КРИПТОГРАФИЯ

ПОДГОТОВИЛА: ХОМИНА АНАСТАСИЯ 10 “А”

Что такое криптография?

Это наука о методах обеспечения конфиденциальности (невозможности прочтения информации посторонним), целостности данных (невозможности незаметного изменения информации), аутентификации (проверки подлинности авторства или иных свойств объекта), а также невозможности отказа от авторства. Считается, что основы криптографии заложил Эней Тактик. Попытки зашифровать данные делали ещё в древней Индии и Месопотамии, но они были не очень удачными. Первая надёжная система защиты была разработана в Древнем Китае. Методы криптографии нашли своё применение и в Средние века, но их уже взяли на вооружение купцы и дипломаты. Золотым веком данной науки называют эпоху Возрождения. Тогда же был предложен двоичный способ шифрования, аналогичный которому используется в компьютерной технике в наши дни. Во время Первой мировой войны она была признана полноценным боевым инструментом. Стоило только разгадать сообщения противника – и можно было получить ошеломляющий результат. В качестве примера можно привести перехват телеграммы, посланной немецким послом Артуром Циммерманом американскими спецслужбами. Конечным результатом этого стало то, что США вступило в боевые действия на стороне Антанты. Вторая мировая война стала своеобразным кристаллизатором процесса развития компьютерных сетей. И немалый вклад в это внесла криптография. Некоторые правительства так испугались открывающихся возможностей, что наложили мораторий на применение **шифрования данных.**

Шифрование данных

Шифрование данных – это метод сокрытия исходного смысла документа или сообщения, которое обеспечивает искажение его первоначального вида. Простыми словами, это способ защиты информации. Такой метод еще называют кодированием, так как с помощью специальных программ или вручную ваш текст переводят в непонятный для постороннего человека код. Сама процедура зависит от последовательности изменения вида данных. Такую последовательность принято называть алгоритмом. Шифрование данных относят к криптографии. Эта наука тщательно изучается мировыми разведывательными организациями, и с каждым днем разгадываются и создаются новые криптографические алгоритмы. Методы шифрования были известны еще в древности, когда римские военачальники передавали с гонцами важные письма в зашифрованном виде. Алгоритмы тогда были примитивными, но успешно запутывали врагов. Шифрование данных помогает не только защитить информацию, оно выступает еще и как «сжиматель». Многие **архиваторы** экономят место на диске именно с помощью шифрования. Например, известный всем WinRAR использует алгоритм шифрования AES с длиной ключа – 128. Многие пользователи хранят данные на своем компьютере только в архивированном виде, и при этом каждый архив защищают паролем. С развитием интернета хорошо подготовленному хакеру не стоит труда взломать незащищенный компьютер и заполучить нужную ему информацию. Поэтому специалисты рекомендуют шифровать все важные для вас данные.

Архиватор

Программа, предназначенная для упаковки без потерь одного и более файлов в единый файл-архив или в серию архивов для удобства переноса и/или хранения данных. Распаковка архивов выполняется с помощью того же архиватора либо посредством сторонних совместимых утилит. Большинство архиваторов имеет функцию проверки целостности хранящихся в архиве данных. Для этого в архив при добавлении туда файлов вносится информация об их **контрольных суммах.** При распаковке (или тестировании) архива обязательно вычисляется контрольная сумма каждого извлекаемого файла, и, если она не совпадает с суммой, хранящейся в архиве, то выводится сообщение об ошибке. Таким образом, архиваторы предоставляют очень важную возможность, о которой многие даже не задумываются: гарантию целостности данных. Кроме того, некоторые архиваторы (например RAR) имеют функции защиты архивов от физических повреждений или даже полной утери отдельных томов многотомных архивов, благодаря чему архив можно рассматривать не только как средство для хранения данных, но и для их восстановления в исходном виде в случае повреждений. Некоторые архиваторы позволяют создавать так называемые многотомные архивы, то есть архивы, состоящие из нескольких частей указанного или разного размера. Такие архивы удобно применять для переноса больших объёмов данных на носителях меньшего размера и обмена данными через Интернет, когда вместо одного огромного архива практичнее передать несколько файлов меньшего размера.

Контрольная сумма файла

Некоторое значение, рассчитанное по набору данных путём применения определённого алгоритма и используемое для проверки целостности данных при их передаче или хранении. Несмотря на своё название, контрольная сумма не обязательно вычисляется путём суммирования. С точки зрения математики контрольная сумма является результатом **хеш-функции**, используемой для вычисления контрольного кода — небольшого количества бит внутри большого блока данных. Значение контрольной суммы добавляется в конец блока данных непосредственно перед началом передачи или записи данных на какой-либо носитель информации. Впоследствии оно проверяется для подтверждения целостности данных. Популярность использования контрольных сумм для проверки целостности данных обусловлена тем, что подобная проверка просто реализуема в двоичном цифровом оборудовании, легко анализируется и хорошо подходит для обнаружения общих ошибок, вызванных наличием шума в каналах передачи данных. Криптографическая функция MD5 уже почти не используется для определения контрольных сумм, так как оказалось, что для неё можно быстро создавать с помощью современных компьютеров два разных файла, имеющих разную длину в байтах, но одинаковые величины контрольных сумм, подсчитанных с помощью алгоритма MD5. Использование термина сумма связано с тем, что на заре цифровой связи при байтовых передачах информационными были 7 бит, а восьмой — контрольный — рассчитывался как младший разряд сложения информационных.

Хэш-функция

Хеширование — преобразование массива входных данных произвольной длины в (выходную) битовую строку установленной длины, выполняемое определённым алгоритмом. Функция, воплощающая алгоритм и выполняющая преобразование, называется «хеш-функцией» или «функцией свёртки». Исходные данные называются входным массивом, «ключом» или «сообщением». Результат преобразования (выходные данные) называется «хешем», «хеш-кодом», «хеш-суммой», «сводкой сообщения».

Расшифровать хэш очень и очень сложно, можно сказать, что практически невозможно. Хэш-функция часто используется для хранения очень важной информации, такой как пароль, логин, номер удостоверения и другая персональная информация. Вместо сравнивания сведений, вводимых пользователем, с теми, которые хранятся в базе данных, происходит сопоставление их хешей. Это дает гарантию, что при случайной утечке информации никто не сможет воспользоваться важными данными для своих целей. Путем сравнения хеш-кода также удобно проверять правильность загрузки файлов с интернета, особенно если во время скачивания происходили перебои связи.

В зависимости от своего предназначения хэш-функция может быть одного из трех типов:

1. Функция для проверки целостности информации.
2. Функция, предназначенная для создания эффективной структуры данных.
3. Криптографическая функция.

Конец