И.Р. Брынцева, РГППУ,
гр. КТ-518
Руководитель: ст. преподаватель каф. СИС
С.В. Ченушкина

СОВРЕМЕННАЯ КРИПТОГРАФИЯ

Одной из важнейших способностей человека является умение общаться с другими людьми - передавать им сведения о том, что происходит в окружающем их мире, и о фактах своей субъективной реальности. Коммуникация в человеческом обществе избирательна. Мы разговариваем с разными людьми и то, что сообщаем одним, стараемся скрыть от других.

С возникновением письменности появилась проблема обеспечения секретности и подлинности передаваемых сообщений. Поэтому именно после возникновения письменности появилось искусство тайнописи ("тайно писать") - набор методов, предназначенных для секретной передачи записанных сообщений от одного человека другому. С развитием информационных технологий и широким распространением сети Internet задача сохранения конфиденциальности информации стала особенно актуальной. Эту задачу успешно решает криптография – наука о защите данных.

Криптография покрывает все практические аспекты секретного обмена сообщениями, включая аутенфикацию, цифровые подписи и многое другое.

Криптография неразрывно связана с криптоанализом. Криптоанализ – это наука о том, как вскрыть шифрованное сообщение, то есть как извлечь открытый текст не зная ключа. Криптографией занимаются криптографы, а криптоанализом занимаются криптоаналитики. Криптографию и криптоанализ объединяет еще одна наука – криптологоия.

В криптографической терминологии исходное послание именуют открытым текстом. Изменение исходного текста так, чтобы скрыть от прочих его содержание, называют шифрованием. Зашифрованное сообщение называют шифротекстом. Процесс, при котором из шифротекста извлекается открытый текст называют дешифровкой. Обычно в процессе шифровки и дешифровки используется некий ключ и

алгоритм обеспечивает, что дешифрование можно сделать лишь зная этот ключ.

Классические криптографические методы разделяют на два основных типа: симметричные и асимметричные.В симметричных методах для шифрования и дешифрования используется один и тот же секретный ключ.

Наиболее известным стандартом на симметричное шифрование с закрытым ключом является стандарт для обработки информации в государственных учреждениях США DES (Data Encryption Standard). Алгоритм DES использует ключ длиной 56 бит, что требует от злоумышленника перебора 72 квадриллионов возможных ключевых комбинаций. Более криптостойкая (но втрое менее быстродействующая) версия алгоритма DES — Triple DES позволяет задать ключ длиной 112 бит.

Другим популярным алгоритмом шифрования является IDEA (International Data Encryption Algorithm), отличающийся применением ключа длиной 128 бит. Он считается более стойким, чем DES.

Отечественный подобный стандарт шифрования данных — ГОСТ 28147-89 “Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования” определяет алгоритм симметричного шифрования с ключом длиной до 256 бит.

К достоинствам симметричных методов относят высокое быстродействие и простоту.

Основным недостатком указанных методов является то, что ключ должен быть известен и отправителю, и получателю. Это существенно усложняет процедуру назначения и распределения ключей между пользователями. По существу, в открытых сетях должен быть предусмотрен физически защищенный канал передачи ключей.

В ассиметричных методах шифрования используются разные ключи для шифрования и расшифровывания (открытый и закрытый ключи).

Такие методы широко применяются в различных сетевых протоколах, в частности, в протоколах TLS и его предшественнике SSL (лежащих в основе HTTPS), а так же SSH, PGP, S/MIME и т. д. Российский стандарт, использующий асимметричное шифрование - ГОСТ Р 34.10-2001.

На данный момент асимметричное шифрование на основе открытого ключа RSA (расшифровывается, как Rivest, Shamir and Aldeman - создатели алгоритма) использует большинство продуктов на рынке информационной безопасности.

Его криптостойкость основывается на сложности разложения на множители больших чисел, а именно - на исключительной трудности задачи определить секретный ключ на основании открытого, так как для этого потребуется решить задачу о существовании делителей целого числа. Наиболее криптостойкие системы используют 1024-битовые и большие числа.

При передачи документов по электронной почте для обеспечения их подлинности используется механизм электронной цифровой подписи (ЭЦП).

По сути ЭЦП — это некая последовательность символов, которая получена в результате определенного преобразования исходного документа (или любой другой информации) при помощи специального программного обеспечения. ЭЦП добавляется при пересылке к исходному документу. Любое изменение исходного документа делает ЭЦП недействительной. На практике ЭЦП уникальна для каждого документа и не может быть перенесена на другой документ; невозможность подделки электронной цифровой подписи обеспечивается очень большим объёмом математических вычислений, необходимым для её подбора. Таким образом, при получении документа, подписанного ЭЦП, получатель может быть уверен в авторстве и неизменности текста данного документа.

ЭЦП является на сегодняшний день законодательно оформленной процедурой обмена защищенными данными через интернет. В статье закона, регулирующей документирование информации (Закон 149-ФЗ), говорится, что электронное сообщение, подписанное электронной цифровой подписью (ЭЦП), признается равнозначным документу, подписанному собственноручно, если иным нормативным актом не предусмотрена обязательность бумажного носителя.