**Группа 4110-2-Дом**

****

| **Вариант** | **Текстовый фрагмент** |
| --- | --- |
| **15** | Раньше шифрование выполнялось вручную. Специалист-шифровальщик обрабатывал сообщение посимвольно и таким образом получал зашифрованный текст. Несмотря на то, что результат шифрования многократно проверялся, известны исторические факты ошибок шифровальщиков. После изобретения механических шифровальных машин процесс обработки данных при шифровании был автоматизирован и ускорен благодаря применению аппаратных средств. Кроме того, применение шифровальной техники снизило вероятность ошибок в процессе шифрования и расшифрования. Дальнейшее развитие техники привело к появлению сначала электромеханических, а затем электронных аппаратных криптографических устройств. Если все процедуры шифрования и расшифрования выполняются специальными электронными схемами по определенным логическим правилам, то такой способ реализации криптографического метода называется аппаратным. |
| **16** | Изначально криптография изучала методы шифрования информации – обратимого преобразования открытого (исходного) текста на основе секретного алгоритма или [ключа](https://ru.wikipedia.org/wiki/%D0%9A%D0%BB%D1%8E%D1%87_(%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F)) в шифрованный текст (шифротекст). Аппаратным способом могут быть реализованы многие криптоалгоритмы. Традиционная криптография образует раздел симметричных криптосистем, в которых зашифровывание и расшифровывание проводится с использованием одного и того же секретного ключа. На разработку аппаратного устройства необходимы существенные затраты, однако при массовом выпуске устройства эти затраты окупаются. Аппаратная реализация криптографического метода отличается высокой производительностью, простотой в эксплуатации, защищенностью. Во всем мире выпускаются ежегодно миллионы криптографических аппаратных устройств. |
| **17** | Повсеместное внедрение вычислительной техники, а особенно персональных компьютеров, привело к появлению программных реализаций алгоритмов шифрования. Интересно, что разработчики первых блочных шифров, используемых, например, в старом американском стандарте DES, и не предполагали, что придуманные ими алгоритмы будут реализовываться программно. Благодаря тому, что все методы криптографического преобразования могут быть представлены в виде конечной алгоритмической процедуры, они могут быть запрограммированы. Основным достоинством программных методов реализации защиты является их гибкость, т.е. возможность быстрого изменения алгоритмов шифрования или их настройки. Кроме того, программные реализации криптографических методов отличаются меньшей стоимостью. Основным же недостатком программной реализации является существенно меньшее быстродействие по сравнению с аппаратными средствами. |
| **18** | В средние века криптографические методы использовались, прежде всего, в военном деле, шпионаже, дипломатии. Изучением шифров занимались священники, ученые и дипломаты. На практике применялись различные шифры. Первые труды по криптографии созданы в XIV – XVI веках Чикко Симоннети (сотрудником папской канцелярии), Габлиэлем де Лавиндой (секретарем папы Клементия XII), Леоном Баттистой Альберти (знаменитым итальянским архитектором и философом), аббатом Иоганнесом Тритемием, жившем в Германии. Все указанные деятели внесли большой вклад в развитие криптографии, так как не только рассматривали в своих трудах существующие шифры, но и предлагали различные усовершенствованные методы шифрования, а также некоторые простейшие методы криптоанализа. |
| **19** | Огромное влияние на развитие криптографии оказывают достижения научно-технического прогресса. Так, например, в середине XIX века после изобретения телеграфа появилось несколько дипломатических и коммерческих шифров, ориентированных на применение телеграфа. Возрастание скорости передачи данных требовало увеличения скорости шифрования. В конце XIX века появились механические шифраторы Джефферсона и Уитстона. С конца XIX века криптография стала серьезной отраслью научных знаний и стала изучаться как отдельная наука в военных академиях. В XX веке появились новые возможности по передаче информации на большие расстояния с большой скоростью. В связи с применением радиосвязи расширились возможности доступа к шифрованной информации в процессе ее передачи. |
| **20** | В 20-х годах XX века для автоматизации процесса шифрования появились многочисленные механические устройства. В частности, широко использовались роторные шифровальные машины, в которых для выполнения операций замены символов применялись механические колеса – роторы. Шифровальные машины заменяли открытый текст на зашифрованный, состоящий из символов того же алфавита. После этого зашифрованная информация могла передаваться различными способами, например, по радиоканалу. Во всех развитых странах, в том числе и в СССР, создавались скоростные шифровальные машины, которые широко применялись во время второй мировой войны и позже. В середине ХХ века разработкой шифровальных алгоритмов стали заниматься профессиональные математики и специалисты в области информатики. |
| **21** | С развитием информационных технологий криптография не только приобрела новые сферы применения, но и претерпела значительные изменения. В древние времена в процессе обмена зашифрованными сообщениями участвовало только две стороны, поэтому ключом шифрования необходимо было обеспечить только эти две стороны. В современных информационных системах в процессе передачи информации задействовано множество абонентов, и все они заинтересованы в надежных и удобных каналах получения ключей шифрования. Проблема распределения ключей была решена в двадцатом веке благодаря изобретению нового принципа шифрования – асимметричного шифрования или шифрования с открытым ключом. В асимметричных алгоритмах шифрования используются специальные математические функции – односторонние функции. Открытие асимметричных криптосистем позволило еще больше расширить сферы применения криптографии. |
| **22** | Информация в процессе хранения, передачи и преобразования сообщений подвергается воздействию различных атак. Атаки осуществляются противниками (оппонентами, перехватчиками, врагами). Основными нарушениями безопасности являются раскрытие информационных ценностей (потеря конфиденциальности), модификация без разрешения автора (потеря целостности) или неавторизованная потеря доступа к этим ценностям (потеря доступности).  Атаки могут быть пассивными и активными. Пассивной называется атака, при которой противник не имеет возможности изменять передаваемые сообщения. При пассивной атаке возможно лишь прослушивание передаваемых сообщений, их дешифрование и анализ трафика. При активной атаке противник имеет возможность модифицировать передаваемые сообщения и даже добавлять свои сообщения. |
| **23** | Атака на основе известного открытого текста имеет место в том случае, если криптоаналитик получает в свое распоряжение какие-либо открытые тексты, соответствующие раннее переданным зашифрованным сообщениям. Сопоставляя пары "текст-шифротекст", противник пытается узнать секретный ключ, чтобы с его помощью дешифровать все последующие сообщения. Некоторым покажется, что противнику достаточно сложно заполучить в свое распоряжение некоторое количество пар "текст-шифротекст". На самом деле практически всегда возможно достать такие кусочки открытого текста и шифротекста. Криптоаналитик может иметь информацию о формате перехваченного зашифрованного файла: например, знать, что это файл с изображением JPEG, документ Word или Excel, файл базы данных. Все эти и многие другие форматы содержат определенные стандартные заголовки или фрагменты. Таким образом, специалист по криптоанализу сможет сформировать необходимые данные для проведения атаки на основе известного открытого текста. |
| **24** | В современной криптографии большое внимание уделяется не только созданию и исследованию шифров, но и разработке криптографических протоколов. Криптографический протокол – это процедура взаимодействия абонентов с использованием криптографических средств, в результате которой абоненты достигают своей цели, а их противники – не достигают. В основе протокола лежит набор правил, регламентирующих использование криптографических преобразований и алгоритмов в информационных процессах. Каждый криптографический протокол предназначен для решения определенной задачи. Любой протокол имеет следующие свойства: при выполнении протокола важен порядок действий; каждое действие должно выполняться в свою очередь и только по окончании предыдущего; протокол должен быть непротиворечивым; протокол должен быть полным, то есть для каждой возможной ситуации должно быть предусмотрено соответствующее действие. |
| **25** | Протоколы аутентификации и идентификации предназначены для предотвращения доступа к некоторой информации лиц, не являющихся ее пользователями, а также предотвращения доступа пользователей к тем ресурсам, на которые у них нет полномочий. Типичная сфера применения – организация доступа пользователей к ресурсам некоторой большой информационной системы. Протоколы распределения ключей необходимы для обеспечения секретными ключами участников обмена зашифрованными сообщениями. Протоколы электронной цифровой подписи позволяют ставить под электронными документами подпись, аналогичную обыкновенной подписи на бумажных документах. В результате выполнения протокола электронной цифровой подписи к передаваемой информации добавляется уникальное числовое дополнение, позволяющее проверить ее авторство. |
| **26** | В интернете криптографические протоколы используются практически при каждом запросе. Не стоит думать, что в те далекие времена не было криптографии. Первые способы шифрования появились около четырех тысяч лет назад. Конечно, это были самые примитивные и нестойкие шифры, однако и такие способы могли защитить информацию от любопытных глаз. Люди всегда нуждались в секретной переписке, поэтому шифрование не стояло на месте. С раскрытием одних шифров придумывали другие, более стойкие. На смену бумажным шифрам пришли шифровальные машины. Даже опытному математику не удавалось взломать шифр, рассчитанный на роторной машине. С появлением первых компьютеров требования к защите информации и, соответственно, интерес к криптографии, возросли многократно. |
| **27** | Рассмотрим простейший протокол для обмена конфиденциальными сообщениями между двумя сторонами, которые будем называть абонент1 и абонент2. Пусть абонент1 желает передать зашифрованное сообщение абоненту2. В этом случае их последовательность действий должна быть следующей. Абоненты выбирают систему шифрования (например, шифр Цезаря со сдвигом на n позиций). Абоненты договариваются о ключе шифрования. Абонент1 шифрует исходное сообщение с помощью ключа выбранным методом и получает зашифрованное сообщение. Зашифрованное сообщение пересылается абоненту2. Абонент2 расшифровывает зашифрованное сообщение с помощью ключа и получает открытое сообщение. |
| **28** | По сути, это сеть сетей, в которой люди могут общаться с устройствами, а устройства могут общаться между собой, реагировать на изменение окружения и принимать решения без участия человека. Устройства Интернета вещей функционируют самостоятельно, хотя люди могут настраивать их или предоставлять доступ к данным. Такие системы работают в режиме реального времени и обычно состоят из сети умных устройств и облачной платформы, к которой они подключены с помощью различных видов связи. Сначала устройства собирают данные – например, о температуре в квартире, затем эти данные отправляются в облако. Там программное обеспечение обрабатывает их. Что происходит, когда температура оказывается слишком высокой или в доме находится грабитель? Система оповещает об этом пользователя или сама выполняет действия – например, звонит в полицию. |
| **29** | Интернет вещей у многих ассоциируется с «умным» домом. Благодаря технологиям и устройствам, пользователи могут совершать онлайн-покупки, регулировать температуру в комнате, включать свет и музыку, отдавая голосовые команды виртуальным помощникам. Вам больше не надо опасаться, что вы забыли выключить утюг или кран – достаточно нажать кнопку в смартфоне, и «умный» дом все исправит. Система наблюдения с помощью компьютерного зрения распознает всех, кто проходит мимо вашей квартиры, и сравнит изображения с базой полиции. Сегодня «умный» дом в России – это в основном интеллектуальный помощник Яндекса «Алиса», которая включает музыку, ищет информацию в интернете, советует фильмы, регулирует освещение и температуру в доме, включает чайник. |
| **30** | Криптографические протоколы – сравнительно молодая отрасль криптографической науки. Первые протоколы появились во второй половине ХХ века. С тех пор эта область криптографии бурно развивалась, и на настоящий момент имеется уже несколько десятков различных типов криптографических протоколов. Все эти типы можно условно разделить на две группы: прикладные протоколы и примитивные. Прикладной протокол решает конкретную задачу, которая возникает (или может возникнуть) на практике. Примитивные же протоколы используются как своеобразные "строительные блоки" при разработке прикладных протоколов. Мы в данном учебном пособии будем рассматривать только примитивные криптографические протоколы, которые при некоторой адаптации к реальным системам связи могут использоваться на практике. |
| **31** | «Умные» IoT позволяют компаниям автоматизировать процессы и снижать трудозатраты. Это сокращает объем отходов, улучшает качество предоставляемых услуг, сокращает затраты на производство и логистику. IoT затрагивает все отрасли. Внедрение интернета вещей в электроэнергетике улучшает контролируемость подстанций и линий электропередачи за счет дистанционного мониторинга, а в здравоохранении позволяет перейти на новый уровень диагностики заболеваний – «умные» устройства контролируют показатели здоровья пациента. В сельском хозяйстве «умные» фермы и теплицы сами дозируют удобрения и воду. Внедрение IoT в логистике сокращает затраты на грузоперевозки и минимизирует влияние человеческого фактора. IoT активно внедряют нефтегазовые и горнодобывающие отрасли. |
| **32** | Основная проблема, с которой связано бурное развитие Интернета вещей, – безопасность. Киберпреступники постоянно пытаются взламывать устройства удаленного наблюдения за пациентами, базы данных с информацией о здоровье людей, интеллектуальные системы управления автомобилем, совершают фишинговые атаки, подгружают вирусы на взломанные устройства и даже совершают целые диверсии на производствах. Поэтому участникам рынка Интернета вещей надо учиться защищать свои системы. Подключение все большего количества устройств к Интернету неизбежно приведет к потере рабочих мест. Например, системы Интернета вещей заменят специалистов по техобслуживанию, ремонту и установке оборудования. Однако правовые аспекты Интернета вещей достаточно расплывчаты. |
| **33** | Многие ошибочно полагают, что блокчейн и распределенный реестр это и одно и то же. На самом деле, [блокчейн](https://prostocoin.com/blog/blockchain-guide" \t "_blank) – один из типов распределенного реестра. Информация в нем записывается строго в блоки, которые соединены между собой последовательно. Каждый блокчейн – распределенный реестр, но не все реестры данных являются блокчейнами. Оба этих понятия объединяет децентрализованное хранение данных и необходимость достижения консенсуса между узлами связи для внесения изменений, а сама информация может записываться в любом виде. На практике, распределенные реестры не требуют создания блоков и не нуждаются в доказательстве работы. Благодаря этому у них теоретически меньшие проблемы с масштабируемостью. |
| **34** | Блокчейн и хешграф преследуют одну и ту же цель с помощью лежащей в их основе технологии распределенного реестра, а именно: получение одноранговой прозрачной валютной системы, которая не требует центрального регулирующего органа. Однако есть некоторые различия в том, каким образом хешграфы выполняют эту задачу в обход ограничений, которые имеет технология блокчейна. Хешграфы полагаются исключительно на механизм консенсуса для проверки транзакций в своей сети. Консенсус достигается с помощью виртуальных методов голосования и сплетен, которые обеспечивают более высокую масштабируемость и более мягкие требования к хранению. В отличие от блокчейна, в реестре хешграфа в пределах одной временной метки в параллельном стеке могут храниться несколько транзакций. |
| **35** | Протоколы конфиденциальной передачи сообщений. Задача конфиденциальной передачи сообщений состоит в следующем. Имеются два участника протокола, которые являются абонентами сети связи. Участники соединены некоторой линией связи, по которой можно пересылать сообщения в обе стороны. Линию связи может контролировать противник. У одного из абонентов имеется конфиденциальное сообщение m, и задача состоит в том, чтобы это сообщение конфиденциальным же образом передать второму абоненту. Протоколы этого типа, наверно, появились раньше других криптографических протоколов, так как задача конфиденциальной передачи сообщений – исторически первая задача, которая решалась криптографией. |