановки.

Методические рекомендации: Учитель посредством презентации рассказывает о методах шифрования с закрытым ключом и ведет беседу с учениками, задавая им различные вопросы по теме.

Вопросы для контроля:

- Поясните общую схему симметричного шифрования.
- Что общего имеют все методы шифрования с закрытым ключом?
- Назовите основные группы методов шифрования с закрытым ключом.
- Приведите примеры шифров замены.
- Сформулируйте общие принципы для методов шифрования заменой.
- В чем заключаются одноалфавитные подстановки?
- Приведите пример шифра одноалфавитной замены.

Урок №4. Шифр Юлия Цезаря (1 час)

Тип урока по ФГОС: урок рефлексии.

Вид урока: практикум.

Цели урока:

Знать

- Методы шифрования заменой.
- Понятие об одноалфавитной замене.
- Принцип дешифровки сообщений.
- Понятие о статических закономерностях языка.
- Понятие о криптостойкости алгоритма шифрования.
- Принцип работы алгоритма шифрования Юлия Цезаря.

Уметь

- Применять алгоритм шифрования Юлия Цезаря.
- Оценивать криптостойкость алгоритма шифрования.

Основные понятия: симметричное шифрование, одноалфавитная замена, дешифровка сообщений, статистические закономерности языка, криптостойкость алгоритма шифрования, алгоритм шифрования Юлия Цезаря.

Методические рекомендации: На данном уроке учитель является главным наблюдателем помощником, в задачу учителя входит корректировать действия ученика и помогать советами в выполнение задания.

Вопросы для контроля:

- Поясните общую схему симметричного шифрования.
- Что общего имеют все методы шифрования с закрытым ключом?
- Сформулируйте общие принципы для методов шифрования заменой.
- В чем заключается одноалфавитная замена?
- Приведите пример шифра одноалфавитной замены.

Практические работы: «Простейшие методы шифрования с закрытым ключом. Алгоритм Юлия Цезаря».

Урок №5. Пропорциональные шифры (1 час)

Тип урока по ФГОС: урок рефлексии.

Вид урока: практикум.

Цели урока:

Знать

- Методы шифрования заменой.
- Понятие об одноалфавитной замене.
- Принцип дешифровки сообщений.
- Принцип использования пропорциональных шрифтов.

Уметь

- Шифровать сообщения, используя пропорциональные шифры.
- Оценивать криптостойкость алгоритма шифрования.

Основные понятия: симметричное шифрование, одноалфавитная замена, дешифровка сообщений, криптостойкость алгоритма шифрования, пропорциональные шифры.

Методические рекомендации: На данном уроке учитель является главным наблюдателем помощником, в задачу учителя входит корректировать действия ученика и помогать советами в выполнение задания.

Вопросы для контроля:

- Поясните общую схему симметричного шифрования.
- Что общего имеют все методы шифрования с закрытым ключом?
- Сформулируйте общие принципы для методов шифрования заменой.
- В чем заключается одноалфавитная замена?
- Приведите пример использования пропорционального шифра.

Практические работы: «Простейшие методы шифрования с закрытым ключом. Пропорциональные шифры».

Урок №6. Шифр Вижинера (1 час)

Тип урока по ФГОС: урок рефлексии.

Вид урока: практикум.

Цели урока:

Знать

- Методы шифрования заменой.
- Понятие о многоалфавитной замене.
- Принцип дешифровки сообщений.
- Принцип использования алгоритмов многоалфавитной замены.
- Принцип использования шифра Вижинера

Уметь

- Шифровать сообщения, используя алгоритм Вижинера.
- Оценивать криптостойкость алгоритма шифрования.

Основные понятия: симметричное шифрование, многоалфавитная замена, дешифровка сообщений, криптостойкость алгоритма шифрования, шифр Вижинера.

Методические рекомендации: На данном уроке учитель является главным наблюдателем помощником, в задачу учителя входит корректировать действия ученика и помогать советами в выполнение задания.

Вопросы для контроля:

- Поясните общую схему симметричного шифрования.
- Что общего имеют все методы шифрования с закрытым ключом?
- Сформулируйте общие принципы для методов шифрования заменой.
- В чем заключается многоалфавитная замена?
- Приведите пример использования шифра Вижинера.

Практические работы: «Простейшие методы шифрования с закрытым ключом. Многоалфавитная замена».

Урок №7. Методы гаммирования (1 час)

Тип урока по ФГОС: урок рефлексии.

Вид урока: практикум.

Цели урока:

Знать

- Методы шифрования заменой.
- Понятие о многоалфавитной замене.
- Понятие гаммирования.
- Принцип дешифровки сообщений.
- Принцип использования метода гаммирования.

Уметь

- Шифровать сообщения, используя метод гаммирования.

- Оценивать криптостойкость метода гаммирования.

Основные понятия: симметричное шифрование, многоалфавитная замена, дешифровка сообщений, криптостойкость алгоритма шифрования, метод гаммирования.

Методические рекомендации: На данном уроке учитель является главным наблюдателем помощником, в задачу учителя входит корректировать действия ученика и помогать советами в выполнение задания.

Вопросы для контроля:

- Поясните общую схему симметричного шифрования.
- Что общего имеют все методы шифрования с закрытым ключом?
- Сформулируйте общие принципы для методов шифрования заменой.
- В чем заключается многоалфавитная замена?
- Приведите пример использования метода гаммирования.

Практические работы: «Простейшие методы шифрования с закрытым ключом. Метод гаммирования».

Урок №8. Методы перестановки с фиксированным периодом (1 час)

Тип урока по ФГОС: урок рефлексии.

Вид урока: практикум.

Цели урока:

Знать

- Методы шифрования перестановкой.
- Понятие о методе шифрования перестановкой с фиксированным периодом.
- Принцип дешифровки сообщений.
- Принцип использования метода перестановки с фиксированным периодом.

Уметь

- Шифровать сообщения, используя метод перестановки.
- Оценивать криптостойкость метода шифрования перестановкой.

Основные понятия: симметричное шифрование, методы перестановки, дешифровка сообщений, криптостойкость алгоритма шифрования, метод перестановки с фиксированным периодом.

Методические рекомендации: На данном уроке учитель является главным наблюдателем помощником, в задачу учителя входит корректировать действия ученика и помогать советами в выполнение задания.

Вопросы для контроля:

- Поясните общую схему симметричного шифрования.
- Что общего имеют все методы шифрования с закрытым ключом?
- Сформулируйте общие принципы для методов шифрования перестановкой.
- Приведите пример использования метода шифрования перестановкой с фиксированным периодом.

Практические работы: «Простейшие методы шифрования с закрытым ключом. Метод перестановки с фиксированным периодом».

Урок №9. Методы перестановки по таблице (1 час)

Тип урока по ФГОС: урок рефлексии.

Вид урока: практикум.

Цели урока:

Знать

- Методы шифрования перестановкой.
- Понятие о методе шифрования перестановкой по таблице.
- Принцип дешифровки сообщений.
- Принцип использования метода перестановки по таблице.

Уметь

- Шифровать сообщения, используя метод перестановки по таблице.
- Оценивать криптостойкость метода шифрования перестановкой.

Основные понятия: симметричное шифрование, методы перестановки, дешифровка сообщений, криптостойкость алгоритма шифрования, метод перестановки по таблице.

Методические рекомендации: На данном уроке учитель является главным наблюдателем помощником, в задачу учителя входит корректировать действия ученика и помогать советами в выполнение задания.

Вопросы для контроля:

- Поясните общую схему симметричного шифрования.
- Что общего имеют все методы шифрования с закрытым ключом?
- Сформулируйте общие принципы для методов шифрования перестановкой.
- Приведите пример использования метода шифрования перестановкой по таблице.

Практические работы: «Простейшие методы шифрования с закрытым ключом. Метод перестановки по таблице».

Урок №10. Блочные шифры с закрытым ключом (1 час)

Тип урока по ФГОС: урок усвоения новых знаний.

Вид урока: лекция.

Цели урока:

Знать

- Понятие о комбинированном шифре.
- Понятие о блочном шифре.

- Понятие об операциях, используемых в блочных алгоритмах шифрования.

Уметь

- Применять операции побитового сложения по модулю 2, побитового сложения по модулю 2^16, побитового сложения по модулю 2^32, циклического сдвига.

Основные понятия: симметричное шифрование, комбинированный шифр, блочный шифр, операция побитового сложения, операция побитового сложения по модулю 2, операция побитового сложения по модулю 2^16, операция побитового сложения по модулю 2^32, операция циклического сдвига.

Методические рекомендации: Учитель посредством презентации рассказывает о блочных шифрах с открытым ключом и ведет беседу с учениками, задавая им различные вопросы по теме.

Вопросы для контроля:

- В чем особенности блочного шифра?
- Как применить операцию побитового сложения для двоичных чисел?
- Как применить операцию побитового сложения по модулю 2 для двоичных чисел?
- Как применить операцию побитового сложения по модулю 2^16 для двоичных чисел?
- Как применить операцию побитового сложения по модулю 2^32?
- Как применить операцию циклического сдвига для двоичных чисел?

Практические работы: «Блочные шифры с закрытым ключом. Операции, используемые в блочных алгоритмах шифрования».

Урок №11-12. Сеть Фейштеля (2 часа)

Тип урока по ФГОС: урок рефлексии.

Вид урока: практикум.

Цели урока:

Знать

- Понятие о блочном шифре.
- Понятие о сети Фейштеля.
- Особенности работы алгоритма сети Фейштеля.

Уметь

- Применять сеть Фейштеля для шифрования данных.

Основные понятия: симметричное шифрование, комбинированный шифр, блочный шифр, операция побитового сложения, операция побитового сложения по модулю 2, операция XOR, сеть Фейштеля.

Методические рекомендации: На данном уроке учитель является главным наблюдателем помощником, в задачу учителя входит корректировать действия ученика и помогать советами в выполнение задания.

Вопросы для контроля:

- В чем особенности блочного шифра?
- Как применить операцию XOR для двоичных чисел?
- Как применить алгоритм сети Фейштеля для шифрования данных?

Практические работы: «Блочные шифры с закрытым ключом. Сеть Фейштеля».

Урок №13-14. Методы шифрования с открытым ключом (2 часа)

Тип урока по ФГОС: урок усвоения новых знаний.

Вид урока: лекция.

Цели урока:

Знать

- Предпосылки создания методов шифрования с открытым ключом.
- Основные понятия шифрования с открытым ключом.
- Требования к алгоритмам шифрования с открытым ключом.
- Понятия простого и составного числа.
- Понятие операции взятия остатка по модулю n.

Уметь

- Использовать понятийный аппарат по данной теме.
- Приводить примеры простых и составных чисел.
- Применять операцию взятия остатка по модулю n.

Основные понятия: шифрование с открытым ключом, простое число, составное число, операция взятия остатка по модулю n.

Методические рекомендации: Учитель посредством презентации рассказывает об особенностях шифрования с открытым ключом и ведет беседу с учениками, задавая им различные вопросы по теме.

Вопросы для контроля:

- По какой причине были созданы алгоритмы шифрования с открытым ключом?
- Какие требования предъявляются к алгоритмам шифрования с открытым ключом?
- Какое число называется простым?
- Какое число называется составным?
- Как применить операцию взятия остатка по модулю n?

Урок №15-16. Алгоритм RSA (2 часа)

Тип урока по ФГОС: урок рефлексии.

Вид урока: практикум.

Цели урока:

Знать

- Понятие об открытом и закрытом ключе.
- Основные сведения об алгоритме RSA.
- Последовательность действий при шифровании информации в алгоритме RSA.

Уметь

- Шифровать сообщения, используя алгоритм RSA.
- Оценивать криптостойкость метода шифрования.

Основные понятия: закрытый ключ, открытый ключ, шифрование с открытым ключом, криптостойкость алгоритма шифрования, дешифровка сообщений, алгоритм RSA, простое число, операция взятия остатка по модулю n.

Методические рекомендации: На данном уроке учитель является главным наблюдателем помощником, в задачу учителя входит корректировать действия ученика и помогать советами в выполнение задания.

Вопросы для контроля:

- Что такое закрытый ключ?
- Что такое открытый ключ?
- В чем особенность шифрования с открытым ключом?
- Для каких целей может применяться алгоритм RSA?
- Оцените криптостойкость алгоритма RSA.
- Опишите процесс шифрования с использованием алгоритма RSA.

Практические работы: «Шифрование с открытым ключом. Алгоритм RSA».

Урок №17. Понятие о цифровой подписи (1 час)

Тип урока по ФГОС: урок усвоения новых знаний.

Вид урока: лекция.

Цели урока:

Знать

- Понятие цифровой подписи.
- Общая схема создания цифровой подписи.
- Обща схема проверки цифровой подписи.

Уметь

- Использовать понятийный аппарат по данной теме.
- Приводить примеры применения цифровой подписи.
- Объяснять общую схему создания цифровой подписи.
- Объяснять общую схему проверки цифровой подписи.

Основные понятия: цифровая подпись.

Методические рекомендации: Учитель посредством презентации рассказывает об особенностях использования цифровой подписи и ведет беседу с учениками, задавая им различные вопросы по теме.

Вопросы для контроля:

- Что такое цифровая подпись?
- Назовите сферы применения цифровой подписи.
- Какова общая схема создания цифровой подписи?
- Какова общая схема проверки цифровой подписи?

2.3.Описание программно-методической поддержки элективного курса

В качестве программно-методической поддержки были разработаны учебное пособие и программа, реализующая следующие алгоритмы шифрования: шифр Юлия Цезаря, шифр Вижинера, сеть Фейштеля и алгоритм шифрования с открытым ключом RSA.

Учебное пособие было разработано с использованием CMS WordPress и располагается по адресу http://cryptographylife.ru/.

На рисунке 14 представлена главная страница учебного пособия.

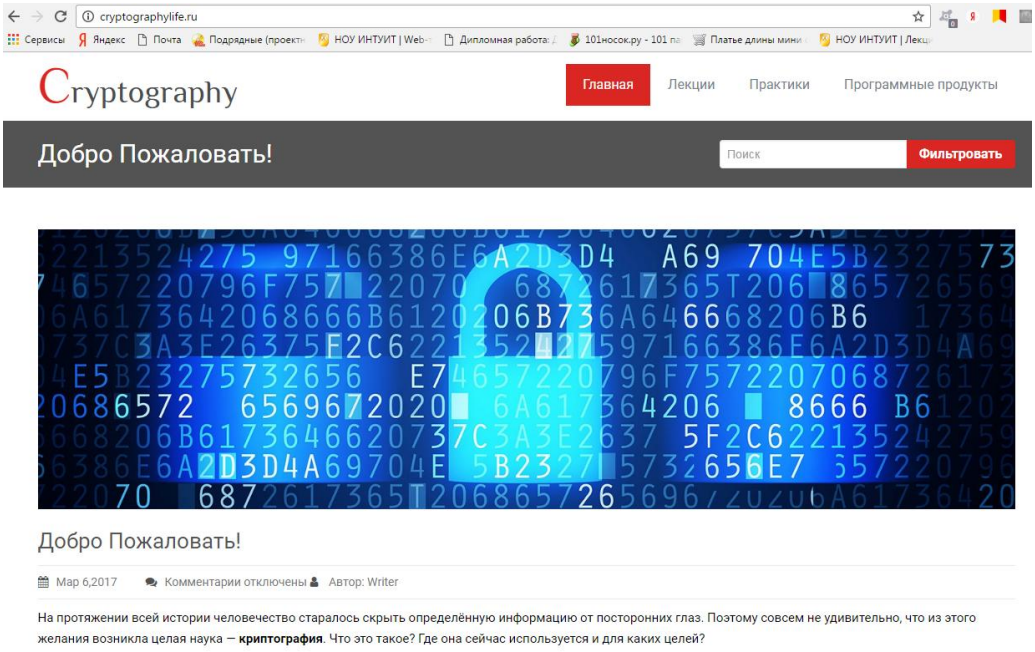


Рис. 14. Главная страница учебного пособия

В верхней части главной страницы располагается меню сайта.

С помощью пункта меню Лекции можно перейти на страницу с содержимым лекционного материала (рисунок 15).

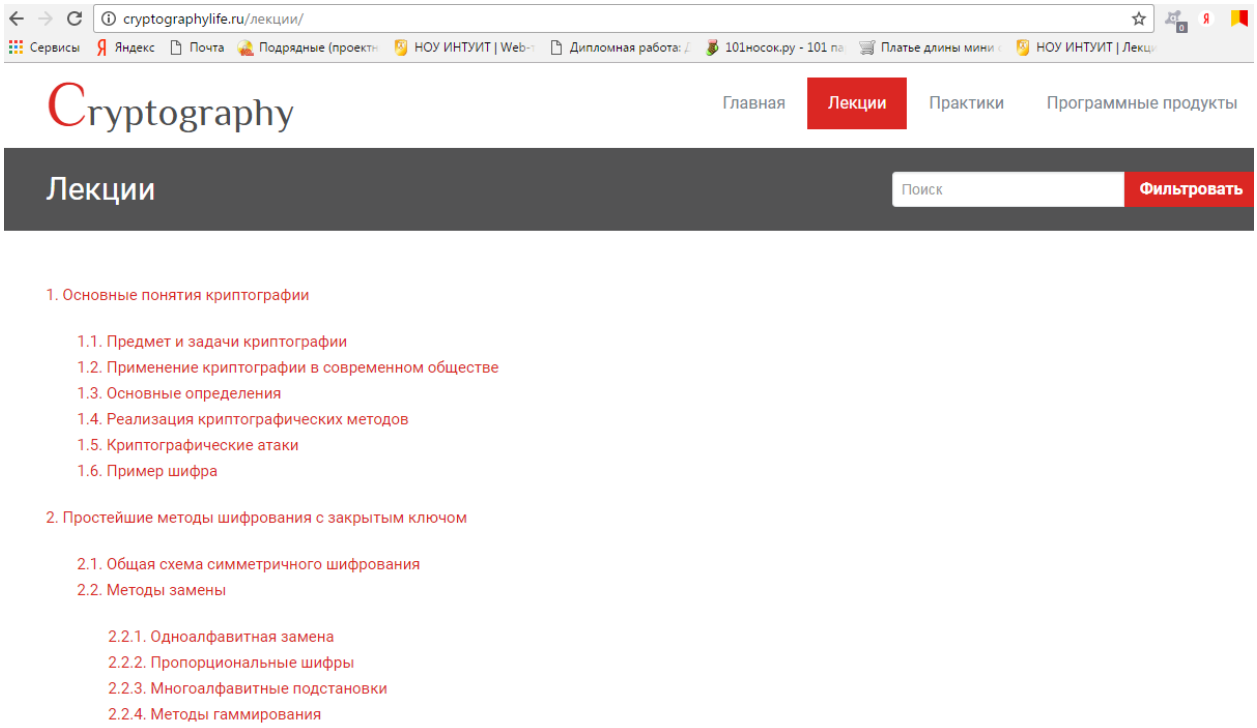
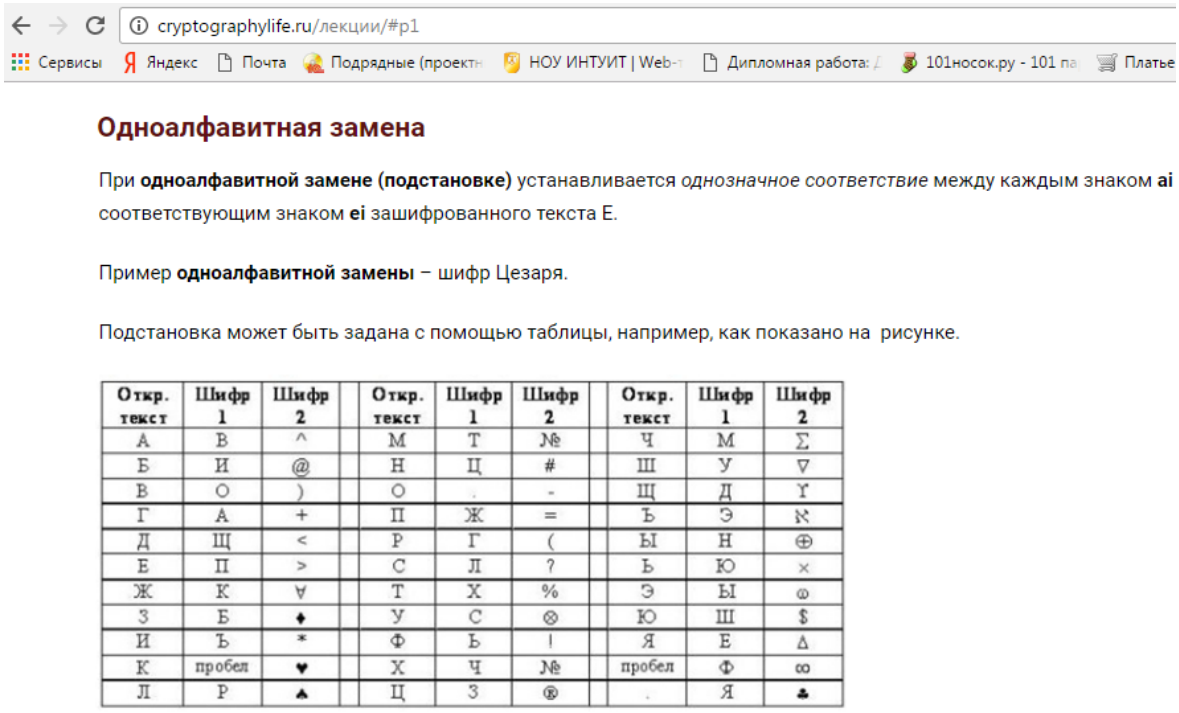


Рис. 15. Содержимое страницы Лекции

Содержимое лекционного материала представлено в виде гиперссылок, с помощью которых можно перейти на страницы сайта, отображающие

соответствующий материал. Например, на рисунке 16 изображена страница учебного пособия, отражающая одну из лекций элективного курса.



Откр. текст	Шифр 1	Шифр 2	Откр. текст	Шифр 1	Шифр 2	Откр. текст	Шифр 1	Шифр 2
А	В	^	М	Т	№	Ч	М	Σ
Б	И	@	Н	Ц	#	Ш	У	∇
В	О	)	О	.	-	Щ	Д	ϒ
Г	А	+	П	Ж	=	Ъ	Э	ℵ
Д	Щ	<	Р	Г	(	Ы	Н	⊕
Е	П	>	С	Л	?	Ь	Ю	×
Ж	К	∀	Т	Х	%	Э	Ы	∅
З	Б	♦	У	С	⊗	Ю	Ш	$
И	Ъ	*	Ф	Ь	!	Я	Е	Δ
К	пробел	♥	Х	Ч	№	пробел	Ф	∞
Л	Р	♠	Ц	З	®	.	Я	♣

Рис. 16. Содержимое страницы, отражающей материал лекции элективного курса

С помощью пункта меню Практики, изображенного на рисунке 17, можно ознакомиться с содержимым практических занятий по темам элективного курса.

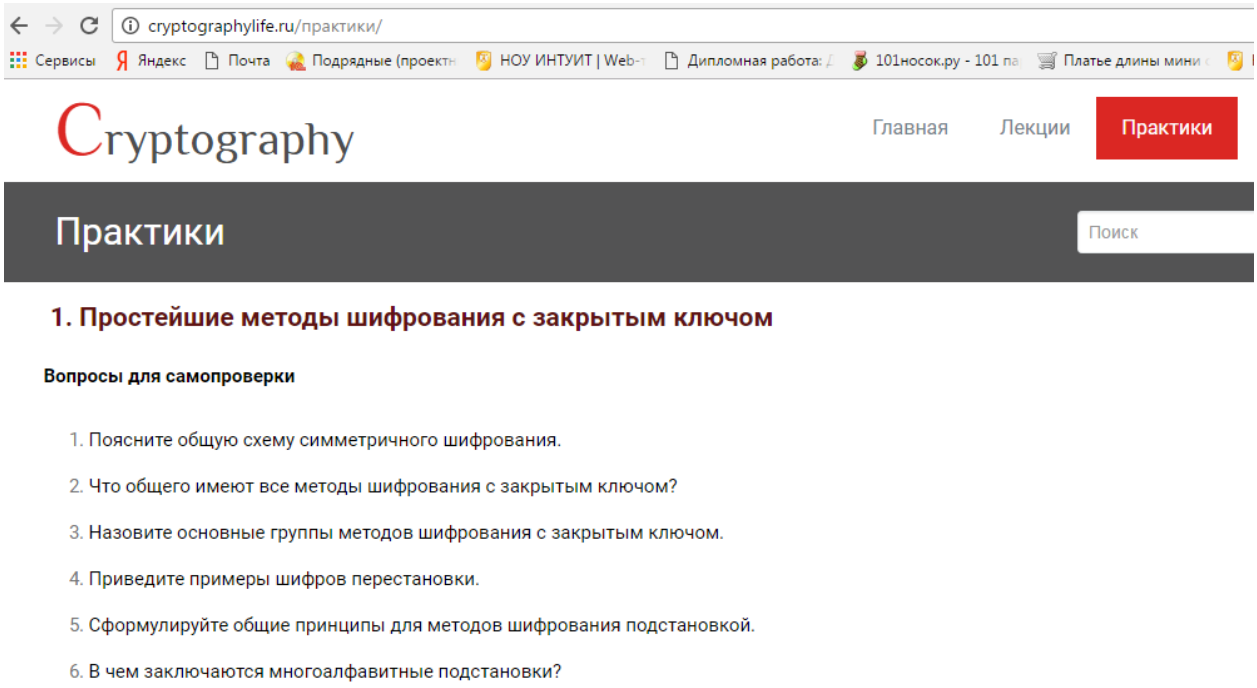


Рис. 17. Содержимое страницы, отражающей материал практического занятия элективного курса

Для скачивания программы, демонстрирующей алгоритмы шифрования, необходимо зайти на страницу Программные продукты сайта. Далее необходимо щелкнуть по гиперссылке Программа! (рисунок 18).

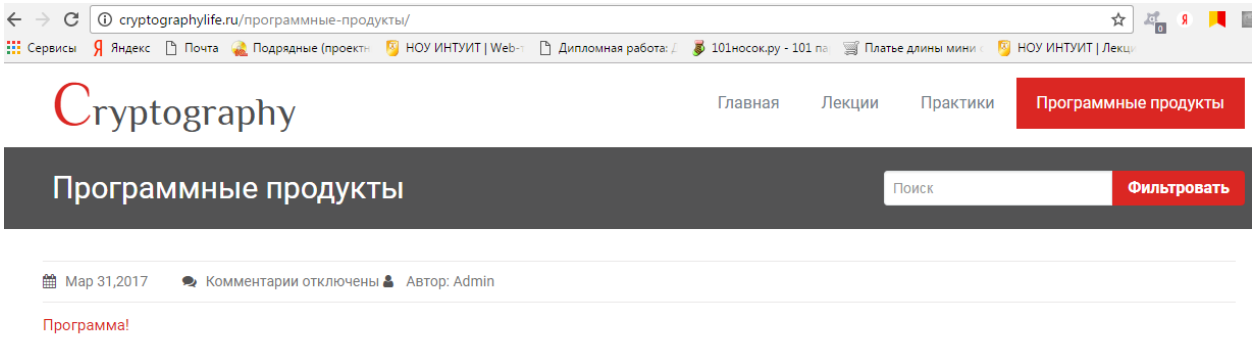


Рис. 18. Содержимое страницы для скачивания программы, демонстрирующей алгоритмы шифрования

Щелчок по гиперссылке Программы! Приведет к копированию на компьютер пользователя архивного файла crypt.rar. Для ознакомления с программой необходимо распаковать архив crypt.rar и запустить программу Криптографические алгоритмы.exe, интерфейс которой показан на рисунке 19.

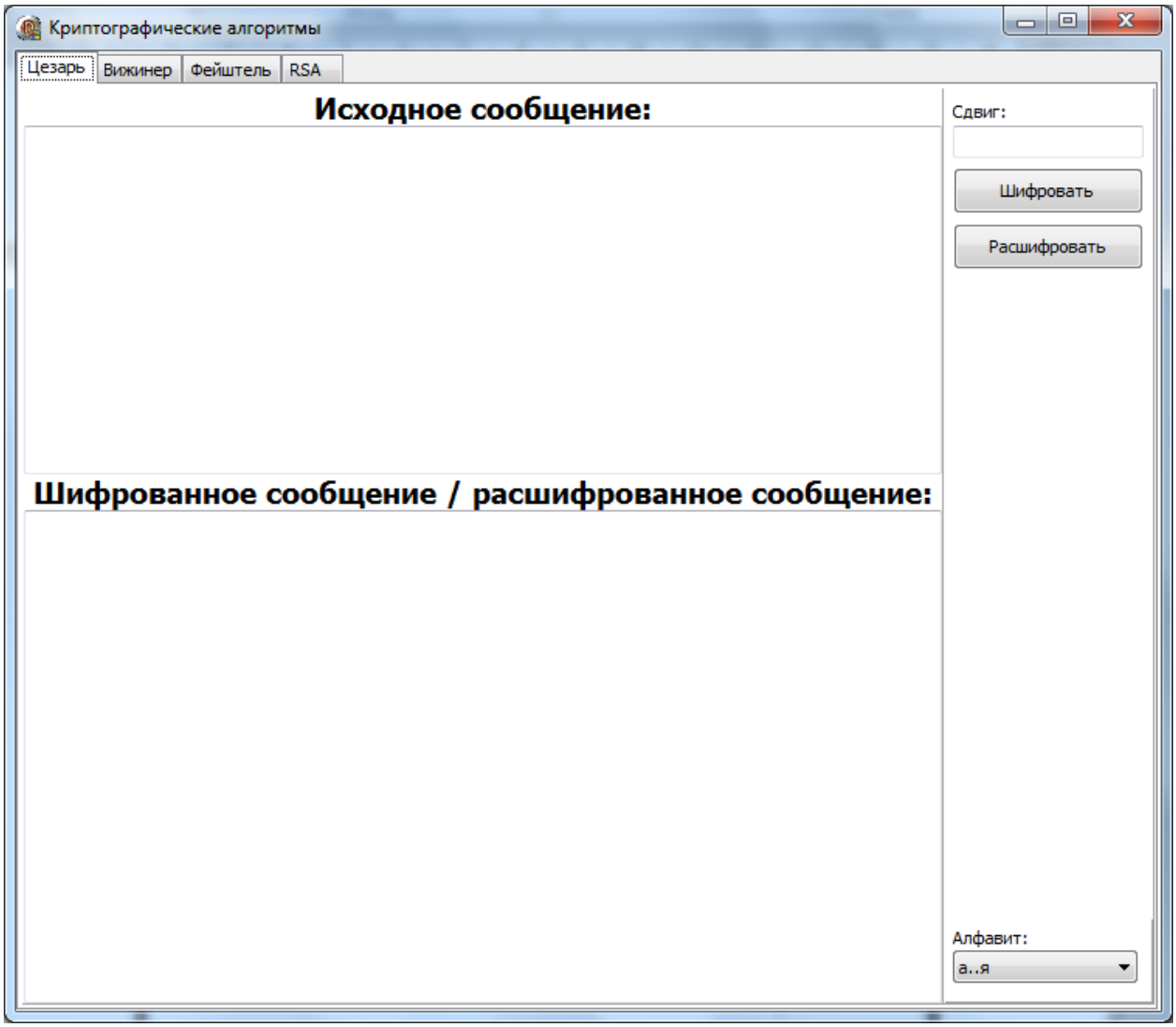


Рис. 19. Внешний вид программы Криптографические алгоритмы.exe

С помощью программы Криптографические алгоритмы.exe реализовано шифрование и расшифрование сообщений по алгоритмам Юлия Цезаря, Вижинера, Фейштеля и RSA.

Для шифрования сообщения по методу Юлия Цезаря необходимо открыть закладку Цезарь, в поле ввода для исходного сообщения ввести информацию, необходимую для шифрования, также в строку Сдвиг ввести значение сдига (рисунок 20). При этом для сдвига используется вся таблица символов Unicode размером 65536 символов. Рассмотрение всей таблицы символов Unicode является более универсальным подходом, так как позволяет шифровать в сообщении символы пробелов, запятых точек и т.п. На этой же закладке можно осуществить расшифровку зашифрованного сообщения.

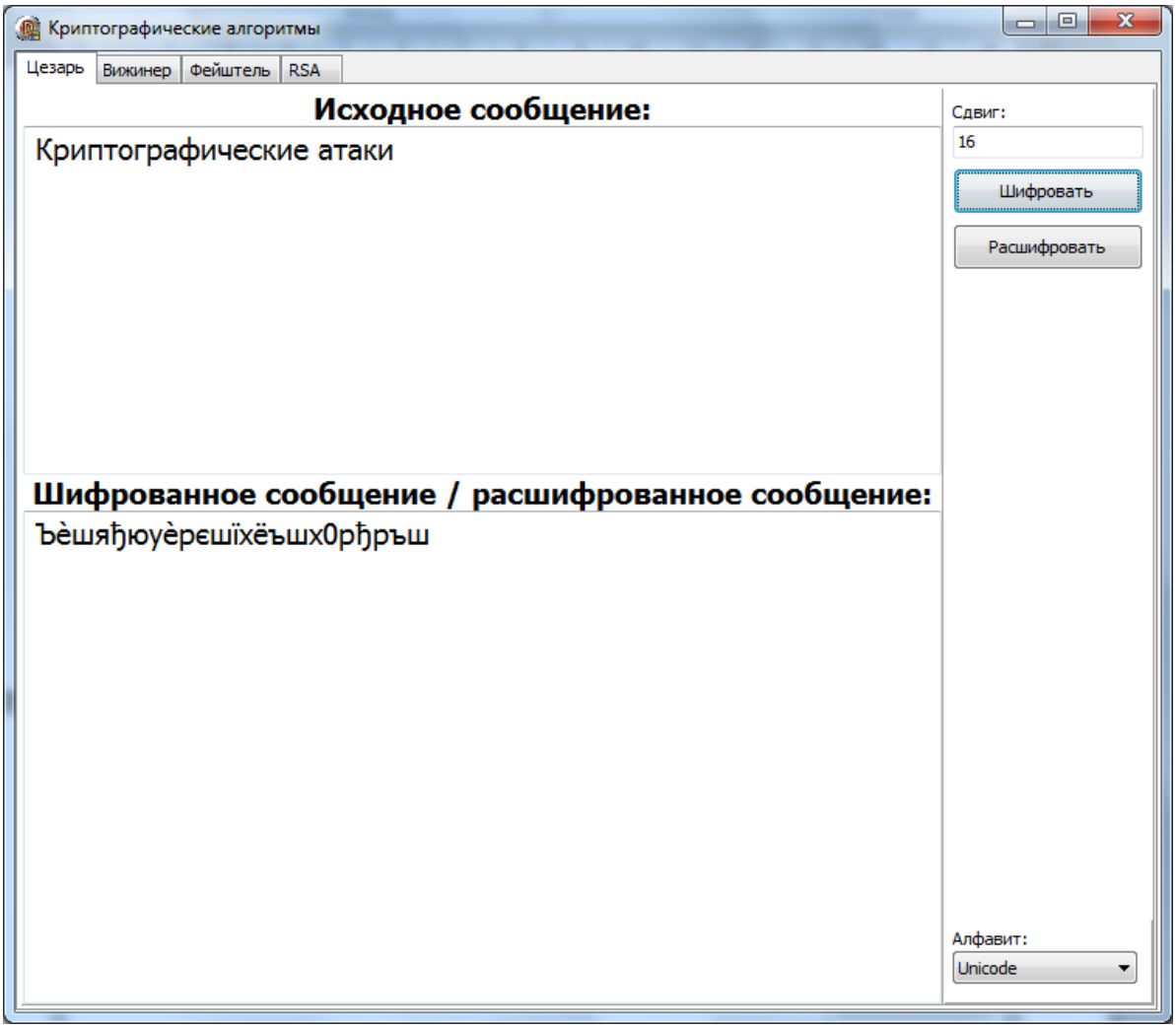


Рис. 20. Пример шифрования исходного сообщения по методу Юлия Цезаря с использованием кодировки Unicode

С помощью списка Алфавит закладки Цезарь можно выбрать набор символов русского алфавита и аналогично протестировать программу (рисунок 21).

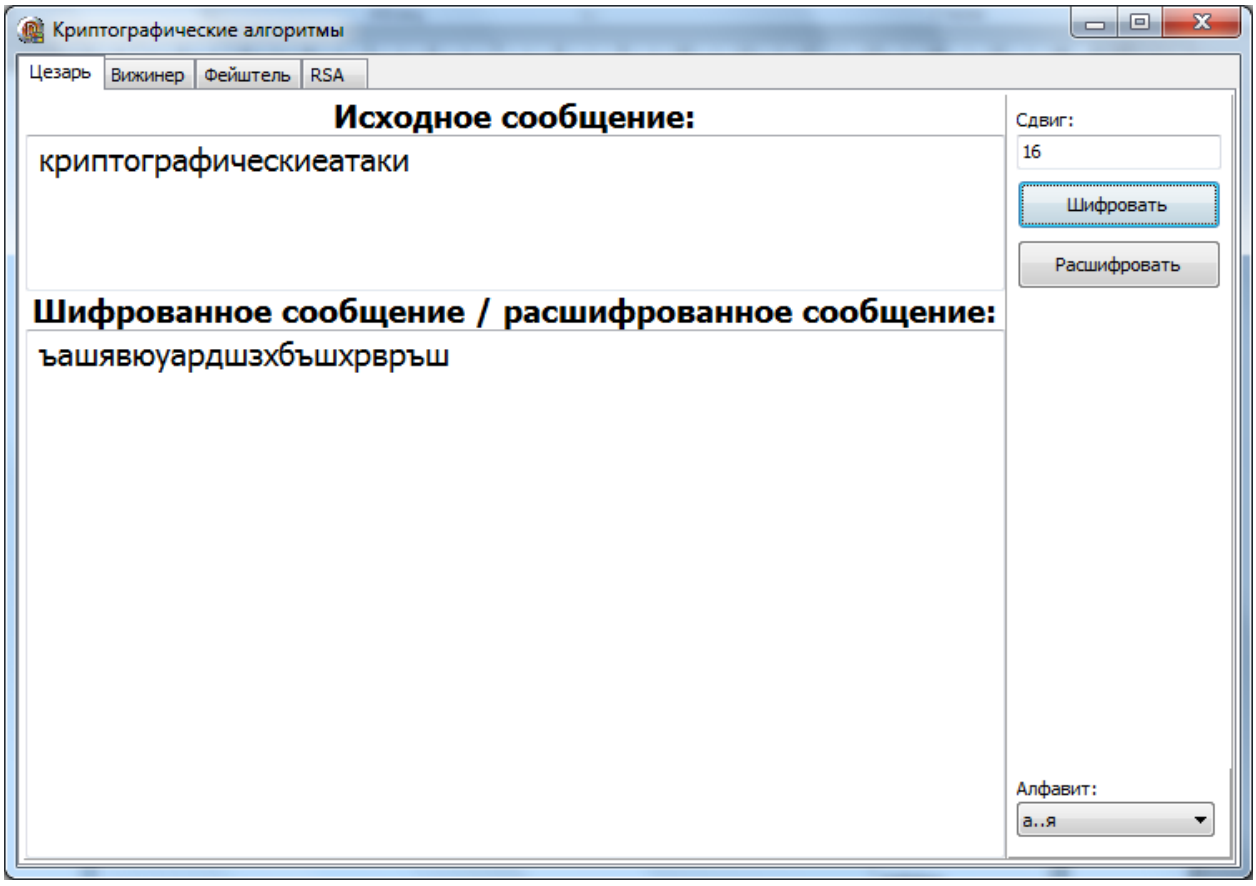


Рис. 21. Пример шифрования исходного сообщения по методу Юлия Цезаря с использованием набора символов русского алфавита

Для шифрования сообщения по методу Вижинера необходимо открыть закладку Вижинер, в поле ввода для исходного сообщения ввести информацию, необходимую для шифрования, также в строку Ключ ввести значение ключа – им может быть любое слово (рисунок 22). При этом для шифрования используется вся таблица символов Unicode размером 65536 символов. Рассмотрение всей таблицы символов Unicode является более универсальным подходом, так как позволяет шифровать в сообщении символы пробелов, запятых точек и т.п. На этой же закладке можно осуществить расшифровку зашифрованного сообщения.

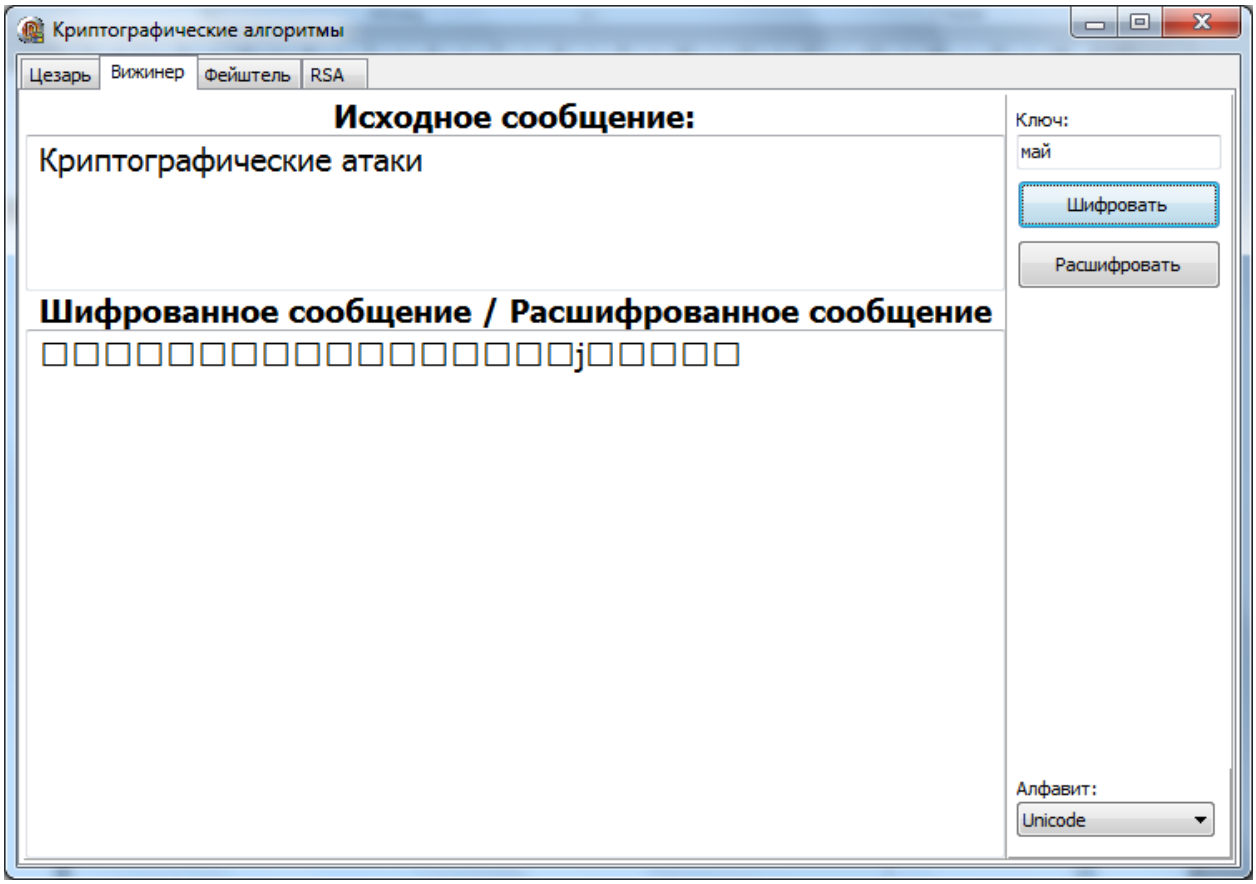


Рис. 22. Пример шифрования исходного сообщения по методу Вижинера с использованием кодировки Unicode

С помощью списка Алфавит закладки Вижинер можно выбрать набор символов русского алфавита и аналогично протестировать программу (рисунок 23).

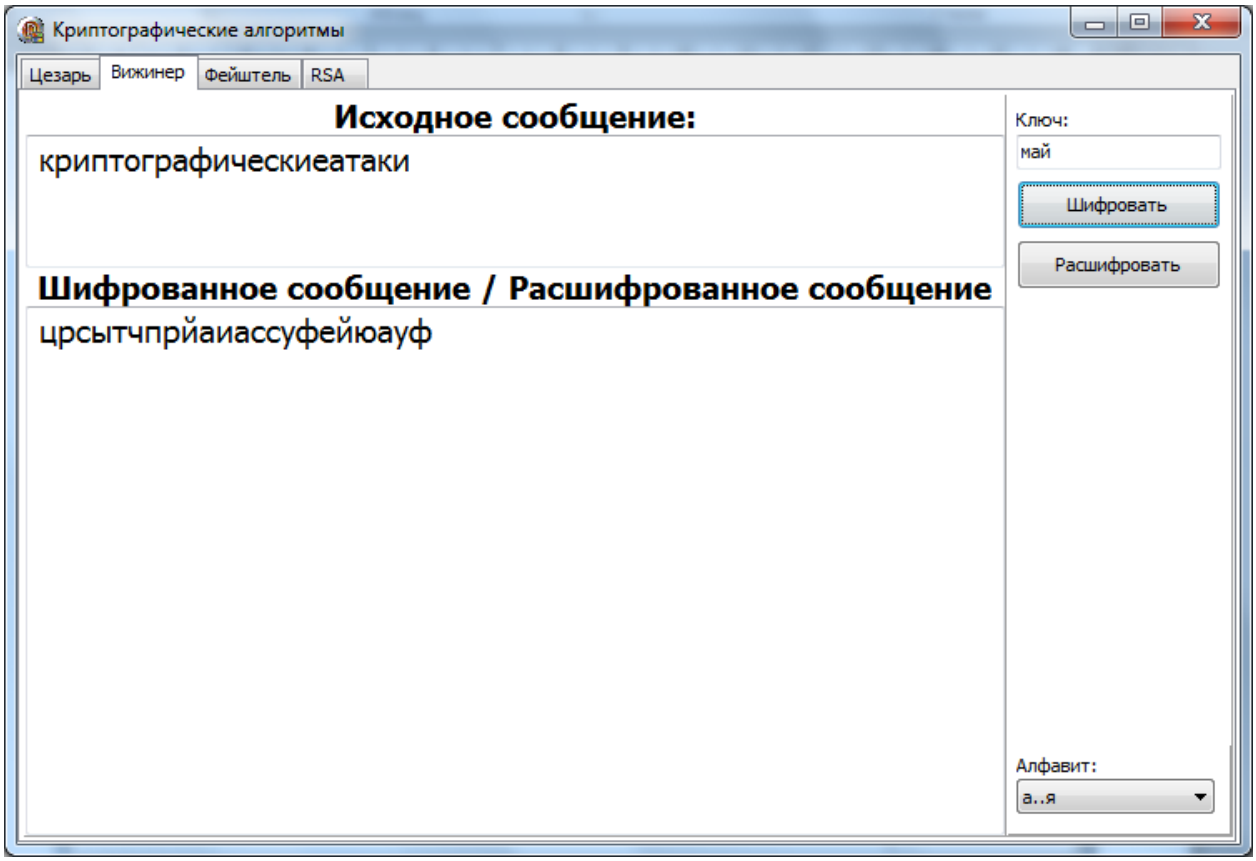


Рис. 23. Пример шифрования исходного сообщения по методу Вижинера с использованием набора символов русского алфавита

Для шифрования сообщения по методу Фейштеля необходимо открыть закладку Фейштель, в поле ввода для исходного сообщения ввести информацию, необходимую для шифрования, также в строку Количество итераций ввести соответствующее числовое значение (рисунок 24). При этом для шифрования используется вся таблица символов Unicode размером 65536 символов. Рассмотрение всей таблицы символов Unicode является более универсальным подходом, так как позволяет шифровать в сообщении символы пробелов, запятых точек и т.п. На этой же закладке можно осуществить расшифровку зашифрованного сообщения.

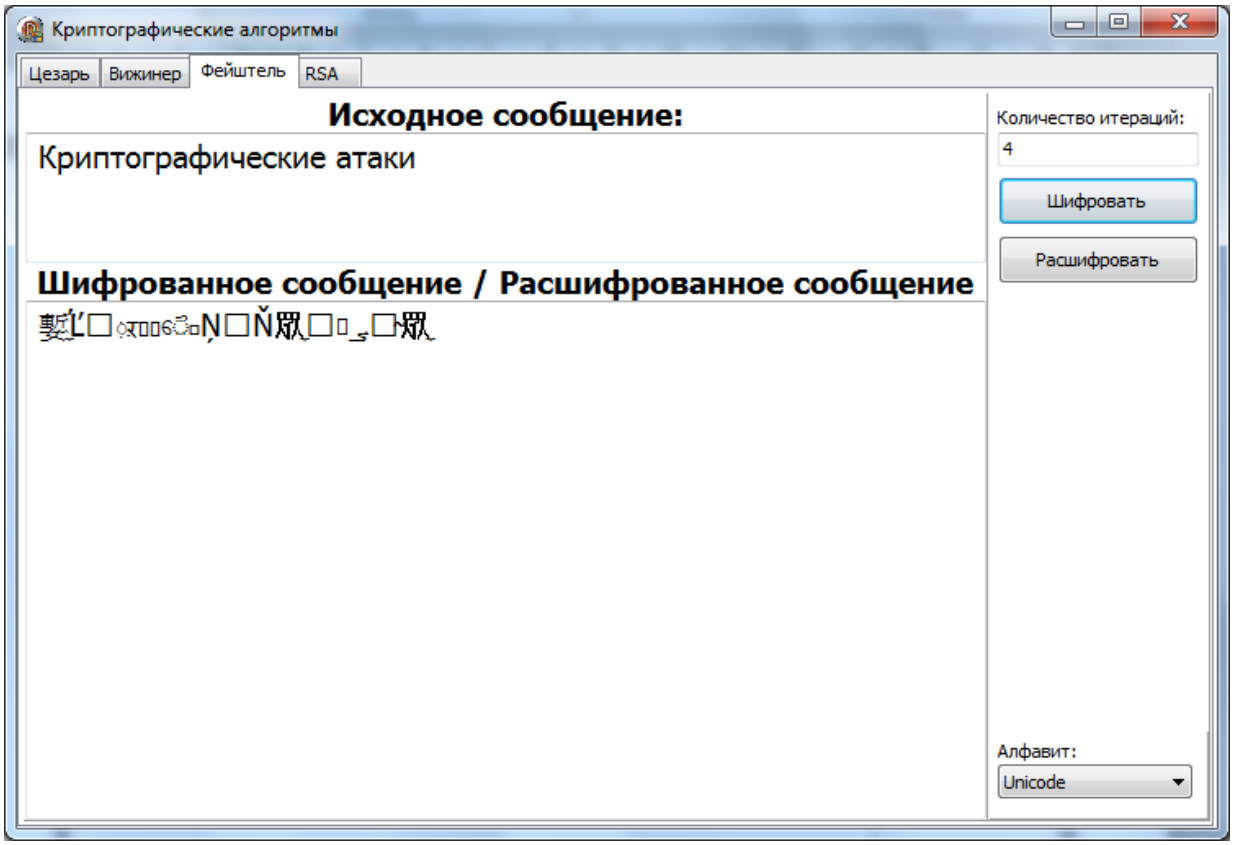


Рис. 24. Пример шифрования исходного сообщения по методу Фейштеля

Для шифрования сообщения по алгоритму RSA необходимо открыть закладку RSA, далее с помощью списков выбрать значения для простых чисел p и q, а также открытого и закрытого ключа (рисунок 25). Затем ввести исходное сообщение и нажать на кнопку Шифровать. На этой же закладке можно осуществить расшифровку зашифрованного сообщения.

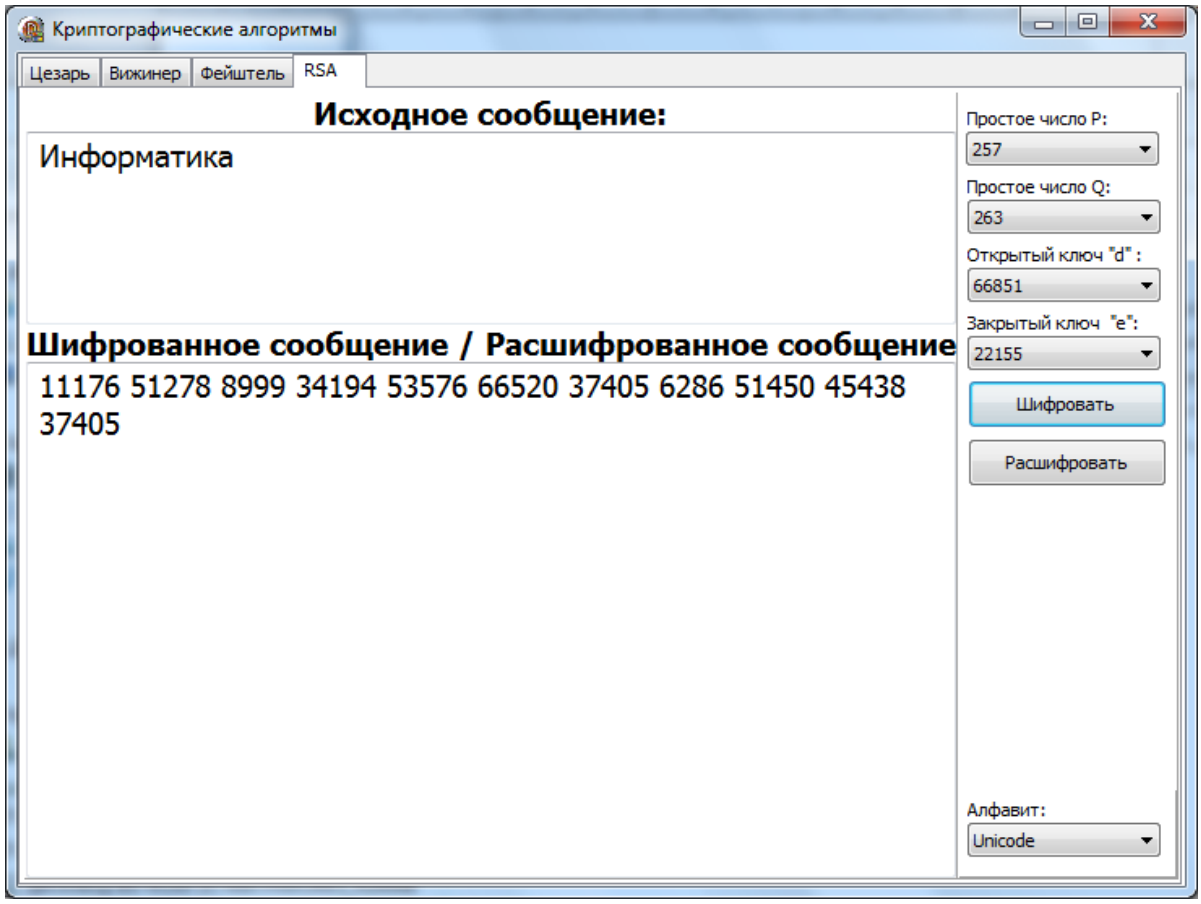


Рис. 25. Пример шифрования исходного сообщения по алгоритму RSA

2.4. Апробация результатов исследования в школе

Педагогическая апробация проводилась во время педагогической практики в МБОУ «Средняя общеобразовательная школа №2» Еманжелинского муниципального района Челябинской области. Курс изучался в общеобразовательном классе. В течение трех занятий были рассмотрены темы:

1. Урок №1 Основные понятия криптографии – 1 час.
2. Урок №2 Методы шифрования с закрытым ключом – 1 час.
3. Урок №3 Шифр Вижинера – 1 час.

Апробация элективного курса прошла успешно. Этому способствовал большой интерес учеников к данной теме еще до проведения курса.

Темы курса оказались новыми для учащихся. Ребята оказались современными, они знали, что во многих сферах жизни применяется шифрование, поэтому каждый урок был заряжен позитивным настроением.

Ученики хорошо усвоили многоалфавитное шифрование методом Вижинера. Так же ученикам было интересно познакомиться с историей криптографии. Наибольший интерес у учеников вызвал урок, на котором они применяли метод шифрования практически.

Выводы по главе 2

На основе теоретических положений, изложенных в первой главе, во второй главе представлено описание элективного курса «Основы криптографии» для учеников 10-11 классов, включающего методическую поддержку в виде электронного пособия, а также демонстрационной программы, реализующей следующие алгоритмы шифрования: шифр Юлия Цезаря, шифр Вижинера, сеть Фейштеля и алгоритм шифрования с открытым ключом RSA.

Апробация курса проводилась в рамках педагогической практики в МБОУ «Средняя общеобразовательная школа №2» Еманжелинского муниципального района Челябинской области. На занятиях ученики 10 классов с удовольствием выполняли задания.

Таким образом, во второй главе исследования мы разработали и апробировали элективный курс «Основы криптографии» и программно-методическую поддержку к нему.

ЗАКЛЮЧЕНИЕ

Подводя итоги данной работы, следует отметить, что проведенное исследование направлено на изучение теоретических положений по основам криптографической обработки информации, разработку элективного курса и программно-методической поддержки названного курса.

В процессе исследования были выполнены поставленные задачи и получены следующие результаты:

1. Изучены теоретические положения по проблеме исследования, в школьном курсе данная тема рассматривается очень скудно.

2. Разработан 17-ти часовой элективный курс и адаптирован как школьный элективный курс по изучению основ криптографической обработки информации в школе для 10-11 классов.

3. Разработана программно-методическая поддержка элективного курса в виде сайта, созданного с помощью CMS WordPress. Также разработана программа, демонстрирующая работу следующих алгоритмов шифрования: шифр Юлия Цезаря, шифр Вижинера, сеть Фейштеля и алгоритм шифрования с открытым ключом RSA

В подтверждении гипотезы можно сказать, что данный курс позволяет поднять уровень компетентности учащихся в области защиты информации.

Таким образом, поставленные задачи можно считать выполненными и можно сделать вывод о верности поставленной гипотезы.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Басалова, Г. В. Основы криптографии [Текст]: Уч. Пособие / Г.В. Басалова – Тула: Тульский госуниверситет, 2009. — 145 с.

2. Босова, Л. , Босова А. Информатика. [Текст]: Учебник для 7 класса / Л. Бо-сова, А. Босова–М.:БИНОМ. Лаборатория знаний, 2013. – 224с.

3. Гейн, А., Юнерман Н. Информатика. [Текст]: Учебник для 9 класса / А. Гейн, Н. Юнерман.: Просвещение, 2014. – 142с.

4. Гейн, А., Сенокосов А.. Информатика и ИКТ. [Текст]: Учебник для 11 клас-са общеобразовательное учреждение: базовый и профильный уровень / А. Гейн, А. Сенокосов.: Просвещение, 2009. – 336с.

5. Панасенко, С.П. Алгоритмы шифрования. Специальный справочник [Текст] / С.П.Панасенко – СПб.: БХВ-Петербург, 2009. - 576 с.: ил.

6. Поляков К. , Еремин Е. Информатика. Углубленный уровень. [Текст]: Учеб-ник для 10 класс. / К. Поляков, Е. Еремин. –М.:БИНОМ. Лаборатория зна-ний, 2013. – 304с.

7. Поляков, К., Еремин Е. Информатика. Углубленный уровень. [Текст]: Учеб-ник для 10 класса: в 2 ч. Ч.2 . / К. Поляков, Е. Еремин. – М.:БИНОМ. Лаборатория знаний, 2013. – 304с.

8. Поляков К. , Еремин Е. Информатика. Углубленный уровень. [Текст]: Учеб-ник для 11 класса. / К. Поляков, Е. Еремин. –М.:БИНОМ. Лаборатория зна-ний, 2013. – 310с.

9. Поляков, К., Еремин Е. Информатика. Углубленный уровень. [Текст]: Учеб-ник для 11 класса: в 2 ч. Ч.2 . / К. Поляков, Е. Еремин. – М.:БИНОМ. Лаборатория знаний, 2013. – 310с.

10. Рябко, Б.Я., Основы современной криптографии и стеганографии [Текст] / Б.Я. Рябко, А.Н.Фионов – М.: Горячая линия-Телеком, 2010. – 232с.

11. Танова Э.В., Введение в криптографию: как защитить свое письмо от любопытных. Элективный курс: методическое пособие / Э.В.Танова. – М.: БИНОМ. Лаборатория знаний, 2008. – 79с.

12. Угринович, Н. Информатика и ИКТ. [Текст]: Учебник для 9 класса / Н. Уг-ринович.: БИНОМ. Лаборатория знаний, 2012. – 295с.

13. Фороузан, Б.А Криптография и безопасность сетей: учебное пособие / Б.А. Фороузан – М: БИНОМ. Лаборатория знаний, 2010. - 784с.

14. Чечета, С. Введение в дискретную теорию информации и кодирования. Учебное пособие / С.Чечета – МЦНМО, 2011. – 224с.

15. УМК «Информатика» 7 – 9 класс (ФГОС), автор Угринович Н. Д. [Элек-тронный ресурс] - http://metodist.lbz.ru/authors/informatika/1/

16. УМК «Информатика и ИКТ» 8 – 9 класс, автор Угринович Н. Д. [Электрон-ный ресурс] - http://metodist.lbz.ru/authors/informatika/1/

17. УМК «Информатика» для 10-11 классов ФГОС, углублённый уровень Ав-тор Семакин И. Г. и др. [Электронный ресурс] - http://metodist.lbz.ru/authors/informatika/2/

18. Федеральный государственный образовательный стандарт основного общего образования 2009г [Электронный ресурс] - http://минобрнауки.рф/документы/543

19. Л.Л. Босова, А.Ю. Босова Программа курса «Информатика и ИКТ» для ос-новной школы (8–9 классы) [Электронный ресурс] - http://metodist.lbz.ru/authors/informatika/3/

20. Рабочая программа по информатике и ИКТ 9 класс Автор программы учитель информатики и ИКТ высшей категории Осокина Е.О. 2011-2012 учебный год [Электронный ресурс] - http://teacher.76310s010.edusite.ru/

ПРИЛОЖЕНИЕ 1

Тема урока «Основные понятия криптографии»

Знать

- Предмет и задачи криптографии.
- Применение криптографии в современном обществе.
- Основные определения.
- Реализация криптографических методов.
- Понятие о криптографических атаках.
- Пример простейшего шифра.

Уметь

- Использовать понятийный аппарат по данной теме.
- Приводить примеры применения криптографии в современном обществе.
- Приводить примеры реализации криптографических методов.

Основные понятия: криптография, криптоанализ, криптология, стеганография, шифр, шифрование, расшифрование, дешифрование, ключ, шифрование с закрытым ключом, шифрование с открытым ключом, механические шифровальные машины, аппаратные шифраторы, криптографические атаки.

Методические рекомендации: Учитель посредством презентации рассказывает об основных понятиях криптографии и ведет беседу с учениками, задавая им различные вопросы по теме.

Этап урока	Действия учителя	Действия ученика	Время
Организационный период	Приветствие учеников. Учитель открывает презентацию «Основные понятия криптографии». Запускает презентацию на показ. Зачитывает тему урока с первого слайда презентации. Тема сегодняшнего урока: «Основные понятия криптографии». Сегодня на занятии мы изучим что такое криптография, основные понятия криптографии, узнаем историю развития криптографии и ответим на контрольные вопросы по изученному материалу.	Приветствие учителя. Изучение хода урока	2
Объяснение нового материала	3 слайд презентации: Проблемой защиты информации при ее передаче между абонентами люди занимаются на протяжении всей своей истории. Человечеством изобретено ***множество способов,*** позволяющих в той или иной мере *скрыть смысл*	Ученики внимательно слушают учителя	30

	передаваемых сообщений от противника. На практике выработалось *несколько групп методов* защиты секретных посланий. Назовем некоторые из них, применяющиеся так же давно, как и криптографические. 4 слайд презентации: **Первым способом** является **физическая защита** *материального носителя информации от противника*. В качестве носителя данных может выступать бумага, компьютерный носитель (DVD-диск, флэш-карта, магнитный диск, жесткий диск компьютера и т.д.). Для реализации этого способа необходим надежный **канал связи, недоступный для перехвата**. В различное время для этого использовались почтовые голуби, специальные курьеры, радиопередачи на секретной частоте. 5 слайд презентации: **Второй способ защиты** информации, известный с давних времен – **стеганографическая защита информации.** Этот способ защиты основан на попытке скрыть от противника		

	сам *факт наличия интересующей его информации*. К таким способам относят, например, "запрятывание" микрофотографии с тайной информацией в несекретном месте: под маркой на почтовом конверте, под обложкой книги и т.д. 6 слайд презентации: **Третий способ защиты** информации – наиболее надежный и распространенный в наши дни – **криптографический**. Этот метод защиты информации предполагает *преобразование информации для сокрытия ее смысла от противника*. 7 слайд презентации: **Криптография** в переводе с греческого означает *"тайнопись"*. В настоящее время *криптография* занимается поиском и исследованием *математических методов преобразования информации* 8 слайд презентации: Наряду с криптографией развивается и совершенствуется **криптоанализ** – наука о *преодолении* криптографической защиты информации.		

	Криптоаналитики исследуют *возможности расшифровывания* информации **без** знания **ключей** 9 слайд презентации: Иногда *криптографию* и *криптоанализ* объединяют в одну науку – **криптологию** (kryptos - тайный, logos - наука) Криптология занимается вопросами обратимого *преобразования информации* с целью *защиты* от несанкционированного доступа 10 слайд презентации: Как Вы думаете где криптография может применяться в современном обществе? • шифрование данных при передаче по открытым каналам связи (например, при совершении покупки в Интернете сведения о сделке, такие как адрес, телефон, номер кредитной карты, обычно зашифровываются в целях безопасности); • обслуживание банковских пластиковых карт; • хранение и обработка паролей пользователей в сети;		

	• сдача бухгалтерских и иных отчетов через удаленные каналы связи. 11 слайд презентации: Теперь рассмотрим основные определения криптографии: **Шифр** – совокупность заранее оговоренных *способов преобразования* исходного секретного сообщения с целью его защиты 12 слайд презентации: *Исходные сообщения* обычно называют **открытыми текстами** 13 слайд презентации: Сообщение, полученное *после преобразования* с использованием любого шифра, называется **шифрованным сообщением** (закрытым текстом, криптограммой) 14 слайд презентации: Преобразование *открытого текста* в *криптограмму* называется **зашифрованием.** Обратное действие называется **расшифрованием.** 15 слайд презентации:		

	Ключ – информация, необходимая для *шифрования* и *расшифрования* сообщений 16 слайд презентации: **Криптостойкостью** называется *характеристика шифра*, определяющая его стойкость к дешифрованию без знания ключа 17 слайд презентации: Все методы преобразования информации с целью защиты от несанкционированного доступа делятся на две большие группы: • *методы шифрования* **с закрытым ключом** • *методы шифрования* ***с*** **открытым ключом** 18 слайд презентации: **Шифрование с закрытым ключом** (шифрование *с секретным ключом* или *симметричное шифрование*) - для шифрования и расшифрования данных в этих методах используется **один и тот же ключ**, который обе стороны стараются хранить *в секрете* от противника		

	19 слайд презентации: Как проходило развитие криптографических методов? **Первый механический шифровальный прибор «скитала»** был изобретен в Древней Спарте в 4 – 5 веке до н.э. Для зашифровки текста использовался цилиндр, на который наматывалась пергаментная лента и писался текст  20 слайд презентации: В "докомпьютерную" эпоху *шифрование* данных выполнялось **вручную.** Специалист-шифровальщик обрабатывал исходное сообщение *посимвольно* и таким образом получал зашифрованный текст. Несмотря на то, что результат шифрования многократно проверялся, известны исторические факты ошибок		

	шифровальщиков 21 слайд презентации: Одним из самых известных механических шифровальных устройств является **шифратор Джефферсона**  22 слайд презентации: **Эни́гма** (от др.-греч. αἴνιγμα — загадка) — портативная шифровальная машина, использовавшаяся для шифрования и		

	дешифрования секретных сообщений  Трёхроторная военная немецкая шифровальная машина Энигма 23 слайд презентации: **Сегодня** для шифрования данных наиболее широко применяют три вида шифраторов: *аппаратные, программно-аппаратные и программные*. Их основное различие заключается не только в способе реализации шифрования и степени надёжности защиты		

	данных, но и в *цене*. **USB-шифратор ruToken** - российское средство аутентификации (проверки подлинности) и защиты информации, использующее сертифицированные алгоритмы шифрования и аутентификации и объединяющее в себе российские и международные стандарты безопасности  24 слайд презентации: Давайте рассмотрим пример простейшего шифра. **«Шифр Юлия Цезаря»** – одна из простейших и *первых* систем шифрования. Предполагается, что знаменитый римский император и полководец, живший в 1 веке до н. э., использовал этот шифр в своей переписке 25 слайд презентации:		

	Шифр Цезаря применительно к русскому языку состоит в следующем. Каждая буква сообщения заменяется на другую, которая в русском алфавите отстоит от исходной на три позиции дальше. Таким образом, буква А заменяется на Г , Б на Д и так далее вплоть до буквы Ь , которая заменялась на Я , затем Э на А , Ю на Б и, наконец, Я на В *АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ* Например, слово **ЗАМЕНА** после шифрования методом Цезаря превратится в **КГПЗРГ** 26 слайд презентации: Как расшифровать криптограмму, зашифрованную по методу Юлия Цезаря? Для расшифрования сообщения КГПЗРГ необходимо *знать только сам алгоритм шифрования*. Любой человек, знающий способ шифрования, легко может расшифровать секретное сообщение.		

	Таким образом, *ключом* в данном методе является сам *алгоритм*. Итак		
Практическая часть	Учитель просит учеников открыть тетради и выполнить небольшое задание по вариантам. 1. **Определите ключи шифра Цезаря**, если известны следующие пары открытый текст – шифротекст (исходный алфавит: АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ): • АПЕЛЬСИН - ТВЧЮОДЫА • МАНДАРИН – ТЁУЙЁЦОУ 2. **Расшифруйте следующие сообщения**, зашифрованные шифром Цезаря, и определите ключ n, 0<n<33, если известно, что исходные сообщения составлены из алфавита АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ: • ЮВПЛШУХ • СФЫЮБШЯФУ	Ученики выполняют задания в тетрадях.	10

Итоги урока	Итак, ответьте на вопросы: Что такое криптография? Что такое шифрование? Что такое ключ? Что представляла собой первая механическая шифровальная машина? Учитель подводит итоги урока, спрашивает, что понравилось ребятам, все ли было понятно. Сообщает, что на следующем занятии мы начнем рассматривать основные алгоритмы шифрования с открытым ключом. Для выполнения домашнего задания необходимо зайти на сайт http://cryptographylife.ru/, в разделе Лекции прочитать материал по теме «Основные понятия криптографии».	Ученики слушают учителя, спрашивают, задают вопросы, отвечают на вопрос учителя, записывают домашнее задание.	3

Тема урока «Методы шифрования с закрытым ключом»

Знать

- Общий принцип работы методов шифрования с закрытым ключом.
- Виды методов шифрования с закрытым ключом.
- Понятие о методах замены.
- Понятие о методах перестановки.
- Примеры алгоритмов шифрования как методов замены.
- Примеры алгоритмов шифрования как методов перестановки.

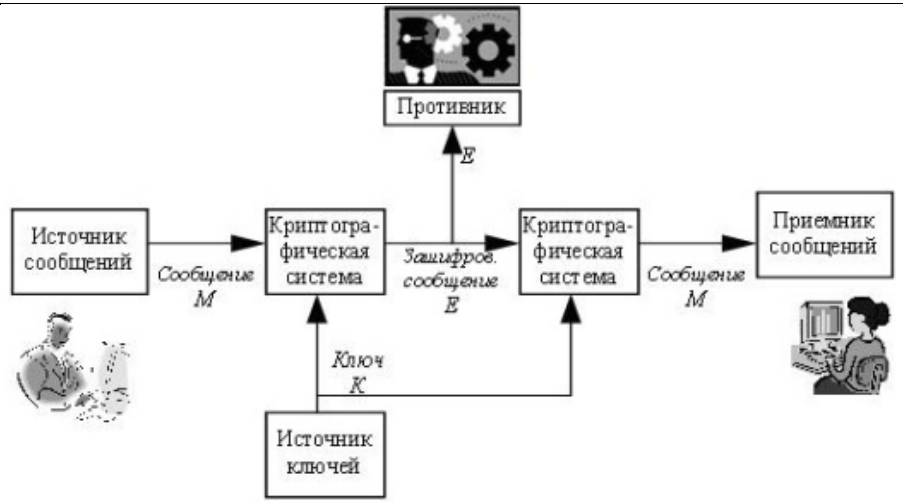
Уметь

- Использовать понятийный аппарат по данной теме.
- Приводить примеры алгоритмов шифрования как методов замены.
- Приводить примеры алгоритмов шифрования как методов перестановки.

Основные понятия: шифрование с закрытым ключом, симметричное шифрование, методы замены, методы перестановки.

Методические рекомендации: Учитель посредством презентации рассказывает о методах шифрования с закрытым ключом и ведет беседу с учениками, задавая им различные вопросы по теме.

Этап урока	Действия учителя	Действия ученика	Время
Организационный период	Приветствие учеников. Учитель открывает презентацию «Методы шифрования с закрытым ключом». Запускает презентацию на показ. Зачитывает тему урока с первого слайда презентации. Тема сегодняшнего урока: «Методы шифрования с закрытым ключом». Сегодня на занятии мы изучим общий принцип алгоритмов шифрования с закрытым ключом, рассмотрим алгоритмы замены и перестановки, а также ответим на контрольные вопросы по изученному материалу.	Приветствие учителя. Изучение хода урока	2
Объяснение нового материала	3 слайд презентации: В методах шифрования с закрытым ключом используется *один* и *тот же ключ для шифрования и расшифрования*, расшифрование является обратным действием для шифрования. Общая схема шифрования выглядит следующим образом:	Ученики внимательно слушают учителя	30



Давайте приведем пояснения к приведенной схеме шифрования. На передающей стороне имеются источник сообщений и источник ключей. Источник ключей выбирает конкретный ключ К среди всех возможных ключей данной системы. Этот ключ К передается некоторым способом принимающей стороне, причем предполагается, что его нельзя перехватить, например, ключ передается специальным курьером (поэтому симметричное шифрование называется также шифрованием с закрытым ключом).

Источник сообщений формирует некоторое сообщение М, которое затем шифруется с использованием выбранного ключа.

В результате процедуры шифрования получается зашифрованное

	сообщение E (называемое также криптограммой). Далее криптограмма E передается по каналу связи. Так как канал связи является открытым, незащищенным, например, радиоканал или компьютерная сеть, то передаваемое сообщение может быть перехвачено противником. На принимающей стороне криптограмму E с помощью ключа расшифровывают и получают исходное сообщение M. 4 слайд презентации: Методы шифрования с закрытым ключом можно разделить на следующие группы:		

В **методах замены** (или подстановки) символы открытого текста *заменяются* некоторыми эквивалентами шифрованного текста.

В **методах перестановки** символы исходного текста *меняются местами друг с другом* по определенному правилу.

5 слайд презентации:

При **одноалфавитной замене (подстановке)** устанавливается *однозначное*

соответствие между каждым знаком **ai** исходного алфавита сообщений A и соответствующим знаком **ei** зашифрованного текста E.

Пример **одноалфавитной замены** – шифр Цезаря.

Подстановка может быть задана с помощью таблицы, например, как показано на рисунке:

Откр. текст	Шифр 1	Шифр 2	Откр. текст	Шифр 1	Шифр 2	Откр. текст	Шифр 1	Шифр 2
А	В	^	М	Т	№	Ч	М	∑
Б	И	@	Н	Ц	#	Ш	У	∇
В	О	)	О	.	-	Щ	Д	ϒ
Г	А	+	П	Ж	=	Ъ	Э	ℵ
Д	Щ	<	Р	Г	(	Ы	Н	⊕
Е	П	>	С	Л	?	Ь	Ю	×
Ж	К	∀	Т	Х	%	Э	Ы	ω
З	Б	♦	У	С	⊗	Ю	Ш	$
И	Ъ	*	Ф	Ь	!	Я	Е	Δ
К	пробел	♥	Х	Ч	№	пробел	Ф	∞
Л	Р	♠	Ц	З	®	.	Я	♣

6 слайд презентации:

Можно привести следующий пример метода одноалфавитной замены:

Открытое сообщение																			
В	Ы	Ш	Л	И	Т	Е		П	О	Д	К	Р	Е	П	Л	Е	Н	И	Е
Зашифрованное сообщение с использованием шифра 1																			
О	Н	У	Р	Ъ	Х	П	Ф	Ж	.	Щ		Г	П	Ж	Р	П	Ц	Ъ	П
Зашифрованное сообщение с использованием шифра 2																			
)	⊕	∇	♠	*	%	>	∞	=	-	<	♥	(	>	=	♠	>	#	*	>

Как Вы считаете, какова криптостойкость данного метода?

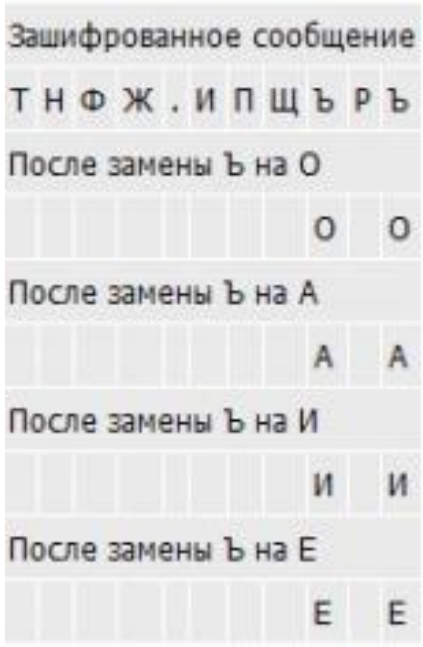
Полученный таким образом текст имеет сравнительно *низкий уровень защиты*, так как исходный и зашифрованный тексты имеют одинаковые статистические закономерности.

При этом *не имеет значения*, какие символы использованы для замены – перемешанные символы исходного алфавита или таинственно выглядящие знаки.

Зашифрованное сообщение может быть *вскрыто* путем так называемого **частотного криптоанализа**.

Для этого могут быть использованы некоторые *статистические данные языка*, на котором написано сообщение

	Известно, что в текстах на русском языке наиболее часто встречаются символы О, И. Немного реже встречаются буквы Е, А. Из согласных самые частые символы Т, Н, Р, С. В распоряжении криптоаналитиков имеются специальные таблицы частот встречаемости символов для текстов разных типов – научных, художественных. Криптоаналитик внимательно изучает полученную криптограмму, подсчитывая при этом, какие символы сколько раз встретились. Вначале наиболее часто встречаемые знаки зашифрованного сообщения заменяются, например, буквами О. Далее производится попытка определить места для букв И, Е, А. Затем подставляются наиболее часто встречаемые согласные. На каждом этапе оценивается возможность "сочетания" тех или иных букв. Например, в русских словах трудно найти четыре подряд гласные буквы, слова в русском языке не начинаются с буквы Ы и т.д. *Давайте приведем еще один пример работы криптоаналитика.* Пусть, например, в руки криптоаналитиков попало зашифрованное с помощью некоторого шифра одноалфавитной замены сообщение: **ТНФЖ.ИПЩЪРЪ**		

	В зашифрованном сообщении символ Ъ встречается 2 раза. Предположим, что в открытом тексте на месте зашифрованного знака Ъ стоит гласная О, А, И или Е.  Все приведенные варианты замены могут встретиться на практике. Варианты второго этапа криптоанализа зашифрованного сообщения:		

Зашифрованное сообщение										
Т	Н	Ф	Ж	.	И	П	Щ	Ъ	Р	Ъ
Варианты подобранных дешифрованных сообщений										
Ж	Д	И		С	У	М	Р	А	К	А
Д	Ж	О	Н	А		У	Б	И	Л	И
В	С	Е	Х		П	О	Б	И	Л	И
М	Ы		П	О	Б	Е	Д	И	Л	И

Кроме представленных в предыдущей таблице сообщений можно подобрать еще большое количество подходящих фраз.

Таким образом, если *ничего не известно* заранее о *содержании* перехваченного сообщения *малой длины*, **дешифровать** его **однозначно не получится.**

Если же в руки криптоаналитиков попадает достаточно *длинное сообщение*, зашифрованное *методом простой замены*, его обычно удается **успешно дешифровать**.

На помощь специалистам по вскрытию криптограмм приходят **статистические закономерности языка**.

Чем длиннее зашифрованное сообщение, тем больше вероятность его

	однозначного дешифрования. Если попытаться **замаскировать** *статистические характеристики* открытого текста, то задача вскрытия шифра простой замены значительно усложнится. Например, с этой целью можно перед шифрованием **"сжимать"** открытый текст с использованием компьютерных *программ-архиваторов.* Таким образом, с *усложнением правил замены* увеличивается **надежность шифрования.** 7 слайд презентации: Можно *заменять не отдельные символы*, а, например, двухбуквенные сочетания – *биграммы* Пример таблицы замен для двухбуквенных сочетаний:		

Откр. текст	Зашифр. текст	Откр. текст	Зашифр. текст
аа	кх	бб	пш
аб	пу	бв	вь
ав	жа	...	...
...	...	яэ	сы
ая	ис	яю	ек
ба	цу	яя	рт

С усложнением правил замены увеличивается надежность шифрования.

Возможны варианты использования триграммного или вообще n-граммного шифра. Такие шифры обладают более высокой криптостойкостью, но они сложнее для реализации и требуют гораздо большего количества ключевой информации (большой объем таблицы замен).

Однако, все n-граммные шифры могут быть вскрыты с помощью частотного криптоанализа, только используется статистика встречаемости не отдельных символов, а сочетаний из n символов

К одноалфавитным методам замены относятся **пропорциональные** или **монофонические шифры**, в которых *для знаков*, встречающихся *часто*,

используется относительно *большое число возможных эквивалентов*.

8 слайд презентации:

Символ	Варианты замены					Символ	Варианты замены					
А	760	128	350	201		С	800	767	105			
Б	101					Т	759	135	214			
В	210	106				У	544					
Г	351					Ф	560					
Д	129					Х	768					
Е	761	130	802	352		Ц	545					
Ж	102					Ч	215					
З	753					Ш	103					
И	762	211	131			Щ	752					
К	754	764				Ъ	561					
Л	132	354				Ы	136					
М	755	742				Ь	562					
Н	763	756	212			Э	750					
О	757	213	765	133	353	Ю	570					
П	743	766				Я	216	104				
Р	134	532				Пробел	751	769	758	801	849	035...

Как в этом случае будет зашифровано сообщение ***БОЛЬШОЙ СЕКРЕТ?***

	Проверьте свой результат шифрования: **10175713256210321376275180076175413413075 9** *Пропорциональные шифры* **более сложны** для вскрытия, чем шифры простой одноалфавитной замены. Однако, если имеется хотя бы одна пара "открытый текст – шифротекст", вскрытие производится тривиально. Если же в наличии имеются только шифротексты, то вскрытие ключа, то есть нахождение таблицы замен, становится более **трудоемким**, но тоже вполне **осуществимым.** 9 слайд презентации: При использовании шифров перестановки исходный текст делится на *блоки*, в каждом из которых выполняется *перестановка символов*. Простейшим примером перестановки является **перестановка с фиксированным периодом d**. В этом методе сообщение делится на блоки по d символов и в каждом блоке производится одна и та же перестановка. Правило, по которому производится перестановка, является ключом. В результате сами буквы сообщения не изменяются, но передаются в другом		

	порядке. **Пример:** зашифровать текст: **ЭТО_ТЕКСТ_ДЛЯ_ШИФРОВАНИЯ** для **d=6** в качестве **ключа** перестановки можно взять 436215. Это означает, что в каждом блоке из 6 символов четвертый символ становится на первое место, третий – на второе, шестой – на третье и т.д. 10 слайд презентации: **Пример:** Количество символов в сообщении **ЭТО_ТЕКСТ_ДЛЯ_ШИФРОВАНИЯ** равно 24, следовательно, сообщение необходимо разбить на 4 блока для d=6 и ключа 436215. **Результатом шифрования** с помощью перестановки 436215 будет сообщение **_ОЕТЭТ_ТЛСКДИШР_ЯФНАЯВОИ** Теоретически, если блок состоит из d символов, то число возможных перестановок равно **d!=1*2*...*(d-1)*d** В последнем примере d=6, следовательно, число перестановок равно		

	6!=1*2*3*4*5*6=720. Таким образом, если противник перехватил зашифрованное сообщение из рассмотренного примера, ему понадобится не более 720 попыток для раскрытия исходного сообщения (при условии, что размер блока известен противнику). Для повышения криптостойкости можно последовательно применить к шифруемому сообщению две или более перестановки с разными периодами Другим примером методов перестановки является **перестановка по таблице**. В этом методе производится запись исходного текста по строкам некоторой таблицы и чтение его по столбцам этой же таблицы. *Последовательность заполнения строк и чтения столбцов* может быть любой и задается *ключом*. 11 слайд презентации: **Пример:** Пусть в таблице кодирования будет 4 столбца и 3 строки (размер блока равен 3*4=12 символов). Зашифровать текст:		

ЭТО ТЕКСТ ДЛЯ ШИФРОВАНИЯ

Количество символов в исходном сообщении равно 24, следовательно, сообщение необходимо разбить на 2 блока. Запишем каждый блок в свою таблицу по строчкам:

1 блок				2 блок			
Э	Т	О		Я		Ш	И
Т	Е	К	С	Ф	Р	О	В
Т		Д	Л	А	Н	И	Я

Затем будем считывать из таблицы каждый блок последовательно по столбцам:

ЭТТТЕ ОКД СЛЯФА РНШОИИВЯ

Можно считывать столбцы не последовательно, а, например, так: третий, второй, первый, четвертый:

ОКДТЕ ЭТТ СЛШОИ РНЯФАИВЯ

Таким образом, в этом случае *порядок считывания столбцов* и будет

<table>
<tr><td></td><td>ключом.
В случае, если размер сообщения не кратен размеру блока, можно дополнить сообщение какими-либо символами, не влияющими на смысл, например, пробелами.
Однако это может способствовать определению противником в случае перехвата криптограммы информации о длине блока.</td><td></td><td></td></tr>
<tr><td>Практическая часть</td><td>Учитель просит учеников открыть тетради и выполнить небольшое задание. Имеется таблица замены для двух шифров простой замены: шифра №1 и шифра №2.
<table>
<tr><th>Откр. текст</th><th>Шифр 1</th><th>Шифр 2</th><th></th><th>Откр. текст</th><th>Шифр 1</th><th>Шифр 2</th><th></th><th>Откр. текст</th><th>Шифр 1</th><th>Шифр 2</th></tr>
<tr><td>А</td><td>В</td><td>^</td><td></td><td>М</td><td>Т</td><td>№</td><td></td><td>Ч</td><td>М</td><td>∑</td></tr>
<tr><td>Б</td><td>И</td><td>@</td><td></td><td>Н</td><td>Ц</td><td>#</td><td></td><td>Ш</td><td>У</td><td>∇</td></tr>
<tr><td>В</td><td>О</td><td>)</td><td></td><td>О</td><td>.</td><td>-</td><td></td><td>Щ</td><td>Д</td><td>ϒ</td></tr>
<tr><td>Г</td><td>А</td><td>+</td><td></td><td>П</td><td>Ж</td><td>=</td><td></td><td>Ъ</td><td>Э</td><td>ℵ</td></tr>
<tr><td>Д</td><td>Щ</td><td><</td><td></td><td>Р</td><td>Г</td><td>(</td><td></td><td>Ы</td><td>Н</td><td>⊕</td></tr>
<tr><td>Е</td><td>П</td><td>></td><td></td><td>С</td><td>Л</td><td>?</td><td></td><td>Ь</td><td>Ю</td><td>×</td></tr>
<tr><td>Ж</td><td>К</td><td>∀</td><td></td><td>Т</td><td>Х</td><td>%</td><td></td><td>Э</td><td>Ы</td><td>ω</td></tr>
<tr><td>З</td><td>Б</td><td>♦</td><td></td><td>У</td><td>С</td><td>⊗</td><td></td><td>Ю</td><td>Ш</td><td>$</td></tr>
<tr><td>И</td><td>Ъ</td><td>*</td><td></td><td>Ф</td><td>Ь</td><td>!</td><td></td><td>Я</td><td>Е</td><td>Δ</td></tr>
<tr><td>К</td><td>пробел</td><td>♥</td><td></td><td>Х</td><td>Ч</td><td>№</td><td></td><td>пробел</td><td>Ф</td><td>∞</td></tr>
<tr><td>Л</td><td>Р</td><td>♠</td><td></td><td>Ц</td><td>З</td><td>®</td><td></td><td>.</td><td>Я</td><td>♣</td></tr>
</table></td><td>Ученики выполняют задания в тетрадях.</td><td>8</td></tr>
</table>

	Расшифруйте сообщения, зашифрованные с помощью шифра №1: И.РЮУ.ЪФОБГНО Расшифруйте сообщение, зашифрованное с помощью шифра №2: 		
Итоги урока	Итак, ответьте на вопросы: • Поясните общую схему симметричного шифрования. • Что общего имеют все методы шифрования с закрытым ключом? • Назовите основные группы методов шифрования с закрытым ключом. • Приведите примеры шифров замены. • В чем заключаются одноалфавитные подстановки? • Приведите пример шифра одноалфавитной замены. Учитель подводит итоги урока, спрашивает, что понравилось ребятам, все ли было понятно. Сообщает, что на следующем занятии мы будем шифровать сообщение методом Вижинера. Для выполнения домашнего задания необходимо зайти на сайт http://cryptographylife.ru/, в разделе Лекции прочитать материал по теме «Простейшие методы шифрования с закрытым ключом».	Ученики слушают учителя, спрашивают, задают вопросы, отвечают на вопрос учителя, записывают домашнее задание.	5

Тема урока «Шифр Вижинера»

Знать

- Методы шифрования заменой.
- Понятие о многоалфавитной замене.
- Принцип дешифровки сообщений.
- Принцип использования алгоритмов многоалфавитной замены.
- Принцип использования шифра Вижинера

Уметь

- Шифровать сообщения, используя алгоритм Вижинера.
- Оценивать криптостойкость алгоритма шифрования.

Основные понятия: симметричное шифрование, многоалфавитная замена, дешифровка сообщений, криптостойкость алгоритма шифрования, шифр Вижинера.

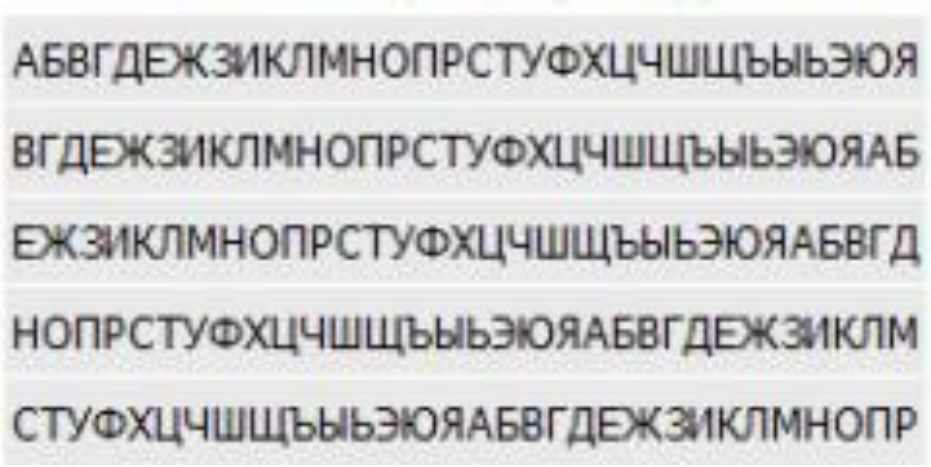
Методические рекомендации: На данном уроке учитель является главным наблюдателем помощником, в задачу учителя входит корректировать действия ученика и помогать советами в выполнение задания.

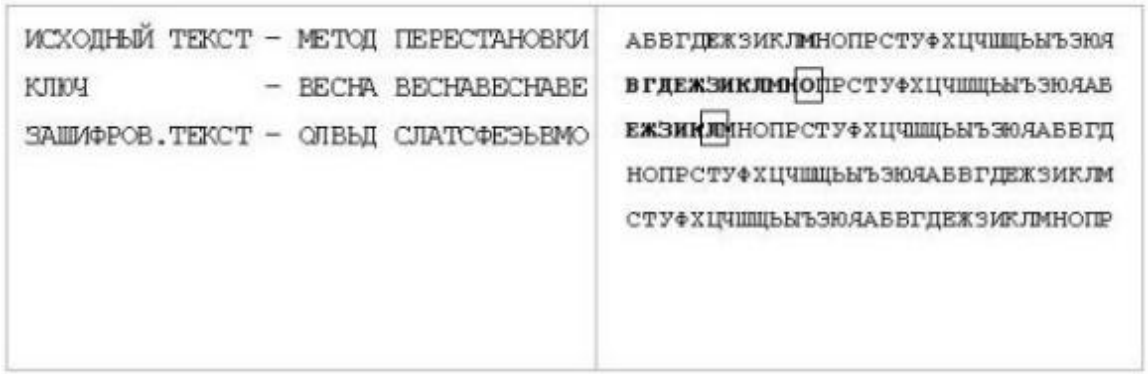
Этап урока	Действия учителя	Действия ученика	Время
Организационный период	Приветствие учеников. Учитель открывает презентацию «Шифр Вижинера». Запускает	Приветствие учителя.	2

	презентацию на показ. Тема сегодняшнего урока: «Шифр Вижинера». Сегодня на занятии мы изучим понятие многоалфавитной замены, рассмотрим принцип использования шифра Вижинера, зашифруем текст по этому методу и ответим на контрольные вопросы по изученному материалу.	Изучение хода урока	
Объяснение нового материала	2 слайд презентации: В целях маскирования естественной частотной статистики исходного языка применяется *многоалфавитная подстановка*. В многоалфавитных подстановках для замены символов исходного текста используется не один, а *несколько алфавитов*. Обычно алфавиты для замены образованы из символов исходного алфавита, записанных в другом порядке *Примером* многоалфавитной подстановки может служить схема, основанная на использовании **таблицы Вижинера**. Этот метод, известный уже в XVI веке, был описан французом *Блезом Вижинером* в "Трактате о шифрах", вышедшем в 1585 году. 3 слайд презентации: В этом методе для шифрования используется таблица, представляющая	Ученики внимательно слушают учителя	20

	собой квадратную матрицу с числом элементов NxN, где N — количество символов в алфавите. В первой строке матрицы записывают буквы в порядке очередности их в исходном алфавите, во второй — ту же последовательность букв, но с циклическим сдвигом влево на одну позицию, в третьей — со сдвигом на две позиции и т. д.		

	 4 слайд презентации: Для шифрования текста выбирают **ключ**, представляющий собой некоторое слово или набор символов исходного алфавита. Далее из полной матрицы выписывают *подматрицу шифрования*, включающую *первую строку* и строки матрицы, начальными буквами		

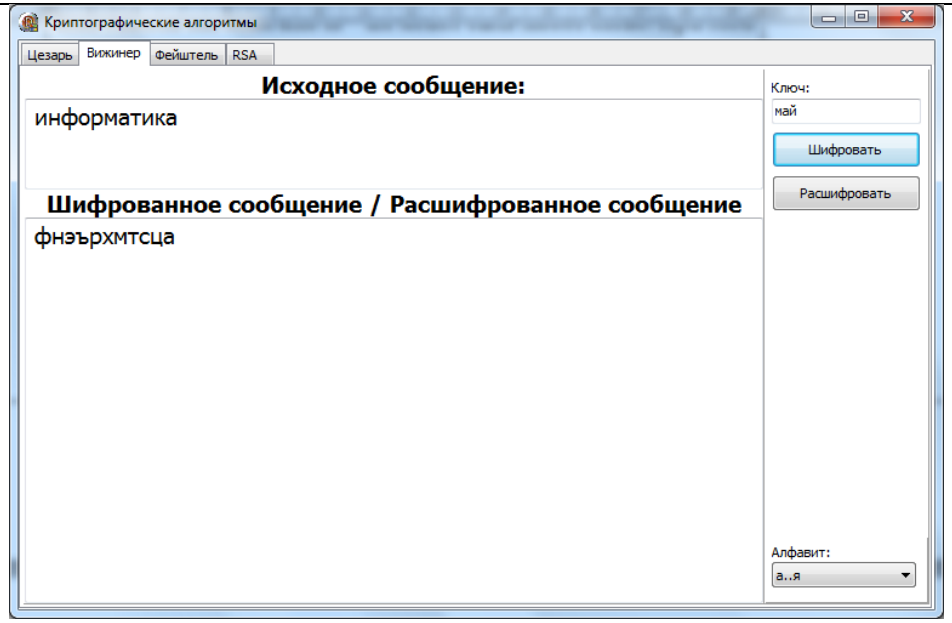
	которых являются последовательно буквы ключа. Например, если выбрать ключ "весна", то таблица шифрования будет следующей:  5 слайд презентации: Механизм шифрования многоалфавитной заменой заключается в следующем: 1) под каждой буквой шифруемого текста записывают буквы ключа, повторяющие ключ требуемое число раз; 2) шифруемый текст по таблице шифрования заменяют буквами, расположенными на пересечениях линий, соединяющих буквы текста		

	первой строки таблицы и буквы ключа, находящейся под ней.  Например, под первой буквой исходного текста "М" записана буква "В" ключа. В таблице кодирования находим столбец, начинающийся с "М" и строку, начинающуюся с "В". На их пересечении располагается буква "О". Она и будет первым символом зашифрованного сообщения. Следующая буква исходного сообщения – "Е", символ ключа – тоже "Е". Находим пересечение строки, начинающейся с "Е", и столбца, начинающегося с "Е". Это будет буква "Л" – второй символ зашифрованного сообщения. 6 слайд презентации: Как будет выглядеть расшифровка сообщения, зашифрованного по методу Вижинера:		

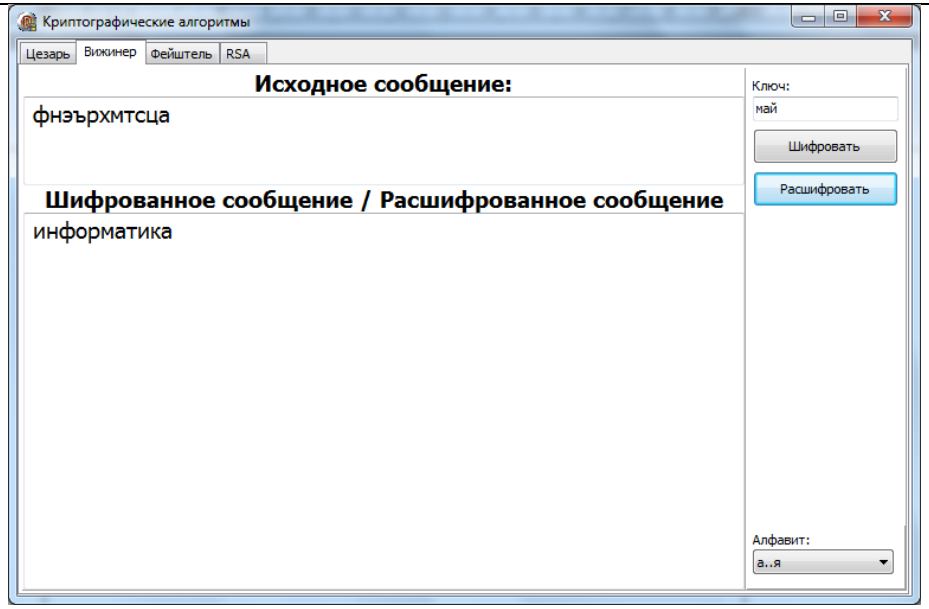
	КЛЮЧ ВЕСНАВЕСНАВЕСНАВ ЗАШИФРОВАННЫЙ ТЕКСТ КЕКХТВОЭЦОТССВИЛ РАСШИФРОВАННЫЙ ТЕКСТ ЗАЩИТАИНФОРМАЦИИ ИСХОДНЫЙ ТЕКСТ ЗАЩИТА ИНФОРМАЦИИ Расшифровка текста выполняется в следующей последовательности: • над буквами шифрованного текста сверху последовательно записывают буквы ключа, повторяя ключ требуемое число раз; • в строке подматрицы таблицы Вижинера для каждой буквы ключа отыскивается буква, соответствующая знаку шифрованного текста. Находящаяся над ней буква первой строки и будет знаком расшифрованного текста; • полученный текст группируется в слова по смыслу. С целью повышения надежности шифрования текста можно использовать подряд *два* или *более зашифрования* по методу Вижинера с разными ключами (составной шифр Вижинера). На практике кроме метода Вижинера использовались также различные		

	модификации этого метода. Например, шифр Вижинера с перемешанным один раз алфавитом. В этом случае для расшифрования сообщения получателю необходимо кроме ключа знать порядок следования символов в таблице шифрования. 7 слайд презентации: Методы многоалфавитной подстановки, в том числе и метод Вижинера, значительно труднее поддаются "ручному" криптоанализу. С использованием компьютера вскрытие метода многоалфавитной подстановки возможно достаточно быстро благодаря высокой скорости проводимых операций и расчетов. В первой половине XX века для автоматизации процесса выполнения многоалфавитных подстановок стали широко применять **роторные шифровальные машины**. Главными элементами в таких устройствах являлись **роторы** – механические колеса, используемые для выполнения подстановки. А теперь рассмотрим процесс шифрования сообщений по методу Вижинера с помощью программы Криптографические алгоритмы.exe.		

	С помощью программы Криптографические алгоритмы.exe можно зашифровать и расшифровать сообщения по алгоритмам Юлия Цезаря, Вижинера, Фейштеля и RSA. Для шифрования сообщения по методу Вижинера необходимо открыть закладку Вижинер, в поле ввода для исходного сообщения ввести информацию, необходимую для шифрования, также в строку Ключ ввести значение ключа – им может быть любое слово. С помощью списка Алфавит закладки Вижинер можно выбрать набор символов русского алфавита и протестировать программу:		



Для проверки работы программы зашифрованное сообщение расшифруем:

			
Практическая часть	Учитель просит учеников открыть тетради и выполнить задание. Пусть исходный алфавит содержит следующие символы: АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ Зашифруйте с помощью шифра Вижинера и ключа ЯБЛОКО сообщения: • КРИПТОСТОЙКОСТЬ • ГАММИРОВАНИЕ Пусть исходный алфавит состоит из следующих знаков (символ "_"	Ученики выполняют задания в тетрадях.	20

	(подчеркивание) будем использовать для пробела): АБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ_ Расшифруйте сообщения, зашифрованные с помощью шифра Вижинера и ключа ОРЕХ: • ШВМБУЖНЯ • ЯБХЪШЮМХ		
Итоги урока	Итак, ответьте на вопросы: • Поясните общую схему симметричного шифрования. • Что общего имеют все методы шифрования с закрытым ключом? • Сформулируйте общие принципы для методов шифрования заменой. • В чем заключается многоалфавитная замена? Учитель подводит итоги урока, спрашивает, что понравилось ребятам, все ли было понятно. Сообщает, что будет изучаться на следующем занятии. Для выполнения домашнего задания необходимо зайти на сайт http://cryptographylife.ru/, в разделе Лекции прочитать материал по теме	Ученики слушают учителя, спрашивают, задают вопросы, отвечают на вопрос учителя.	3

	«Простейшие методы шифрования с закрытым ключом. Шифр Вижинера». А в разделе Практика выполнить задание по шифрованию текста по методу Вижинера в соответствии с вариантом.		