Министерство образования и науки Российской Федерации

Федеральное государственное автономное
образовательное учреждение высшего образования
«Санкт-Петербургский политехнический университет Петра Великого»

Институт среднего профессионального образования

Методические указания и контрольные задания по дисциплине

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

для студентов заочной формы обучения

по специальности

09.02.03 «Программирование в компьютерных системах»

Санкт-Петербург

2022

СОДЕРЖАНИЕ

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА 3
МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ИЗУЧЕНИЮ ДИСЦИПЛИНЫ 4
ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ 4
Раздел 1. Понятия и определения информационной безопасности 4
Раздел 2. Основные понятия криптографии 12
Раздел 3. Симметричные и асимметричные алгоритмы 21
МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ВЫПОЛНЕНИЯ КОНТРОЛЬНОЙ РАБОТЫ 25
СТРУКТУРА И СОДЕРАЖНИЕ КОНТРОЛЬНОЙ РАБОТЫ 28
ЗАДАНИЕ НА КОНТРОЛЬНУЮ РАБОТУ 28
ЛИТЕРАТУРА ДЛЯ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ И ВЫПОЛНЕНИЯ КОНТРОЛЬНОЙ РАБОТЫ 32
Приложение 1 34
Приложение 2 47

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Рабочая программа, методические указания и контрольные задания учебной дисциплины «Информационная безопасность» предназначены для реализации государственных требований к уровню подготовки выпускников по техническим специальностям среднего профессионального образования.

Методические указания разработаны для организации самостоятельной работы студентов, которая поможет развитию умений искать основную информацию, работать с учебной литературой и применять получаемые знания в учебной и практической деятельности.

В методических указаниях даны краткие теоретические сведения, контрольная работа и список необходимой литературы. По результатам изучения дисциплины «Информационная безопасность» студент должен:

знать:

- вопросы административного и нормативно-правового обеспечения защиты информации
- основные системы защиты информации в России и в ведущих зарубежных странах;
- основные программно-аппаратные средства и методы защиты информации в компьютерных системах.

уметь:

- выбирать средства обеспечения информационной безопасности информационной системы современного предприятия;
- ограничивать использование ресурсов компьютера на основе раздельного доступа пользователей в операционную систему;
- организовывать защиту информации в локальной сети на уровнях входа в сеть и системы прав доступа;
- организовывать безопасную работу в Интернет и отправку почтовых сообщений в глобальной сети;

– использовать средства защиты данных от разрушающих программных воздействий компьютерных вирусов.

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ИЗУЧЕНИЮ ДИСЦИПЛИНЫ

ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

Курс «Информационная безопасность» посвящен изучению современного представления о методах и средствах обеспечения защиты информационных ресурсов, а также информационной безопасности личности и общества.

Цель курса - формирование у будущих специалистов знаний и умений, связанных с правовыми и программно-техническими методами защиты информации государственных и негосударственных организаций и учреждений, осуществляющих взаимодействие и обмен данными посредством электронных коммуникаций, основ информационной безопасности и практических методов регулирования взаимодействий информационных процессов.

Раздел 1. Понятия и определения информационной безопасности

Алгоритмический контроль – заключается в том, что задача, решенная по какому-либо алгоритму, проверяется повторно по сокращенному алгоритму с достаточной степенью точности.

Атака – действие, предпринимаемое нарушителем в поиске и использовании той или иной уязвимости. Угрозы могу быть разделены на угрозы, не зависящие от деятельности человека, и искусственные угрозы, связанные с деятельностью человека.

Аутентификация – установление подлинности, заключается в проверке, является ли проверяемый объект (субъект) в самом деле тем, за кого себя выдает.

Биометрические технологии – идентификация человека по уникальным, присущим только ему биологическим признакам.

Владелец информации – субъект, осуществляющий владение и пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации.

Владелец сертификата ключа подписи – физическое лицо, на имя которого удостоверяющим центром выдан сертификат ключа подписи и которое владеет соответствующим закрытым ключом электронной
цифровой подписи, позволяющим с помощью средств электронной цифровой подписи создавать свою электронную цифровую подпись в электронных документах (подписывать электронные документы).

Вредоносные программы – программы, к которым относятся: классические файловые вирусы, сетевые черви, троянские программы, спам, хакерские

утилиты и прочие программы, наносящие заведомый вред компьютеру, на котором они запускаются на выполнение, или другим компьютерам в сети.

Дешифровывание – процесс, при котором из шифротекста извлекается открытый текст.

Доступ к информации – получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств.

Естественные угрозы – угрозы, вызванные воздействиями на АСОИ и ее элементы объективных физических процессов или стихийных природных явлений, не зависящих от человека.

Закрытый ключ электронной цифровой подписи – уникальная последовательность символов, известная владельцу сертификата ключа подписи и предназначенная для создания в электронных документах электронной цифровой подписи с использованием средств электронной цифровой подписи.

Защита информации – деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Защита информации от агентурной разведки – деятельность по предотвращению получения защищаемой информации агентурной разведкой.

Защита информации от иностранной технической разведки – деятельность по предотвращению получения защищаемой информации иностранной разведкой с помощью технических средств.

Защита информации от аварийных ситуаций – создание средств предупреждения, контроля и организационных мер по исключению НСД на комплексе средств автоматизации в условиях отказов его функционирования, отказов системы защиты информации, систем жизнеобеспечения людей на объекте размещения и при возникновении стихийных бедствий.

Защита информации от иностранной разведки – деятельность по предотвращению получения защищаемой информации иностранной разведкой.

Защита информации от непреднамеренного воздействия – деятельность по предотвращению воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений или иных нецеленаправленных на изменение информации воздействий, связанных с функционированием технических средств, систем или с деятельностью людей, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Защита информации от несанкционированного воздействия – деятельность по предотвращению воздействия на защищаемую информацию с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к

информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Защита информации от несанкционированного доступа – деятельность по предотвращению получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации. Заинтересованными субъектами, осуществляющими несанкционированный доступ к защищаемой информации, могут выступать: государство, юридическое лицо, группа физических лиц, в том числе общественная организация, отдельное физическое лицо.

Защита информации от разглашения – деятельность по предотвращению несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

Защита информации от утечки – деятельность по предотвращению неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа к защищаемой информации и от получения защищаемой информации [иностранными] разведками.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации. Собственниками информации могут быть – государство, юридическое лицо, группа физических лиц, отдельное физическое лицо.

Злоумышленник – нарушитель, намеренно идущий на нарушение из корыстных побуждений.

Идентификация – присвоение какому-либо объекту или субъекту уникального образа, имени или числа.

Интернет – объединение в масштабе всей планеты группы сетей, которое использует единый протокол для передачи данных.

Информационная безопасность РФ – состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

Информационная система – совокупность документов и массивов документов и информационных технологий.

Информационная система общего пользования – информационная система, которая открыта для использования всеми физическими и юридическими лицами и в услугах которой этим лицам не может быть отказано.

Информационные процессы – процессы сбора, накопления, обработки хранения, распределения и поиска информации.

Информационные ресурсы – документы или массив документов, существующие отдельно или в составе информационной системы.

Информация – сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления. Информация является

одним из объектов гражданского права том числе и прав собственности, владения, пользования.

Искусственные угрозы – угрозы АСОИ, вызванные деятельностью человека. Среди них, исходя из мотивации действий, можно выделить непреднамеренные и преднамеренные.

Категорирование защищаемой информации – установление градаций важности защиты защищаемой информации.

Классические вирусы – это программы, распространяющие свои копии по ресурсам локального компьютера.

Ключ – используется в процессе шифровки и дешифровки.

Кодирование информации – осуществляется заменой слов и предложений исходной информации кодами.

Компьютерные преступления против государственных и общественных интересов – преступления, направленные против государственной и общественной безопасности (например, угрожающие обороноспособности государства, злоупотребления с автоматизированными системами голосования и т.д.).

Компьютерные преступления против личных прав и частной сферы – незаконный сбор данных о лице, разглашение частной информации (например, банковской или врачебной тайны, информации о расходах и т.д.).

Контроль доступа к аппаратуре – означает, что внутренний монтаж аппаратуры и технологические органы и пульты управления закрыты крышками, дверцами или кожухами, на которые установлены датчики.

Контроль организации защиты информации – проверка соответствия состояния организации, наличия и содержания документов требованиям правовых, организационно-распорядительных и нормативных документов по защите информации.

Контроль состояния защиты информации – проверка соответствия организации и эффективности защиты информации, установленным требованиям и/или нормам в области защиты информации.

Контроль эффективности защиты информации – проверка соответствия эффективности мероприятий по защите информации установленным требованиям или нормам эффективности защиты информации.

Конфиденциальность информации – известность ее содержания только имеющим соответствующие полномочия субъектам.

Корпоративная информационная система – информационная система, участниками которой может быть ограниченный круг лиц, определенный ее владельцем или соглашением участников этой информационной системы.

Кракер – лицо, изучающее систему с целью ее взлома. Именно кракеры реализуют свои криминальные наклонности в похищении информации и написании вирусов, разрушающих ПО. Они применяют различные способы атак на компьютерную систему, используя принципы построения протоколов

сетевого обмена. Кракеры разрабатывают специальное программное обеспечение, засылая его на взломанную машину.

Криптоанализ **–** исследование возможности расшифровки информации без ключа.

Криптография **–** построение и исследование математических методов преобразования информации.

Мероприятие по защите информации **–** совокупность действий по разработке и/или практическому применению способов и средств защиты информации.

Мероприятие по контролю эффективности защиты информации **–** совокупность действий по разработке и/или практическому применению методов, способов и средств контроля эффективности защиты информации.

Метод контроля эффективности защиты информации **–** порядок и правила применения определенных принципов и средств контроля эффективности защиты информации.

Непреднамеренное воздействие на защищенную информацию **–** воздействие на нее из-за ошибок пользователя, сбой техники или программных средств, природных явлений и т.д.

Несанкционированное воздействие **–** на защищенную информацию – воздействие с нарушением правил ее изменения.

Несанкционированный доступ **–** получение защищенной информации заинтересованным субъектом с нарушением правилом доступа к ней.

Нормы эффективности защиты информации **–** значения показателей эффективности защиты информации, установленные нормативными документами.

Носитель информации **–** физическое лицо, или материальный объект, в том числе физическое поле, в которых информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов.

Объект защиты **–** информация или носитель информации, или информационный процесс, в отношении которых необходимо обеспечивать защиту в соответствии с поставленной целью защиты информации.

Ограничение доступа **–** создание некоторой физической замкнутой преграды вокруг объекта защиты с организацией контролируемого доступа лиц, связанных с объектом защиты по своим функциональным обязанностям.

Одноалфавитная подстановка **–** прямая замена символов шифруемого сообщения другими буквами того же самого или другого алфавита.

Орган защиты информации **–** административный орган, осуществляющий организацию защиты информации.

Организационные мероприятия по защите информации в АСОИ **–** разработка и реализация административных и организационно-технических мер при подготовке и эксплуатации системы.

Организационный контроль эффективности защиты информации **–** проверка полноты и обоснованности мероприятий по защите информации требованиям нормативных документов по защите информации.

Организация защиты информации – содержание и порядок действий по обеспечению защиты информации.

Открытый ключ электронной цифровой подписи – уникальная последовательность символов, соответствующая закрытому ключу электронной цифровой подписи, доступная любому пользователю информационной системы и предназначенная для подтверждения с использованием средств электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе.

Подтверждение подлинности электронной цифровой подписи в электронном документе – положительный результат проверки соответствующим сертифицированным средством электронной цифровой подписи с использованием сертификата, ключа, подписи, принадлежности электронной, цифровой подписи в электронном документе владельцу сертификата ключа подписи и отсутствия искажений в подписанном данной электронной цифровой подписью электронном документе.

Показатель эффективности защиты информации – мера или характеристика для оценки эффективности защиты информации.

Пользователь (потребитель) информации – субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации либо с их нарушением.

Пользователь сертификата ключа подписи - физическое лицо, использующее полученные в удостоверяющем центре сведения о сертификате ключа подписи для проверки принадлежности электронной цифровой подписи владельцу сертификата ключа подписи.

Правило доступа к информации – совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям.

Право доступа к информации – совокупность правил доступа к информации, установленных правовыми документами или собственником, владельцем информации.

Преднамеренные (умышленные) угрозы – связаны с корыстными устремлениями людей (злоумышленников).

Предоставление привилегий на доступ – к информации заключается в том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы.

Разграничение доступа – в вычислительной системе – разделение информации, циркулирующей в ней, на части и организация доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями.

Сертификат ключа подписи – документ на бумажном носителе или электронный документ с электронной цифровой подписью уполномоченного лица удостоверяющего центра, которые включают в себя открытый ключ

электронной цифровой подписи и которые выдаются удостоверяющим центром участнику информационной системы для подтверждения подлинности электронной цифровой подписи и идентификации владельца сертификата ключа подписи.

Сертификат средств электронной цифровой подписи **–** документ на бумажном носителе, выданный в соответствии с правилами системы сертификации для подтверждения соответствия средств электронной цифровой подписи установленным требованиям.

Сетевые черви **–** программы, распространяющие свои копии по локальным и/или глобальным сетям.

Сжатие информации **–** метод криптографического преобразования информации.

Система защиты информации **–** совокупность органов и/или исполнителей, используемая ими техника защиты информации, а также объекты защиты, организованные и функционирующие по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами по защите информации.

Скамеры **–** мошенники, рассылающие свои послания в надежде поймать на наживку наивных и жадных.

Интернет-телефония становится все более популярной. На сегодня зарегистрировано уже довольно много случаев обращения мошенников к пользователям Skype – сервисом IP-телефонии, позволяющим пользователям связываться посредством компьютер-компьютер и компьютер-телефон.

Собственник информации **–** субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения информацией в соответствии с законодательными актами.

Спамеры **–** те, от кого приходят в наши почтовые ящики не запрошенные массовые рассылки.

Способ защиты информации **–** порядок и правила применения определенных принципов и средств защиты информации.

Средства электронной цифровой подписи **–** аппаратные и (или) программные средства, обеспечивающие реализацию хотя бы одной из следующих функций – создание электронной цифровой подписи в электронном документе с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе, создание закрытых и открытых ключей электронных цифровых подписей.

Средство защиты информации **–** техническое, программное средство, вещество и/или материал, предназначенные или используемые для защиты информации.

Средство контроля эффективности защиты информации *– техническое, программное средство, вещество и/или материал, предназначенные или используемые для контроля эффективности защиты информации.*
Стеганография – метод скрытой передачи информации.
Стойкость метода – тот минимальный объем зашифрованного текста, статистическим анализом которого можно вскрыть исходный текст. Таким образом, стойкость шифра определяет допустимый
объем информации, зашифровываемый при использовании одного ключа.
Субъект доступа к информации – участник правоотношений в информационных процессах. ***Информационные процессы –*** процессы создания, обработки, хранения, защиты от внутренних и внешних
угроз, передачи, получения, использования и уничтожения информации.
Тестовый контроль – применяется для проверки работоспособности комплекса средств автоматизации при помощи испытательных программ.
Техника защиты информации – средства защиты информации, средства контроля эффективности защиты информации, средства и системы управления, предназначенные для обеспечения защиты информации.
Технический контроль эффективности защиты информации – контроль эффективности защиты информации, проводимый с использованием средств контроля.
Троянский конь – программы, осуществляющие различные несанкционированные пользователем действия: сбор информации и ее передачу злоумышленнику, ее разрушение или злонамеренную модификацию, нарушение работоспособности компьютера, использование ресурсов компьютера.
Трудоемкость метода – число элементарных операций, необходимых для шифрования одного символа исходного текста.
Угроза информационной безопасности в компьютерной системе – события или действия, которые могут вызвать изменения функционирования КС, связанные с нарушением защищенности информации, обрабатываемой в ней.
Удаленная атака – несанкционированное информационное воздействие на распределенную вычислительную систему, программно осуществляемое по каналам связи.
Утечка информации – неконтролируемое распространение защищенной информации путем ее разглашения, несанкционированного доступа.
Уязвимость информации – возможность возникновения на каком-либо этапе жизненного цикла КС такого ее состояния, при котором создадутся условия для реальной угрозы безопасности в ней.
Фишеры (от англ. fisher – рыбак)– сравнительно недавно появившаяся разновидность Интернет-мошенников, которые обманным путем выманивают у доверчивых пользователей сети конфиденциальную информацию: различные пароли, пин-коды, данные, используя фальшивые электронные адреса и поддельные веб-сайты и т.п.

Фишинг (ловля на удочку) **–** это распространение поддельных сообщений от имени банков или финансовых компаний. Целью такого сообщения является сбор логинов, паролей и пин-кодов пользователей.
Фракеры **–** приверженцы электронного журнала Phrack, осуществляют взлом интрасети в познавательных целях для получения информации**.**
Хакер **–** в XIX веке называли плохих игроков в гольф, своего рода дилетантов.
Цель защиты информации– предотвращение ущерба собственнику, владельцу, пользователю информации в результате возможной утечки информации и/или несанкционированного и непреднамеренного воздействия на информацию.
Черный пиар **–** акция, которая имеет цель опорочить ту или иную фирму, компанию, политического кандидата и т.п.
Шифрование – изменение исходного текста так, чтобы скрыть от посторонних его содержание.
Шифрование информации **–** преобразование информации, в результате, которого содержание информации становится непонятным для субъекта, не имеющего соответствующего доступа. Результат шифрования называется шифротекстом.
Шифротекст **–** зашифрованное сообщение.
Экономические компьютерные преступления **–** являются наиболее распространенными. Они совершаются по корыстным мотивам и включают в себя компьютерное мошенничество, кражу программ («компьютерное пиратство»), кражу услуг и машинного времени, экономический шпионаж.
Электронная цифровая подпись **–** реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.
Электронная цифровая подпись (англ. digital signature)– это цифровой код (последовательность символов), присоединяемый к электронному сообщению для идентификации отправителя.
Электронный документ– документ, в котором информация представлена в электронно-цифровой форме.
Эффективность защиты информации **–** степень соответствия результатов защиты информации поставленной цели.
Защиты информации **–** степень соответствия результатов защиты поставленной цели. Объектом защиты может быть информация, ее носитель, информационный процесс, в отношении которого необходимо производить защиту в соответствии с поставленными целями.

Раздел 2. Основные понятия криптографии

2.1 Основные задачи и принципы криптографической защиты

Криптография — наука о методах обеспечения конфиденциальности и аутентичности информации. Математическая криптография возникла как наука о шифровании информации, т.е. как наука о криптосистемах. В классической модели системы секретной связи имеют место два полностью доверяющих друг другу участника, которым необходимо передавать между собой информацию, не предназначенную для третьих лиц. Такая информация называется конфиденциальной или секретной. Задача обеспечения конфиденциальности, т.е. защита секретной информации от противника - первая задача криптографии. Часто возникает ситуация, когда информация не является конфиденциальной, но важен факт поступления сообщений в неискаженном виде, т.е. наличие гарантии, что сообщение не было подделано. Такая гарантия называется обеспечением целостности информации и составляет вторую задачу криптографии.

При передаче электронных документов (в том числе и через Интернет) возможна как их подмена или редактура, так и — в случае секретного текста — доступ посторонних лиц к передаваемой информации. Таким образом, электронные документы также нуждаются в криптографической защите.

Возникают две основные задачи по их защите от несанкционированного доступа:

- Обеспечение уверенности получателя в том, что документ подлинный и корректный, т.е. при передаче не был подменен или отредактирован;
- Обеспечение невозможности доступа посторонних лиц к содержанию документа.

Когда речь идет об электронных документах, первая задача решается применением электронной подписи, вторая — зашифрованием документа.

Электронная подпись (ЭП) — цифровой аналог ручной подписи, обеспечивающий возможность проверки подлинности и корректности документа. Существует техническая возможность проверки электронной подписи: если документ подменен или искажен при передаче, подпись при проверке будет признана некорректной.

Зашифрование документа — видоизменение текста документа таким образом, что только тот или те, для кого текст документа предназначен, в состоянии восстановить исходный текст.

2.2 Криптографические программные продукты

Для защиты информации используются специальные пользовательские программные продукты. Они разделяются на две основные группы.

Первая группа, очень широко распространенная — это криптопровайдеры (или CSP, Cryptographic Service Providers). CSP не являются самостоятельными приложениями, они предоставляют криптографические функции другим приложениям — например, таким, как почтовые программы. Пользователь фактически не имеет дела непосредственно с CSP, работая с привычным ему пользовательским интерфейсом. CSP обладают универсальностью — один и тот же CSP может использоваться для работы со множеством различных программ. Примером такого продукта производства ООО «Криптоком» является криптопровайдер МагПро CSP.

Вторая группа — это библиотеки криптографических функций. Такие библиотеки содержат готовые функции, решающие криптографические задачи, и могут использоваться для создания новых приложений. Примером такого продукта производства ООО «Криптоком» является **программный продукт «МагПро КриптоПакет»**.

2.3 Криптографические алгоритмы

Для того чтобы с помощью электронной подписи можно было установить факт подмены или редактуры документа при передаче, необходимо, чтобы электронная подпись вырабатывалась на основе самого текста документа. Т.е. ЭП представляет собой последовательность символов, связанную с текстом документа так, что при изменении документа нарушается заданное соответствие между ЭП и текстом. Таким образом, для получения ЭП под документом нужно провести некоторое преобразование текста документа.

Для получения зашифрованного текста исходный текст также преобразовывается так, чтобы восстановление исходного текста было практически невозможным без знания определенной информации. Лица, обладающие этой информацией, должны быть в состоянии восстановить исходный текст. Очевидно, что информация, необходимая для восстановления текста (расшифрования), должна быть известна только адресатам.

Совокупность операций, которые производятся над текстом при криптографическом преобразовании, называется криптографическим алгоритмом.

В настоящее время существует множество криптографических алгоритмов, используемых для решения различных криптографических задач.

Алгоритмы, т.е. сами последовательности действий, не являются секретными.

2.4 Стандарты на криптографические алгоритмы

На криптографические алгоритмы существуют стандарты. Надежность алгоритмов, соответствующих стандартам, тщательно анализируется специалистами. При работе с официальной документацией разрешается пользоваться только алгоритмами, соответствующими стандартам.

В разных странах существуют различные стандарты на алгоритмы. В программном обеспечении широко используются алгоритмы, соответствующие американским стандартам, чаще всего это алгоритм RSA.

В России существуют собственные государственные стандарты на алгоритмы шифрования и выработки/проверки электронной подписи: **ГОСТ 28147-89**, **ГОСТ Р 34.10-94**, **ГОСТ Р 34.10-2001**.

Для выработки и проверки электронной подписи, а также зашифрования и расшифрования документов используются определенные последовательности действий, называемые криптографическими алгоритмами.

Криптографический алгоритм — это серьезная разработка, требующая немалого труда специалистов и отвечающая определенным требованиям. Одним и тем же алгоритмом может пользоваться для защиты информации большое количество пользователей, т.к. алгоритмы не являются секретной информацией.

На криптографические алгоритмы существуют стандарты, т.е. официально оформленные совокупности требований, которым эти алгоритмы должны отвечать. Эти стандарты различны в разных странах и изменяются со временем. Популярные американские алгоритмы — **RSA, DSA** и т.д. — которые часто используются в распространенных программных продуктах, отвечают американским стандартам.

В России также приняты государственные стандарты на криптографические алгоритмы. Российские производители, в том числе ООО «Криптоком», используют в своих программных продуктах алгоритмы, соответствующие российским стандартам.

2.5 Криптографические ключи

В качестве секретной информации используются криптографические ключи.

Криптографический ключ представляет собой последовательность символов, выработанную по определенным правилам. Эта последовательность используется при криптографических преобразованиях текстов. Для каждого криптографического алгоритма существуют свои требования, в соответствии с которыми создаются ключи. Каждый ключ создается для определенного алгоритма.

Для того чтобы обеспечить невоспроизводимость электронной подписи и невозможность прочтения зашифрованных текстов посторонними людьми, в криптографии применяются криптографические ключи.

Современный криптографический ключ — это последовательность чисел определенной длины, созданная по определенным правилам на основе последовательности случайных чисел. Для каждого ключа последовательность случайных чисел создается заново, ни одна последовательность не используется более одного раза. Для генерации последовательностей

случайных чисел используются специальные программные объекты или устройства, называемые датчиками случайных чисел.

Каждый алгоритм предъявляет собственные требования к ключам, поэтому любой криптографический ключ создается для определенного алгоритма и используется только с этим алгоритмом.

Если выработка электронной подписи и ее проверка, или зашифрование и расшифрование текста выполняются с помощью одного и того же ключа, такой подход называется **симметричной криптографией** (соответственно симметричные алгоритмы и симметричные ключи). Операции симметричной криптографии выполняются быстро и сравнительно просты. Но они требуют знания ключа по меньшей мере двумя людьми, что значительно повышает риск их компрометации (т.е. доступа к ним посторонних лиц).

Поэтому сейчас в основном используется **асимметричная криптография**. В асимметричной криптографии выработка электронной подписи или зашифрование выполняются на одном ключе, а проверка подписи или расшифрование — на другом, парном ключе.

В асимметричной криптографии применяются так называемые ключевые пары (key pairs). Каждая такая пара состоит из двух связанных между собой ключей. Один из этих ключей — закрытый (private key). Он известен только владельцу ключа и ни при каких условиях не должен быть доступен никому другому. Другой ключ — открытый (public key), он может быть доступен любому желающему.

Для выработки ЭП необходим закрытый ключ автора сообщения, для проверки — открытый. Таким образом, создать ЭП может только владелец закрытого ключа, а проверить — любой пользователь, получивший соответствующий открытый ключ.

Для зашифрования текста применяется открытый ключ адресата, для расшифрования — закрытый. Таким образом, зашифровать сообщение может любой человек, а расшифровать — только владелец соответствующего закрытого ключа, т.е. адресат.

Ключевая пара, используемая для работы с ЭП (выработки и проверки ЭП), называется ключами подписи (signature keys). Ключевая пара, используемая для зашифрования и расшифрования сообщений, называется ключами обмена (exchange keys).

Проблема асимметричной криптографии состоит в том, что зашифрование по асимметричным алгоритмам происходит намного медленнее, чем по

симметричным. Кроме того, если зашифрованный текст предназначен для нескольких адресатов, в отправляемое сообщение приходится включать копию текста для каждого адресата, что резко увеличивает как объем сообщения, так и время, необходимое для его зашифрования.

Эта проблема решается с помощью так называемой **гибридной криптографии.**

В процессе шифрования прежде всего создается одноразовый (так называемый сеансовый) ключ шифрования (session encryption key). Это симметричный ключ, т.е. один и тот же ключ используется и для зашифрования, и для расшифрования. Одноразовым или сеансовым он называется потому, что используется для зашифрования/расшифрования только одного сообщения.

На сеансовом ключе шифрования зашифровывается сообщение. Поскольку сообщение зашифровывается по симметричному алгоритму, процесс зашифровывания сообщения происходит достаточно быстро.

Затем сам ключ шифрования зашифровывается по асимметричному алгоритму на открытом ключе обмена получателя. Поскольку ключ шифрования представляет собой сравнительно небольшой объем данных, зашифрование такого ключа не занимает много времени.

Зашифрованный ключ шифрования включается в сообщение.

В результате сообщение получается незначительно больше по объему (за счет добавленной зашифрованной копии ключа шифрования), но процесс зашифрования происходит гораздо быстрее, чем если бы само сообщение зашифровывалось по асимметричному алгоритму.

Если получателей несколько, то сообщение зашифровывается один раз на сеансовом ключе шифрования, а ключ (сравнительно небольшой объем данных) зашифровывается отдельно на открытом ключе обмена каждого получателя. Таким образом, зашифрованное сообщение вместо нескольких копий сообщения, зашифрованных для каждого получателя, содержит одну зашифрованную копию сообщения и несколько копий одноразового сеансового ключа шифрования, зашифрованных для каждого получателя. Объем зашифрованного сообщения и время, необходимое для его зашифрования, оказываются существенно меньшими, чем если бы сообщение шифровалось по асимметричному алгоритму для каждого получателя.

Когда адресат получает сообщение, среди зашифрованных сеансовых ключей, включенных в сообщение, ищется сеансовый ключ, зашифрованный на открытом ключе обмена получателя. Если такой ключ находится, он

расшифровывается с помощью закрытого ключа обмена получателя, а потом с помощью этого ключа расшифровывается само сообщение.

Таким образом, основное требование к процессу зашифрования по асимметричному алгоритму — чтобы к закрытому ключу обмена никто не имел доступа, кроме владельца этого ключа — соблюдается. Для того, чтобы получить доступ к ключу шифрования, необходим доступ к закрытому ключу обмена; но после того, как произведено расшифрование ключа шифрования с помощью закрытого ключа обмена, этот ключ шифрования больше никогда не используется, так что говорить о его компрометации не имеет смысла.

2.6 Сертификаты

Сертификаты — это принятая сейчас форма хранения и передачи открытых ключей. Сертификат — это набор данных специального формата, содержащий сам открытый ключ и всю информацию о нем и о его владельце. Все открытые ключи хранятся и передаются в виде сертификатов.

Сертификаты выпускаются специальными уполномоченными центрами, которые могут носить различные названия: удостоверяющий центр, центр сертификации, пункт регистрации абонентов и т.д. В любом случае такой центр выполняет административные функции. Центр и пользователи (абоненты), которые пользуются услугами центра, составляют криптосеть.

Для того чтобы центр выпустил сертификат на открытый ключ, абоненту необходимо прислать заявку (запрос) на такой сертификат. Заявка содержит открытый ключ и всю информацию о нем и о владельце. Центр проверяет подлинность и корректность этой информации (как именно — зависит от регламента центра) и выпускает сертификат, заверяя его своей электронной подписью.

2.7 Цепочки доверия

Часто возникает необходимость проверять документ с помощью другого документа, который так же требует проверки. Например, подпись под документом проверяется с помощью сертификата на открытый ключ, парный тому секретному, на котором подпись выработана. Но сам сертификат — это тоже документ, корректность и подлинность которого требует проверки. Подпись под сертификатом проверяется на сертификате на открытый ключ подписи того центра, который выпустил сертификат. Сертификат центра, в свою очередь, тоже может быть подписан электронной подписью и требовать проверки.

Такие цепочки документов, каждый из которых проверяется на следующем, называются цепочками доверия.

Очевидно, что в конце концов цепочка заканчивается — в ней обязательно существует документ, который невозможно проверить на другом документе (например, самый первый сертификат центра). Такие документы могут называться самозаверенными, корневыми, доверенными и т.д. Существуют разные способы проверки корректности и подлинности таких документов, зависящие от используемого программного обеспечения и принятого регламента: контрольные записи, цифровые отпечатки и т.д. Общим во всех этих способах проверки является то, что они требуют участия каких-то бумажных документов (распечаток) и не могут быть проверены автоматически: необходимо, чтобы человек сравнил информацию из проверяемого электронного документа с распечатанной и убедился в совпадении.

Документ может считаться корректным только в том случае, если корректны все документы, входящие в цепочку доверия от данного документа до документа, которым заканчивается цепочка (корневого).

Разумеется, при каждой проверке подписи полной проверки цепочки доверия с участием человека не происходит. Обычно корневой документ проверяется при его установке на компьютер, а затем проверка цепочек доверия, заканчивающихся этим документом, происходит автоматически.

2.8. Датчики случайных чисел и создание ключей

Ключи создаются по специальным алгоритмам на основе последовательностей случайных чисел.

Для того чтобы криптографическая защита на ключе была надежной, последовательность случайных чисел, на которой создана ключевая пара, должна быть уникальной для каждой ключевой пары. Кроме того, она должна быть действительно случайной, т.е. не допускать повторов даже через очень большие промежутки.

Такие уникальные последовательности случайных чисел генерируются во время создания ключей с помощью специальных устройств или программ, называемых датчиками случайных чисел.

Очень удобны и быстры так называемые аппаратные датчики случайных чисел, представляющие собой физические устройства — платы, подключенные к компьютеру. Такие датчики создают последовательности случайных чисел на основе физических процессов. Генерация последовательностей случайных

чисел с помощью аппаратного датчика происходит очень быстро и без участия пользователя.

Но такие датчики устанавливаются не на каждом компьютере. Поэтому часто для создания ключей используется клавиатурный датчик случайных чисел~--- программа, использующая для создания последовательности случайных чисел физический процесс нажатия клавиш пользователем. Для инициализации такого датчика пользователю необходимо нажать определенное количество указываемых ему клавиш (если все клавиши нажаты безошибочно, то нужно 40 нажатий; если пользователь допускает ошибочные нажатия, количество необходимых нажатий увеличивается). Создание ключей с помощью клавиатурного датчика — более медленный процесс, чем создание ключей с помощью аппаратного датчика, но его можно осуществить на любом компьютере.

2.9 Хранение закрытых ключей

Для удобства хранения закрытых ключей может создаваться файл специального формата, в котором хранятся закрытые ключи. Файл, в свою очередь, может храниться на жестком диске компьютера, на дискете, на флэш-накопителе. Для защиты закрытого ключа от несанкционированного чтения он хранится в файле в зашифрованном виде, т.е. для того, чтобы прочитать закрытый ключ и воспользоваться им, необходимо знать пароль (парольную фразу), на которой зашифрован ключ.

Возможно также хранение закрытых ключей на внешних устройствах. Такие устройства должны иметь следующие свойства:

- Устройство должно включать в себя область памяти, достаточной, чтобы записать туда закрытые ключи (иногда эту область памяти называют «хранилищем ключей»);
- Устройство должно легко подключаться к компьютеру, чтобы ключи могли быть считаны;
- Устройство должно легко отключаться от компьютера, чтобы злоумышленники не могли считать с него ключи.

Таким условиям удовлетворяет **USB-токен «Вьюга»**, разработанный в ООО «Криптоком». Устройство «Вьюга» включает в себя генератор случайных чисел (т.е. может использоваться как датчик случайных чисел при генерации ключей) и область памяти объема, достаточного для хранения ключей. Устройство подключается к компьютеру через USB-порт. Возможно подключение устройства к компьютеру непосредственно в процессе работы.

2.10 Компрометация ключей

Компрометация ключей — понятие, которое включает в себя факт доступа посторонних лиц к секретным ключам, а также возможность такого доступа или подозрение на него. Скомпрометированный секретный ключ — главная опасность для любой системы защиты информации, поэтому принимаются специальные меры для защиты секретных ключей: их никогда не записывают на жесткий диск компьютера, их держат на отдельных носителях, их зашифровывают, их защищают на пароле и т.д. Тем не менее, случаи компрометации возможны.

В случае компрометации секретный ключ и парный к нему открытый вносятся в специальные списки, содержащие скомпрометированные ключи. Такие списки в разных криптографических продуктах также могут называться по-разному — стоп-листы, списки отзыва сертификатов и т.д. Действие скомпрометированных ключей прекращается. Подпись, выработанная на скомпрометированном ключе, автоматически считается некорректной; информацию из документа, зашифрованного на скомпрометированном ключе, нельзя считать секретной.

Владелец скомпрометированных ключей создает для себя новые ключи.

Раздел 3. Симметричные и асимметричные алгоритмы

Для симметричной криптосистемы характерно применение одного и того же ключа, как при шифровании, так и при дешифровании сообщений. В асимметричных криптосистемах для дешифрования данных используется один (общедоступный) ключ, а для дешифрования – другой (секретный) ключ.

3.1 Алгоритм Диффи-Хеллмана

Этот алгоритм предполагает, что два абонента дистанционно будут генерировать ключ для шифрования в дальнейшем, например, каким-либо симметричным алгоритмом. Алгоритм Диффи-Хеллмана (1976 год) использует функцию дискретного возведения в степень.

Последовательность действий в алгоритме Диффи-Хелмана:

1. Сначала генерируются два больших простых числа **n** и **q**. Эти два числа не обязательно хранить в секрете.

2. Далее один из партнеров **P1** генерирует случайное число **x** и посылает другому участнику будущих обменов **P2** значение $\mathbf{A = q^x \bmod n}$.

3. По получении **A** партнер **P2** генерирует случайное число **y** и посылает P2 вычисленное значение $\mathbf{B = q^y \bmod n}$.

4. Партнер **P1,** получив **B,** вычисляет $\mathbf{K_x = B^x \bmod n}$.

5. Партнер **P2,** получив **A** вычисляет $\mathbf{K_y = A^y \bmod n}$.

6. Алгоритм гарантирует, что числа $\mathbf{K_y}$ и $\mathbf{K_x}$ равны и могут быть использованы в качестве секретного ключа для шифрования.

Как видно из алгоритма, даже «перехватив» числа A и B, вычислить $\mathbf{K_x}$ или $\mathbf{K_y}$ невозможно.

Пример. Представим итерации алгоритма в виде последовательности действий партнеров в табличной форме (табл. 2.1). *Таблица 2.1*

№ пп	Действия партнеров	
	Партнер P1	Партнер P2
1	Генерация двух больших простых чисел и обмен ими. Пусть **n** = 17, **q** = 11	
2	Генерируем случайное число **x,** **x = 5.** Вычисляем $\mathbf{A = q^x \bmod n = 11^5 \bmod 17 = 10}$ Посылаем значение **A** партнеру	Получено **A = 10** Генерируем случайное число **y,** **y = 7.** Вычисляем $\mathbf{B = q^y \bmod n = 11^7 \bmod 17 = 3}$ Посылаем значение **B** партнеру
3	Получено **B = 3** Вычисляем $\mathbf{K_x = B^x \bmod n = 3^5 \bmod 17 = 5}$	Получено **A = 10** Вычисляем $\mathbf{K_y = A^y \bmod n = 10^7 \bmod 17 = 5}$
4	Сравниваем $\mathbf{K_y}$ и $\mathbf{K_x}$, **5 = 5**	Сравниваем $\mathbf{K_y}$ и $\mathbf{K_x}$, **5 = 5**
	Ключом для шифрования является 5	

Совместным ключом для шифрования будет 5.

3.2 Алгоритм шифрования данных RSA

Алгоритм предложен в 1978 году авторами Rivest, Shamir и Aldeman и основан на трудности разложения больших целых чисел на простые множители. В результате реализации алгоритма имеем пару ключей: первый в дальнейшем используется только для шифрования (открытый ключ), второй для дешифрования (закрытый ключ). При этом, знание одного из ключей не позволяет определить другой ключ. Сгенерированные ключи могут многократно использоваться для шифрования информации.

Последовательность действий пользователя для получения ключей:

1. Получатель выбирает 2 больших простых целых числа p и q, на основе которых вычисляет $N = p^* q$; $M = (p\text{-}1) * (q\text{-}1)$.

2. Получатель выбирает целое случайное число d, которое является взаимно простым со значением M.

3. Вычисляем значение e из условия $(ed) \bmod M = 1$.

4. d и N публикуются как открытый ключ, e и N являются закрытым ключом.

Действия по шифрованию сообщения.

5. Если S – сообщение и его длина: $1 < \text{Len}(S) < N$, то оно шифруется выполнением операции $\boldsymbol{S_ш = S^d \bmod N}$ (то есть, **открытым ключом**).

Действия по дешифрованию сообщения.

6. *Получатель* дешифровывает сообщение с помощью **закрытого ключа** выполнением операции $\boldsymbol{S = S_ш^e \bmod N}$.

Если длина сообщения превышает N, то сообщение делится на фрагменты длины, не превосходящие N.

Рассмотрим реализацию алгоритма на примере. Заметим, что в реальных алгоритмах в качестве простых чисел выбираются отстоящие друг от друга большие числа, порядка 2^{128} – 2^{1024}, поиск которых, вообще говоря, и определяют сложность алгоритма для криптоанализа.

Далее представлены шаги алгоритма:

1. *Выбираем p = 19, q = 13, N = p*q = 247,*

2. *Вычисляем формулу Эйлера M = (p – 1)*(q – 1) = 18* x *12 = 216.*

3. Выбираем целое случайное число *d*, взаимно простое с *M*, *d = 35*. (Действительно, *d* и *M* не имеют общих делителей *35 = 7* x *5*, *216 = 2* x *2* x *2* x *3* x *3* x *3*).

4. Вычисляем *e* такое, что *(e d)* mod *M = 1*, *e = 179*.

5. *(d,N)* **открытый ключ**, т.е. *(35,247)*, *(e,N)*–**закрытый ключ** *(179, 247)*.

6. Шифрование сообщения *2 3 5* **,** используя **открытый ключ** *(35, 247)* по формуле $S_ш = S^d \bmod N$:

$2 \Rightarrow 2^{35} \bmod 247 = 124,$

$3 \Rightarrow 3^{35} \bmod 247 = 165,$

$5 \Rightarrow 5^{35} \bmod 247 = 99.$

Таким образом, шифрованное сообщение имеет вид *124 165 99.*

7. Дешифровка сообщения *124 165 99*, используя закрытый **ключ** *(179, 247)* по формуле $S = S_ш^e \bmod N$:

$124 \Rightarrow 124^{179} \bmod 247 = 2,$

$165 \Rightarrow 165^{179} \bmod 247 = 3,$

$99 \Rightarrow 99^{179} \bmod 247 = 5.$

Расшифрованное сообщение *2 3 5*.

8. Для получения математических расчетов (численной реализации алгоритма RSA) использовать https://web 2.0 calc.com.

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ВЫПОЛНЕНИЯ КОНТРОЛЬНОЙ РАБОТЫ

Контрольная работа представляет собой

a) Титульный лист (Приложение №1);

b) Задание, выполненное согласно номеру варианта;

c) Список использованной литературы.

Варианты заданий дифференцированы по уровню сложности и максимальной оценке за правильное выполнение.

Требования к оформлению и баллы оценки:

1. Заголовки каждой главы (раздела) располагают посередине страницы без точки на конце и печатают прописными буквами, жирным шрифтом. Переносить слова в заголовке не допускается. Названия параграфов печатают строчными буквами и располагают с абзацным отступом 1,25 без строчки в конце.

2. Работа должна быть выполнена печатным способом с использованием компьютера и принтера на одной стороне листа белой бумаги формата А4 через полтора интервала и размером шрифта 14 пунктов.

3. Страницы должны иметь следующие поля: левое - 25 мм, правое - 10 мм, верхнее - 20 мм, нижнее - 20 мм. Абзацный отступ должен быть одинаковым по всему тексту и равен 5-ти знакам. Все страницы, включая иллюстрации и приложения, нумеруются по порядку без пропусков и повторений. Первой страницей считается титульный лист, на котором нумерация страниц не ставится, на следующей странице ставится цифра "2" и т.д. Порядковый номер страницы печатают на середине верхнего поля страницы.

4. Иллюстративный материал может быть представлен рисунками, фотографиями, графиками, схемами, диаграммами и другим подобным материалом. Иллюстрации размещают под текстом, в котором впервые дана ссылка на них, или на следующей странице, а при необходимости - в приложении к контрольной работе. Иллюстрации нумеруют арабскими цифрами сквозной нумерацией или в пределах главы (раздела). Под рисунком посередине страницы делается запись «Рисунок 1- название рисунка» без точки в конце. На все иллюстрации должны быть приведены ссылки в тексте работы. При ссылке следует писать слово "Рисунок" с указанием его номера.

Используемые таблицы размещают под текстом, в котором впервые дана ссылка на них, или на следующей странице, а при необходимости - в приложении к контрольной работе. Таблицы нумеруют арабскими цифрами сквозной нумерацией или в пределах главы (раздела). Над таблицей с абзацным доступом 1,25 делается запись «Таблица 1- название таблицы» без точки в конце. На все таблицы должны быть приведены ссылки в тексте ВКР. При ссылке следует писать слово "Таблица" с указанием ее номера.

5. Список использованных источников должен быть размещен в конце основного текста. Допускаются следующие способы группировки библиографических записей: алфавитный, систематический (в порядке первого упоминания в тексте), хронологический.

При алфавитном способе группировки все библиографические записи располагают по алфавиту фамилий авторов или первых слов заглавий документов. Библиографические записи произведений авторов-однофамильцев располагают в алфавите их инициалов.

При систематической (тематической) группировке материала библиографические записи располагают в определенной логической последовательности в соответствии с принятой системой классификации.

При хронологическом порядке группировки библиографические записи располагают в хронологии выхода документов в свет.

6. Контрольная работа оценивается по 5 балльной системе, пределы оценки заданий

I задание - 0-1 балл,
II задание - 0-2 балла,
III задание - 0-1 балл.

Срок сдачи контрольной работы

Обучающие обязательно должны сдать контрольную работу на проверку не позднее, чем за 10 дней до экзамена или зачета. Без выполнения контрольной работы студенты не допускается до сдачи экзамена или зачета.

СТРУКТУРА И СОДЕРАЖНИЕ КОНТРОЛЬНОЙ РАБОТЫ

1. **Титульный лист**
2. **Задание**
3. **Список литературы**

ЗАДАНИЕ НА КОНТРОЛЬНУЮ РАБОТУ

Задание I
Правовая защита информации

Правовое обеспечение безопасности информационных ресурсов
Цель задания: Ознакомление с нормативно-правовыми актами в сфере обеспечения безопасности информации.

Задача № 1. Подберите перечень нормативно-правовых актов необходимых для решения следующих задач:
1.Производство шифровальной техники
2. Эксплуатация шифровальной техники
3. Обеспечение безопасности информации, обрабатываемой на средствах вычислительной техники и отнесенной к государственной тайне
4. Обеспечение безопасности информации (банковская информация), передаваемой по каналам глобальной сети
5. Разработка для государственных структур всевозможных технических средств для идентификации пользователе.

Задача №2. Дайте краткую характеристику подобранных вами нормативно правовых актов.

Задача №3. Исследуйте самостоятельно вопрос - законодательное обеспечение безопасности от опасной информации. Приведите примеры нормативно правовых актов защиты от опасной информации.

Задача №4. Охарактеризуйте деятельность Федеральной службы по техническому и экспортному контролю (ФСТЭК).

Задача № 5. Проанализируйте основные документы ФСТЭК, приведите пример законодательно-нормативного обеспечения безопасности информации, обрабатываемой в локальной сети предприятия, имеющей доступ в Интернет.

А) Действия по организационно-методическому обеспечению
В) Действия технических специалистов

Задание II
Криптографическая защита информации

Создание зашифрованного сообщения при помощи алгоритмов шифрования.
Цель задания: получение навыков создания зашифрованного сообщения.

1.Сгенерировать ключи для алгоритма Диффи-Хеллмана, зашифровать и расшифровать 3 последние цифры зачетной книжки
2.Сгенерировать ключи алгоритма RSA – зашифровать и расшифровать 3 произвольных числа
3.По алгоритму шифрования Эль Гамаля – зашифровать и расшифровать свою фамилию
4.Организация переписки между 5-ю абонентами по алгоритму Эль Гамаля – зашифровать и расшифровать сверхвозрастающую последовательность из 5 чисел.
5.Шифрование открытым ключом. С помощью алгоритма на основе задачи упаковки ранца – зашифровать и расшифровать свое имя.

Задание III
Организационная защита информации
Анализ защищенность объектов критической инфраструктуры.

Цель задания: изучение средств, методов, способов защиты информации.

Проанализировать защищенности объекта защиты информации.
Описать объект защиты, провести анализ защищенности объекта защиты информации по следующим разделам:
- виды угроз;
- характер происхождения угроз;
- классы каналов несанкционированного получения информации;
- источники появления угроз;
- причины нарушения целостности информации;
- способы, методы, средства защиты информационных ресурсов объекта.

К объектам критической инфраструктуры относятся:

государственный орган, государственное учреждение, российское юридическое лицо и (или) индивидуальный предприниматель, которому на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере:

– здравоохранения ,

– науки,

– транспорта,

– связи,

– энергетики,

– банковской сфере и иных сферах финансового рынка,

– топливно-энергетического комплекса,

– атомной энергии,

– оборонной промышленности,

– ракетно-космической промышленности,

– горнодобывающей промышленности,

– металлургической промышленности,

– химической промышленности;

Исходные данные задания:

Вариант задания соответствует порядковому номеру студента в экзаменационной ведомости и формируется по позиции объекта критической инфраструктуры и объекта защиты. Наименование объекта защиты информации:

1) Одиночно стоящий компьютер в бухгалтерии комбината химической промышленности.

2) Сервер в бухгалтерии комбината металлургической промышленности.

3) Почтовый сервер на станции атомной энергии.

4) Веб-сервер на комбинате горнодобывающей промышленности .

5)Компьютерная сеть материальной группы ракетно-космической промышленности.

6)Одноранговая локальная сеть без выхода в Интернет топливно-энергетического комплекса.

7)Одноранговая локальная сеть с выходом в Интернет топливно-энергетического комплекса.

8) Сеть с выделенным сервером без выхода в Интернет банковской сфере и иных сферах финансового рынка.

9) Сеть с выделенным сервером с выхода в Интернет банковской сфере и иных сферах финансового рынка.

10) Телефонная база данных (содержащая и информацию ограниченного пользования) в твердой копии и на электронных носителях министерства здравоохранения.

11) Телефонная сеть атомной станции.

12) Средства телекоммуникации (радиотелефоны, мобильные телефоны).

13) Банковские операции (внесение денег на счет и снятие) банковской сфере и иных сферах финансового рынка.

14) Операции с банковскими пластиковыми карточками банковской сфере и иных сферах финансового рынка.

15) Компьютер, хранящий конфиденциальную информацию о сотрудниках университета.

16) Компьютер, хранящий конфиденциальную информацию о разработках предприятия оборонной промышленности.

17) Материалы для служебного пользования на твердых и электронных носителях и на электронных носителях в производстве топливно-энергетического комплекса.

18) Материалы для служебного пользования на твердых носителях и электронных носителях, на закрытом предприятии оборонной промышленности.

19) Материалы для служебного пользования на электронных носителях в архиве транспортного предприятия.

20) Материалы для служебного пользования на электронных и твердых носителях и на электронных носителях в налоговой инспекции.

21) Комната для переговоров по сделкам на охраняемой территории.

22) Комната для переговоров по сделкам на неохраняемой территории.

23) Сведения для средств массовой информации, цензура на различных носителях информации (твердая копия, фотографии, электронные носители и др.).

24) Судебные материалы (твердая копия и на электронных носителях).

25) Документы паспортного стола РОВД (твердая копия и на электронных носителях).

ЛИТЕРАТУРА ДЛЯ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ И ВЫПОЛНЕНИЯ КОНТРОЛЬНОЙ РАБОТЫ:

Основная литература

1. Практическая криптография / М. Масленников .— Санкт-Петербург : БХВ-Петербург, 2015 .— 465 с. Доступ по паролю из сети Интернет (чтение) .— ISBN 978-5-9775-1884-0 .— http://ibooks.ru/reading.php?short=1&isbn=978-5-9775-1884-0.
2. Криптография и безопасность в технологии .NET / П. Торстейнсон .— Москва : БИНОМ. Лаборатория знаний, 2015.—482 с. http://ibooks.ru/reading.php?short=1&isbn=978-5-9963-2952-6.
3. Павлов, В. Н. Информационные технологии и защита информации [Электронный ресурс] : учебно-методическое пособие по направлениям подготовки: 080200, 100100, 100700 / М-во образования и науки РФ, ФГБОУ ВПО "С.-Петерб. гос. торг.-экон. ун-т", Каф. информ. систем и информ. технологий .— Электрон. текстовые дан.— Санкт-Петербург: [б. и.], 2015 . http://elib.spbstu.ru/dl/tei/public/10394.pdf.
4. Метод текстовой стеганографии, основанный на применении цепей Маркова = Method of text steganography based on Markov chains / А. Н. Шниперов, К. А. Никитина // Проблемы информационной безопасности. Компьютерные системы / Министерство образования и науки РФ; Санкт-Петербургский государственный политехнический университет. — СПб., 2016 .— № 1 .— С. 94-101 .

Дополнительная литература

1. Безопасность информационных систем. Авторы: Ерохин В.В.Москва: Флинта, 2015 г., 182 с.
2. Безопасность систем баз данных.Авторы: Скрыпников А.В., Родин С.В., Перминов Г.В., Чернышова Е.В.Воронеж: ВГУИТ, 2015 г. , 139
3. Построения защищенных от исследования систем на примере алгоритмов шифрования = Establishing systems protected from research with implementation in encryption algorithms / М. А. Стюгин // Проблемы информационной безопасности. Компьютерные системы / Министерство образования и науки РФ; Санкт-Петербургский государственный политехнический университет. - СПб., 2016. — № 4 .— С. 89-96
4. Реализация симметричного шифрования по алгоритму ГОСТ 28147-89 на графическом процессоре = Realization symmetric encryption on algorithm GOST 28147-89 with GPU / М. Е. Сухопаров, И. С. Лебедев // Проблемы информационной безопасности. Компьютерные системы / Министерство образования и науки РФ; Санкт-Петербургский государственный политехнический университет. - СПб., 2016. — № 2 .— С. 101-105 .

Интернет-источники:

1. https://ru.wikipedia.org/wiki
2. http://www.intuit.ru/studies/courses/10/10/lecture/302?page=2
3. http://cryptography.ru/
4. http://cryptowiki.net/
5. http://linuxgeeks.ru/

Приложения 1

Таблица 3.1

Таблица простых чисел от 1 до 200

1	2	3	5	7	11	13	17	19	23
29	31	37	41	43	47	53	59	61	67
71	73	79	83	89	97	101	103	107	109
113	127	131	137	139	149	151	157	163	167
173	179	181	191	193	197	199			

Таблица 3.2

Последовательность цифр для шифрования

Варианты заданий (последняя цифра номера варианта)									
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*0*
478 956	*598 274*	*854 973*	*972 856*	*726 593*	*648 937*	*275 384*	*765 243*	*475 938*	*815 634*

Таблица 3.3

Простейшие ключи для алгоритма RSA

№ пп	Открытый ключ	Закрытый ключ	№ пп	Открытый ключ	Закрытый ключ	№ пп	Открытый ключ	Закрытый ключ
1	(35,21)	(11,21)	8	(35,35)	(11,35)	15	(35,221)	(11,221)
2	(15,15)	(7,15)	9	(77,77)	(53,77)	16	(35,247)	(179,247)
3	(35,119)	(11,119)	10	(35,91)	(35,91)	17	(35,323)	(107,323)

4	(21,33)	(21,33)	11	(35,161)	(83,161)	18	(35,437)	(215,437)
5	(15,85)	(47,85)	12	(35,133)	(71,133)	19	(15,391)	(47,391)
6	(35,65)	(11,65)	13	(77,209)	(173,209)	20	(35,299)	(83,299)
7	(21,55)	(21,55)	14	(21,187)	(61,187)	21	(15,69)	(3,69)

1. Криптосистема Эль-Гамаля

Эта система открытого шифрования предложена Тахер Эль-Гамалем (ElGamal), египетским шифровальщиком в 1985 р.

В отличие от RSA алгоритм Эль-Гамаля не был запатентован и, поэтому, стал более дешевой альтернативой, так как не требовалась оплата взносов за лицензию.

Основана на трудности вычисления дискретных логарифмов в конечном поле.

Организация шифрованной переписки ***с помощью системы Эль-Гамаля***

Пусть пользователь **А** хочет получить шифрованное сообщение от пользователя **В**.

Пользователь **А** должен**:**

1) выбрать простое большое число p и найти первообразный корень g по модулю p (g – первообразный корень, если $g^{p-1} \equiv 1 (\mathrm{mod}\, p)$ и p не делится на g).

2) выбрать случайное целое число a **из интервала** $(1;\ p-2)$**. Число** a – *закрытый ключ* **пользователя** А**;**

3) вычислить $h = g^a (\mathrm{mod}\ p)$**.** *Открытый ключ* **пользователя** А – **тройка чисел** p, g, h**.**

4) открытым каналом передать пользователю В *открытый ключ* p, g, h**.**

Пользователь **B** должен:

1) **выбрать случайным образом рандомизатор** r **– произвольное целое число из отрезка** $[1; p-1]$**;**
2) **разбить свое сообщение на блоки** $x < p$ **и зашифровать их по формулам**

$$y_1 = g^r \pmod p, \qquad y_2 = x \cdot h^r \pmod p;$$

3) криптограммой открытого текста x **есть пара** $y = (y_1; y_2)$**. Ее он отсылает пользователю** A**.**

Чтобы дешифровать криптограмму, пользователь A **на своем закрытом ключе вычисляет**

$$x \equiv y_2 \cdot (y_1^a)^{-1} \pmod p.$$

Докажем корректность такого шифрования. Так как $g-$ **первообразный корень по модулю** p**, то**

$$y_2 \cdot (y_1^a)^{-1} \pmod p \equiv x \cdot h^r \cdot ((g^r)^a)^{-1} \pmod p \equiv x \cdot h^r (g^a)^r)^{-1} \pmod p \equiv$$

$$\equiv x \cdot h^r \cdot h^{-r} \pmod p \equiv x.$$

Пример 1. Сгенерировать открытый и закрытый ключи для криптосистемы Эль-Гамаля и зашифровать сообщение СКЛО.

Р е ш е н и е. СКЛО = 21 14 15 18. Делим на блоки 2114, 1518, т.е. $x = 2114, \quad x' = 1518$

Выберем простое число $p = 2179$**, большее, чем блоки. Находим первообразный корень** $g = 7$ **по модулю** 2179 **(для корня выполнено условие** $g^{p-1} \equiv 1 \pmod p$**). Теперь случайно выберем целое число** $a = 8$ **из интервала** $(1; 2177)$ **– это закрытый ключ.**

$$h = g^a (\mathrm{mod}\ p) = 7^8 (\mathrm{mod}\, 2179) \equiv 1346.$$

$(2179,\ 7,\ 1346)$ – открытый ключ. Из отрезка $[1;10]$ выберем рандомизатор $r = 9$ и зашифруем:

$$y_1 = g^r (\mathrm{mod}\ p) \equiv 7^9 (\mathrm{mod}\, 2179) \equiv 706;$$

$$y_2 = x \cdot h^r (\mathrm{mod}\ p) \equiv 2114 \cdot 1346^9 (\mathrm{mod}\, 2179) \equiv 51;$$

$$y_2{}' = x' \cdot h^r (\mathrm{mod}\ p) \equiv 1518 \cdot 1346^9 (\mathrm{mod} 11) \equiv 1055.$$

Криптограмма $y = (706;\ 51)$ и $y = (706; 1055)$. Для дешифрования находим

$$x = y_2 \cdot (y_1^a)^{-1} (\mathrm{mod}\ p) = 51 \cdot (706^8)^{-1} (\mathrm{mod}\, 2179) \equiv$$

$$\equiv 51 \cdot 1139^{-1} (\mathrm{mod}\, 2179) \equiv 51 \cdot 2135 (\mathrm{mod}\, 2179) \equiv 2114 = CK$$

Аналогично $x' = 1055$=ЛО.

Криптосистему Эль-Гамаля можно использовать в любой конечной группе в мультипликативной группе $GF(2^m)$ характеристики 2 или в группе точек эллиптической кривой над конечным полем.

Алгоритм стал базой для принятия стандартов цифровой подписи: национального стандарта США (DSA) –1994 г. и государственного стандарта Российской федерации ГОСТ Р 34.10. – 1995 г.

1. Алгоритм передачи сообщений - 5 абонентов

По таблице 3 выбрать сообщение m и секретный ключ x и провести шифрование по методу Эль-Гамаля для пяти абонентов. Вариант задания определяется последними цифрами номера студенческого билета. По номеру i (предпоследняя цифра) студент выбирает сообщение для зашифровывания, по j (последняя цифра) – требуемые для реализации этого алгоритма секретный ключ x. Исходные данные для других четырех секретных ключей x выбираются циклически по процедуре (i+1) и (j+1).

p=23, g=7, m=15, m=13, m=5, m=7,m=9

Решение:

Пусть имеются абоненты A, B, C, D, E которые хотят передавать друг другу зашифрованные сообщения, не имея никаких защищенных каналов связи. Шифр Эль – Гамаля решает эту задачу, используя, в отличие от шифра Шамира, только одну пересылку сообщения. Фактически здесь используется схема Диффи – Хеллмана, чтобы сформировать общий секретный ключ для двух абонентов, передающих друг другу сообщение, и затем сообщение шифруется путем умножения его на этот ключ. Для каждого следующего сообщения секретный ключ вычисляется заново.

Для всей группы абонентов выбираются некоторое большое простое число p и число g, такие, что различные степени g суть различные числа по модулю p. Числа p и g передаются абонентам в открытом виде (они могут использоваться всеми абонентами сети).

Нам необходимо выбрать числа p и g так, чтобы они отвечали следующим требованиям:

$$g^q \bmod p \quad 1,$$

где p=2q+1.

Возьмем p= 23 и g=7.

$$2q+1=23 \quad q=11$$

Проверим соотношение:

$$7^{11} \bmod 23 \Rightarrow \textbf{\textit{22}} \quad \textbf{\textit{1}} \textbf{\textit{ – выполняется.}}$$

Затем каждый абонент группы выбирает свое секретное число c_i:

$1 < C_i < p - 1$

(см. таблицу 5.1), и вычисляет соответствующее ему открытое число d_i:

$d_i=g^{ci} \bmod p$ (3.1)

$$d_a = 7^3 \bmod 23 = 21$$

$$d_b = 7^5 \bmod 23 = 17$$

$$d_c = 7^7 \bmod 23 = 5$$

$$d_d = 7^{11} \bmod 23 = 22$$

$$d_e = 7^{13} \bmod 23 = 20$$

Т а б л и ц а 5.1 – Ключи пользователей в системе Эль – Гамаля

Абонент	Секретный ключ	Открытый ключ
A	3	21
B	5	17
C	7	5
D	11	22
E	13	20

Покажем теперь, как A передает сообщение m абоненту B. Будем предполагать, как и при описании шифра Шамира, что сообщение представлено в виде числа

$m < p$.

Шаг 1. A формирует случайное число к, 1 к p-2, вычисляет числа

$r=g^k \bmod p$, (3.2)

$e=m^* d_B^k \bmod p$, (3.3)

и передает пару чисел (r, e) абоненту B.

Шаг 2. B, получив (r,e), вычисляет

$m'= e^* r^{p-1-c_B} \bmod p$ (3.4)

Утверждение (свойства шифра Эль-Гамаля):

1) Абонент B получил сообщение, т.е. m'=m;

2) противник, зная p, g, d_B, r и e, не может вычислить m.

- Передадим сообщение m = 15 от *E к A*. Возьмем p = 23, g = 7. Пусть абонент A выбрал для себя секретное число c_a= 3 и вычислил по (3.1) d_a=21.

Абонент Q выбирает случайно число k, например k = 8, и вычисляет по (3.2), (3.3):

$r = 7^8 \bmod 23 = 12,$

$e = 15 * 21^8 \bmod 23 = 22$

Теперь Q посылает к A зашифрованное сообщение в виде пары чисел. A вычисляет по (3.4):

$m' = 22 * 12^{23-1-3} \bmod 23 = 15.$

Мы видим, что A смог расшифровать переданное сообщение.

Ясно, что по аналогичной схеме могут передавать сообщения все абоненты в сети. Заметим, что любой абонент, знающий открытый ключ абонента B, может посылать ему сообщения, зашифрованные с помощью открытого ключа d_a. Но только абонент A, и никто другой, может расшифровать эти сообщения, используя известный только ему секретный ключ c_a. Отметим также, что объем шифра в два раза превышает объем сообщения, но требуется только одна передача данных (при условии, что таблица с открытыми ключами заранее известна всем абонентам).

- Передадим сообщение m=13 от *A к B*. p = 23, g = 7. Пусть абонент B выбрал для себя секретное число c_b = 5 и вычислил по (3.1) d_b = 17.

Абонент A выбирает случайно число k, например k = 6, и вычисляет по (3.2), (3.3):

$r = 7^6 \bmod 23 = 4$

$e = 13 \cdot 17^6 \bmod 23 = 18.$

Теперь A посылает к B зашифрованное сообщение в виде пары чисел. B вычисляет по (3.4):

$m' = 18 * 4^{23-1-5} \bmod 23 = 13$

Мы видим, что B смог расшифровать переданное сообщение.

- Передадим сообщение m= 5 от *B к C*. (p = 23, g = 7). Пусть абонент C выбрал для себя секретное число c_C = 7 и вычислил по (3.1) d_C=5.

Абонент B выбирает случайно число k, например k = 5, и вычисляет по (3.2), (3.3):

$r = 7^5 \bmod 23 = 17$,

$e = 5*5^5 \bmod 23 = 8$.

Теперь B посылает к C зашифрованное сообщение в виде пары чисел. C вычисляет по (3.4):

$m' = 8*17^{23-1-7} \bmod 23 = 5$.

Мы видим, что C смог расшифровать переданное сообщение.

- Передадим сообщение m= 7 от *C к D*. (p = 23, g = 7). Пусть абонент D выбрал для себя секретное число c_C =11 и вычислил по (3.1) d_C=22.

Абонент C выбирает случайно число k, например k = 4, и вычисляет по (3.2), (3.3):

$r = 7^4 \bmod 23 = 9$,

$e = 7*22^4 \bmod 23 = 7$.

Теперь C посылает к D зашифрованное сообщение в виде пары чисел. D вычисляет по (3.4):

$m' = 7*9^{23-1-11} \bmod 23 = 7$.

Мы видим, что D смог расшифровать переданное сообщение.

- Передадим сообщение m= 9 от *D к E*. (p = 23, g = 7). Пусть абонент E выбрал для себя секретное число c_C =13 и вычислил по (3.1) d_C=20.

Абонент D выбирает случайно число k, например k = 3, и вычисляет по (3.2), (3.3):

$r = 7^3 \bmod 23 = 21$,

$e = 9*20^3 \bmod 23 = 10$.

Теперь D посылает к E зашифрованное сообщение в виде пары чисел. E вычисляет по (3.4):

$m' = 10*21^{23-1-13} \bmod 23 = 9.$

Мы видим, что E смог расшифровать переданное сообщение.

2. Алгоритм- задача на основе упаковки ранца.

В 1978 г. Меркль и Хеллман предложили использовать задачу об укладке ранца (рюкзака) для асимметричного шифрования. Она относится к классу NP-полных задач и формулируется следующим образом. Дано множество предметов различного веса. Спрашивается, можно ли положить некоторые из этих предметов в ранец так, чтобы его вес стал равен определенному значению? Более формально задача формулируется так: дан набор значений $\mathbf{M_1}$, $\mathbf{M_2}$, ..., $\mathbf{M_n}$ и суммарное значение **S**; требуется вычислить значения $\mathbf{b_i}$ такие что

$$S = b_1M_1 + b_2M_2 + ... + b_nM_n, \qquad (1)$$

где n – количество предметов;

b_i - бинарный множитель. Значение $b_i = 1$ означает, что предмет i кладут в рюкзак, $b_i = 0$ - не кладут.

Например, веса предметов имеют значения 1, 5, 6, 11, 14, 20, 32 и 43. При этом можно упаковать рюкзак так, чтобы его вес стал равен 22, использовав предметы весом 5, 6 и 11. Невозможно упаковать рюкзак так, чтобы его вес стал равен 24.

В основе алгоритма, предложенного Мерклом и Хеллманом, лежит идея шифрования сообщения на основе решения серии задач укладки ранца. Предметы из кучи выбираются с помощью блока открытого текста, длина которого (в битах) равна количеству предметов в куче. При этом биты открытого текста соответствуют значениям **b**, а текст является полученным суммарным весом. Пример шифрограммы, полученной с помощью задачи об укладке ранца, показан в следующей таблице.

Таблица 1. Пример шифрования на основе задачи об укладке ранца

Открытый текст	1 1 1 0 0 1 0 0	0 1 0 1 1 0 0 1	0 0 0 0 0 0 0 0
Рюкзак (ключ)	1 5 6 11 14 20 32 43	1 5 6 11 14 20 32 43	1 5 6 11 14 20 32 43
Шифрограмма	32 (1+5+6+20)	73 (5+11+14+43)	0

Суть использования данного подхода для шифрования состоит в том, что на самом деле существуют две различные задачи укладки ранца - одна из них решается легко и характеризуется линейным ростом трудоемкости, а другая, как принято считать, нет. Легкий для укладки ранец можно превратить в трудный. Раз так, то можно применить в качестве открытого ключа **трудный** для укладки ранец, который легко использовать для шифрования, но невозможно - для дешифрования. А в качестве закрытого ключа применить **легкий** для укладки ранец, который предоставляет простой способ дешифрования сообщения.

В качестве закрытого ключа (легкого для укладки ранца) используется сверхвозрастающая последовательность.

Сверхвозрастающей называется **последовательность**, в которой каждый последующий член больше суммы всех предыдущих. Например, последовательность {2, 3, 6, 13, 27, 52, 105, 210} является сверхвозрастающей, а {1, 3, 4, 9, 15, 25, 48, 76} - нет.

Решение для сверхвозрастающего ранца найти легко. В качестве текущего выбирается полный вес, который надо получить, и сравнивается с весом самого тяжелого предмета в ранце. Если текущий вес меньше веса данного предмета, то его в рюкзак не кладут, в противном случае его укладывают в рюкзак. Уменьшают текущий вес на вес положенного предмета и переходят к следующему по весу предмету в последовательности. Шаги повторяются до тех пор, пока процесс не закончится. Если текущий вес уменьшится до нуля, то решение найдено. В противном случае, нет.

Например, пусть полный вес рюкзака равен 270, а последовательность весов предметов равна {2, 3, 6, 13, 27, 52, 105, 210}. Самый большой вес – 210. Он меньше 270, поэтому предмет весом 210 кладут в рюкзак. Вычитают 210 из 270 и получают 60. Следующий наибольший вес последовательности равен 105. Он больше 60, поэтому предмет весом 105 в рюкзак не кладут. Следующий самый тяжелый предмет имеет вес 52. Он меньше 60, поэтому предмет весом 52 также кладут в рюкзак. Аналогично проходят процедуру укладки в рюкзак предметы весом 6 и 2. В результате полный вес уменьшится до 0. Если бы этот рюкзак был бы использован для дешифрования, то открытый текст, полученный из значения шифртекста 270, был бы равен 10100101.

Открытый ключ представляет собой не сверхвозрастающую (нормальную) последовательность. Он формируется на основе закрытого ключа и, как принято считать, не позволяет легко решить задачу об укладке ранца. Для его получения все значения закрытого ключа умножаются на число **n** по модулю **m**. Значение модуля **m** должно быть больше суммы всех чисел последовательности, например, 420 (2+3+6+13+27+52+105+210=418). Множитель **n** должен быть взаимно простым числом с модулем **m,** например, 31. Результат построения нормальной последовательности (открытого ключа) представлен в следующей таблице.

3. Таблица 2. Пример получения открытого ключа

Закрытый ключ, k_i	2	3	6	13	27	52	105	210
Открытый ключ, $(k_i*n) \bmod m = (k_i*31) \bmod 420$	62	93	186	403	417	352	315	210

Для шифрования сообщение сначала разбивается на блоки, по размерам равные числу элементов последовательности в рюкзаке. Затем, считая, что единица указывает на присутствие элемента последовательности в рюкзаке, а ноль — на его отсутствие, вычисляются полные веса рюкзаков – по одному рюкзаку для каждого блока сообщения.

В качестве примера возьмем открытое сообщение «АБРАМОВ», символы которого представим в бинарном виде в соответствии с таблицей кодов символов Windows 1251. Результат шифрования с помощью открытого ключа {62, 93, 186, 403, 417, 352, 315, 210} представлен в следующей таблице.

Таблица 3 Пример шифрования

Открытое сообщение		Сумма весов	Шифрограмма (рюкзак), c_i
Символ	Bin-код		
А	1100 0000	62+93	155
Б	1100 0001	62+93+210	365
Р	1101 0000	62+93+403	558
А	1100 0000	62+93	155
М	1100 1100	62+93+417+352	924
О	1100 1110	62+93+417+352+315	1239
В	1100 0010	62+93+315	470

Для расшифрования сообщения получатель должен сначала определить обратное число $\mathbf{n^{-1}}$, такое что $\mathbf{(n * n^{-1}) \bmod m = 1}$. В математике **обратное**

число n^{-1} (обратное значение, обратная величина) - число, на которое надо умножить данное число **n**, чтобы получить единицу (**$n * n^{-1} = 1$**). Пара чисел, произведение которых равно единице, называются **взаимно обратными.** Например: 5 и 1/5, -6/7 и -7/6. **Обратными числами по модулю m** называются такие числа **n** и **n^{-1}**, для которых справедливо выражение **$(n * n^{-1}) \bmod m = 1$**. Для вычисления обратных чисел по модулю обычно используется расширенный алгоритм Евклида. После определения обратного числа каждое значение шифрограммы умножается на **n^{-1}** по модулю **m** и с помощью закрытого ключа определяются биты открытого текста.

В нашем примере сверхвозрастающая последовательность равна {2, 3, 6, 13, 27, 52, 105, 210}, m = 420, n = 31.

Значение n^{-1} равно 271 (31*271 mod 420 = 1).

Таблица 4 Пример расшифрования

Шифрограмма (рюкзак), c_i	$(c_i * n^{-1}) \bmod m = (c_i * 271) \bmod 420$	Сумма весов	Открытое сообщение	
			Bin-код	Символ
155	5	2+3	1100 0000	А
365	215	2+3+210	1100 0001	Б
558	18	2+3+13	1101 0000	Р
155	5	2+3	1100 0000	А
924	84	2+3+27+52	1100 1100	М
1239	189	2+3+27+52+105	1100 1110	О
470	110	2+3+105	1100 0010	В

В своей работе авторы рекомендовали брать длину ключа, равную 100 (количество элементов последовательности). В заключении следует отметить, что задача вскрытия данного способа шифрования успешно решена Шамиром и Циппелом в 1982 г.

Задание на практическую работу.

В задании необходимо зашифровать свою фамилию с помощью - алгоритма на основе задачи об укладке ранца;

При оформлении отчета необходимо привести исходное сообщение (фамилию) и таблицы генерации ключей, шифрования и расшифрования. Код символа соответствует его положению в алфавите, в соответствии с кодировкой Windows 1251 (табл.5).

Таблица 5

символ	10-й код	2-й код	символ	10-й код	2-й код	символ	10-й код	2-й код	символ	10-й код	2-й код
Ђ	128	10000000		160	10100000	А	192	11000000	а	224	11100000
Ѓ	129	10000001	Ў	161	10100001	Б	193	11000001	б	225	11100001
‚	130	10000010	ў	162	10100010	В	194	11000010	в	226	11100010
ѓ	131	10000011	Ј	163	10100011	Г	195	11000011	г	227	11100011
„	132	10000100	¤	164	10100100	Д	196	11000100	д	228	11100100
…	133	10000101	Ґ	165	10100101	Е	197	11000101	е	229	11100101
†	134	10000110	¦	166	10100110	Ж	198	11000110	ж	230	11100110
‡	135	10000111	§	167	10100111	З	199	11000111	з	231	11100111
€	136	10001000	Ё	168	10101000	И	200	11001000	и	232	11101000
‰	137	10001001	©	169	10101001	Й	201	11001001	й	233	11101001
Љ	138	10001010	Є	170	10101010	К	202	11001010	к	234	11101010
‹	139	10001011	«	171	10101011	Л	203	11001011	л	235	11101011
Њ	140	10001100	¬	172	10101100	М	204	11001100	м	236	11101100
Ќ	141	10001101	-	173	10101101	Н	205	11001101	н	237	11101101
Ћ	142	10001110	®	174	10101110	О	206	11001110	о	238	11101110
Џ	143	10001111	Ї	175	10101111	П	207	11001111	п	239	11101111
ђ	144	10010000	°	176	10110000	Р	208	11010000	р	240	11110000
‘	145	10010001	±	177	10110001	С	209	11010001	с	241	11110001
’	146	10010010	І	178	10110010	Т	210	11010010	т	242	11110010
“	147	10010011	і	179	10110011	У	211	11010011	у	243	11110011
”	148	10010100	ґ	180	10110100	Ф	212	11010100	ф	244	11110100
•	149	10010101	µ	181	10110101	Х	213	11010101	х	245	11110101
–	150	10010110	¶	182	10110110	Ц	214	11010110	ц	246	11110110
—	151	10010111	·	183	10110111	Ч	215	11010111	ч	247	11110111
□	152	10011000	ё	184	10111000	Ш	216	11011000	ш	248	11111000
™	153	10011001	№	185	10111001	Щ	217	11011001	щ	249	11111001
љ	154	10011010	є	186	10111010	Ъ	218	11011010	ъ	250	11111010
›	155	10011011	»	187	10111011	Ы	219	11011011	ы	251	11111011
њ	156	10011100	ј	188	10111100	Ь	220	11011100	ь	252	11111100
ќ	157	10011101	Ѕ	189	10111101	Э	221	11011101	э	253	11111101
ћ	158	10011110	ѕ	190	10111110	Ю	222	11011110	ю	254	11111110
џ	159	10011111	ї	191	10111111	Я	223	11011111	я	255	11111111

Для численной реализации алгоритмов RSA, EL Gamal, задачи упаковки ранца можно воспользоваться инженерным калькулятором https://web2.0 calc.com.

Приложение 2

Министерство образования и науки Российской Федерации

Федеральное государственное автономное
образовательное учреждение высшего образования
«Санкт-Петербургский политехнический университет Петра Великого»

Институт среднего профессионального образования

КОНТРОЛЬНАЯ РАБОТА ПО ДИСЦИПЛИНЕ
«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Вариант № _____

Выполнил:
студент _____гр.
ФИО _____
Проверил:
Преподаватель: Маковецкая-Абрамова О.В.
Оценка _____
Подпись_____

Санкт-Петербург
2022