3. file:///C:/Users/%D0%90%D0%B4%D0%BC%D0%B8%D0%BD/Downloads/77d0ec79f414efb0f1e8f2456c192d2e.pdf

4. https://cyberleninka.ru/article/n/vliyanie-tsifrovizatsii-ekonomiki-na-metodologii-upravleniya-proektami

ОСНОВЫ КРИПТОГРАФИИ И ТЕОРИИ КОДИРОВАНИЯ

В.Р Корона
Научный руководитель Л.А Сараев

Криптография - это наука об использовании математики для шифровки и дешифровки данных. Криптография позволяет хранить важную информацию или передавать её по ненадёжным каналам связи (таким как Интернет) так, что она не может быть прочитана никем, кроме легитимного получателя.

Проблема защиты информации путем преобразований, исключающих ее прочтение посторонним лицом, волновало человечество с давних времен. Криптография исторически зародилась из потребности передачи секретной информации. История криптографии – ровесница истории письменности. Более того, первоначально письменность сама по себе была криптографической системой, т.к. в древнем обществе ей владели только избранные (например, жрецы). С широким распространением письменности криптография стала формироваться как самостоятельная наука, которая длительное время была связана только с разработкой специальных методов преобразования информации с целью ее представления в форме, недоступной для злоумышленника. С позиций сегодняшнего дня ее методы рассматриваются всего лишь как некоторые ухищрение, чем как строгая научная дисциплина. Современная криптография базируется на самых последних достижениях фундаментальных наук, и в первую очередь,

математики. Сегодня в теоретической криптографии используются понятия и результаты таких разделов математики, как алгебра, теория чисел, теория сложности алгоритмов и вычислений и теория кодирования. Информация, которая может быть прочитана, осмыслена и понята без каких-либо специальных мер, называется открытым текстом. Метод искажения открытого текста таким образом, чтобы скрыть его суть, называется зашифрованием. В большинстве случаев русский термин шифрование является синонимом зашифрования, но иногда обозначает криптографический процесс в целом. Зашифрование открытого текста приводит к его превращению в непонятную абракадабру, именуемую шифртекстом. Шифрование позволяет скрыть информацию от тех, для кого она не предназначается, несмотря на то, что они могут видеть сам шифртекст. Противоположный процесс по обращению шифртекста в его исходный вид называется расшифрованием.

Основные алгоритмы шифрования

Метод шифровки/дешифровки называют шифром. Некоторые алгоритмы шифрования основаны на том, что сам метод шифрования (алгоритм) является секретным. Ныне такие методы представляют лишь исторический интерес и не имеют практического значения. Все современные алгоритмы используют ключ для управления шифровкой и дешифровкой; сообщение может быть успешно дешифровано только если известен ключ. Ключ, используемый для дешифровки может не совпадать с ключом, используемым для шифрования, однако в большинстве алгоритмов ключи совпадают. Алгоритмы с использованием ключа делятся на два класса: симметричные (или алгоритмы секретным ключом) и ассиметричные (или алгоритмы с открытым ключом). Разница в том, что симметричные алгоритмы используют один и тот же ключ для шифрования и для дешифрования (или же ключ для дешифровки просто вычисляется по ключу шифровки). В то время как асимметричные алгоритмы используют разные ключи, и ключ для дешифровки не может быть вычислен по ключу

шифровки. Симметричные алгоритмы подразделяют на потоковые шифры и блочные шифры. Потоковые позволяют шифровать информацию по битам, в то время как блочные работают с некоторым набором бит данных (обычно размер блока составляет 64 бита) и шифруют этот набор как единое целое. Ассиметричные шифры (также именуемые алгоритмами с открытым ключом, или - в более общем плане - криптографией с открытым ключом) допускают, чтобы открытый ключ был доступен всем (скажем, опубликован в газете). Это позволяет любому зашифровать сообщение. Однако расшифровать это сообщение сможет только нужный человек (тот, кто владеет ключом дешифровки). Ключ для шифрования называют открытым ключом, а ключ для дешифрования - закрытым ключом или секретным ключом. Современные алгоритмы шифровки/дешифровки достаточно сложны и их невозможно проводить вручную. Настоящие криптографические алгоритмы разработаны для использования компьютерами или специальными аппаратными устройствами. В большинстве приложений криптография производится программным обеспечением и имеется множество доступных криптографических пакетов. Вообще говоря, симметричные алгоритмы работают быстрее, чем ассиметричные. На практике оба типа алгоритмов часто используются вместе: алгоритм с открытым ключом используется для того, чтобы передать случайным образом сгенерированный секретный ключ, который затем используется для дешифровки сообщения. Многие качественные криптографические алгоритмы доступны широко - в книжном магазине, библиотеке, патентном бюро или в Интернет. К широко известным симметричным алгоритмам относятся DES и IDEA, наверное, самым лучшим асимметричным алгоритмом является RSA.

Обеспечиваемая шифром степень защиты

Теоретически, любой шифровальный алгоритм с использованием ключа может быть вскрыт методом перебора всех значений ключа. Если ключ подбирается методом грубой силы (bruteforce), требуемая мощность компьютера растет экспоненциально с увеличением длины ключа. Ключ

длиной в 32 бита требует 2^{32} (около 10^9) шагов. Такая задача под силу любому дилетанту и решается на домашнем компьютере. Системы с 40-битным ключом (например, экспортный американский вариант алгоритма RC4) требуют 2^{40} шагов - такие компьютерные мощности имеются в большинстве университетов и даже в небольших компаниях. Системы с 56-битными ключами (DES) требуют для вскрытия заметных усилий, однако могут быть легко вскрыты с помощью специальной аппаратуры. Стоимость такой аппаратуры значительна, но доступна для мафии, крупных компаний и правительств. Ключи длиной 64 бита в настоящий момент, возможно, могут быть вскрыты крупными государствами и уже в ближайшие несколько лет будут доступны для вскрытия преступными организациями, крупными компаниями и небольшими государствами. Ключи длиной 80 бит могут в будущем стать уязвимыми. Ключи длиной 128 бит вероятно останутся недоступными для вскрытия методом грубой силы в обозримом будущем. Можно использовать и более длинные ключи. В пределе нетрудно добиться того, чтобы энергия, требуемая для вскрытия (считая, что на один шаг затрачивается минимальный квантовомеханический квант энергии) превзойдет массу солнца или вселенной. Однако, длина ключа это еще не все. Многие шифры можно вскрыть и не перебирая всех возможных комбинаций. Вообще говоря, очень трудно придумать шифр, который нельзя было бы вскрыть другим более эффективным способом. Разработка собственных шифров может стать приятным занятием, но для реальных приложений использовать самодельные шифры не рекомендуется если вы не являетесь экспертом и не уверены на 100 процентов в том, что делаете. Вообще говоря, следует держаться в стороне от неопубликованных или секретных алгоритмов. Часто разработчик такого алгоритма не уверен в его надежности, или же надежность зависит от секретности самого алгоритма. Вообще говоря, ни один алгоритм, секретность которого зависит от секретности самого алгоритма не является надежным. В частности, имея шифрующую программу, можно нанять программиста, который

дизассемблирует ее и восстановит алгоритм методом обратной инженерии. Опыт показывает, что большинство секретных алгоритмов, ставших впоследствии достоянием общественности, оказались до смешного ненадежными. Длины ключей, используемых в криптографии с открытым ключом обычно значительно больше, чем в симметричных алгоритмах. Здесь проблема заключается не в подборе ключа, а в воссоздании секретного ключа по открытому. В случае RSA проблема эквивалентна разложению на множители большого целого числа, которое является произведением пары неизвестных простых чисел. В случае некоторых других криптосистем, проблема эквивалентна вычислению дискретного логарифма по модулю большого целого числа (такая задача считается примерно аналогичной по трудности задаче разложения на множители). Имеются криптосистемы, которые используют другие проблемы. Чтобы дать представление о степени сложности вскрытия RSA, скажем, что модули длиной 256 бит легко факторизуются обычными программистами. Ключи в 384 бита могут быть вскрыты исследовательской группой университета или компании. 512-битные ключи находятся в пределах досягаемости крупных государств. Ключи длиной в 768 бит вероятно не будут надежны продолжительное время. Ключи длиной в 1024 бит могут считаться безопасными до тех пор, пока не будет существенного прогресса в алгоритме факторизации; ключи длиной в 2048 большинство считает надежными на десятилетия. Более подробную информацию о длинах ключей RSA можно почерпнуть из статьи Брюса Шнайера. Важно подчеркнуть, что степень надежности криптографической системы определяется ее слабейшим звеном. Нельзя упускать из вида ни одного аспекта разработки системы --- от выбора алгоритма до политики использования и распространения ключей.

Список использованных источников:

1. http://textarchive.ru/c-2961860-pall.html
2. https://litresp.ru/chitat/ru/%D0%A6/cimmermann-filipp/vvedenie-v-kriptografiyu/2
3. http://algolist.ru/defence/intro.php