Александр КАМИНСКИЙ,
Республика Молдова

КРИПТОГРАФИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

This work about cryptographic measures and of Information Security

Введение:

Успешное ведение торговли, государственных дел, военных действий и частных действий граждан в большой мере зависит от того, насколько взаимодействующие стороны доверяют таким функциям, как засекречивание, установление личности, доказательство права собственности, полномочий, подлинности подписи, подтверждение даты действия, удостоверение источника и/или получателя информации, подтверждение приоритета, неотрицаемости авторства, времени создания и т.д. В результате появился тщательно разработанный, проверенный и частично узаконенный набор протоколов (как на физическом, так и на информационном уровне), которые определяют, как формировать электронные записи (документы, записи в БД и т.д.). Одним из таких наборов и являются Криптографические средства защиты информации.

Основные понятия и характеристики:

Криптография (от греч. κρυπτός – скрытый и γράφω – пишу) – наука о математических методах обеспечения **конфиденциальности** (невозможности прочтения информации посторонним) и **аутентичности** (целостности и подлинности авторства, а также невозможности отказа от авторства) информации.

Криптографическими средствами защиты называются специальные методы и средства преобразования информации, в результате которых маскируется ее содержание. Основными видами криптографического закрытия являются **шифрование** и **кодирование** защищаемых данных.

Шифрование – способ преобразования информации, применяемый для хранения важной информации в ненадёжных источниках или передачи её по незащищённым каналам связи. Согласно *ГОСТ 28147-89*, шифрование – процесс зашифрования или расшифрования. При этом шифрование есть такой вид закрытия, при котором самостоятельному преобразованию подвергается каждый символ закрываемых данных

Кодирование – процесс преобразования сообщения в комбинацию символов в соответствии с кодом, процесс восстановления сообщения из комбинации символов называется **декодированием.** При кодировании защищаемые данные делятся на блоки, имеющие смысловое значение, и каждый такой блок заменяется цифровым, буквенным или комбинированным кодом.

Основной характеристикой меры защищенности информации криптографическим закрытием является **стойкость шифра или криптографическая стойкость** – это способность криптографического алгоритма противостоять криптоанализу.

Производительность шифрования является важной характеристикой системы шифрования и зависит как от используемой системы шифра, так и от способа реализации шифрования аппаратного или программного.

Ключ – сменный элемент шифра, позволяющий сделать сам алгоритм шифрования открытым и использовать его многократно, меняя лишь ключ. Кроме ключа, в алгоритм шифрования могут входить другие **сменные криптографические параметры** – узлы замены (как правило, более долговременные, чем ключ), синхропосылки (наоборот – случайные). Согласно *ГОСТ 28147-89*, ключ – это "конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования, обеспечивающее выбор одного преобразования из совокупности всевозможных для данного алгоритма преобразований".

Электронная цифровая подпись (**ЭЦП**) – 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.

Схема электронной подписи обычно включает в себя:

- алгоритм генерации ключевых пар пользователя;
- функцию вычисления подписи;
- функцию проверки подписи.

Методы криптографической защиты информации:

Применение методов криптографической защиты характерно для решения подавляющего большинства проблем безопасности. Аутентификация, шифрование данных, контроль целостности, электронная цифровая подпись – понятия, хорошо знакомые сегодня достаточно широкому кругу разработчиков и пользователей.

Построение хорошей и надежной системы криптографии (шифрования) данных является сложным и дорогостоящим делом, затраты труда на которую сравнимы с созданием большой системы. Поэтому лучше пользоваться средствами, разработанными специализированными службами по алгоритмам, проверенными теорией и практикой. Различают следующие основные механизмы безопасности или алгоритмы криптографии:

Алгоритмы симметричного шифрования – алгоритмы шифрования, в которых для шифрования и дешифрования используется один и тот же ключ, или ключ дешифрования легко может быть получен из ключа шифрования. Симметричный алгоритм использует секретный ключ общей длиной в 64 бита и обеспечивает наличие почти 10^{17} переборов вариантов кодирования. Симметричная система защиты предполагает закрытое применение информации и предназначена, прежде всего, для государственной информации с ограниченным режимом пользования. К алгоритмам симметричного шифрования относятся: *DES, AES, ГОСТ 28147-89, Camellia, Twofish, Blowfish, IDEA, RC4* и др.

Алгоритмы асимметричного шифрования – алгоритмы шифрования, в которых для шифрования и дешифрования используются два разных ключа, называемые открытым и закрытым ключами, причем, зная один из ключей, вычислить другой невозможно. Длина ключа не фиксирована, чем он длиннее, тем выше уровень шифрования. При этом, однако, увеличиваются процедуры шифрования и дешифрования. Асимметричный способ криптографии предполагает открытый способ взаимодействия, позволяющий создавать собственные системы шифрования. Такие системы применяются при коммуникации коммерческих данных. К алгоритмам асимметричного шифрования относятся: *RSA и Elgamal (Эль-Гамаль)*.

Хэш-функции – функции, входным значением которых является сообщение произвольной длины, а выходным значением – сообщение фиксированной длины таким образом, чтобы изменение входных данных приводило к непредсказуемому изменению выходных данных. Хэш-функции обладают рядом свойств, которые позволяют с высокой долей вероятности определять изменение входного сообщения. Простым примером хеширования может служить нахождение контрольной суммы сообщения: сумма кодов всех входящих в него символов, от которой берётся несколько последних цифр. Полученное число является примером хеш-кода исходного сообщения. Существует множество способов хеширования, подходящих к различным задачам. Алгоритмы Хэш-функции: *MD4, MD5, SHA-1, ГОСТ Р34.11-94*

Создать и реализовать систему шифрования данных, в принципе, технически несложно. Однако при ее использовании могут возникнуть следующие **проблемы**, связанные с:

- уменьшением производительности системы, увеличением времени шифрования и дешифрования данных;
- достижением требуемого уровня секретности;
- надежностью функционирования системы: нечеткость или несовершенство алгоритма могут привести к потере данных, невозможности их восстановления (следует иметь эталонный экземпляр информационных массивов).

Стандарты криптографических средств защиты.

Применение систем и средств криптографии требует их унификации и стандартизации. Данная проблема актуальна как на национальном уровне взаимодействия, так и международном. Концепция криптографии изложена в таких документах, как:

Стандарт *ISO/IEC 7498* «Базовая эталонная модель взаимодействия открытых систем. Часть 2.Архитектура безопасности», принятый в 1989 г. Международной организацией по стандартизации *IOS (International Organization for Standart)*;

Стандарт «Рекомендации X.800: Архитектура безопасности, принятый IOS для применения в *МККТТ* (*Международным консультативным комитетом по телеграфии и телефонии*)», принятом в 1991 г.

Одними из наиболее известных стандартов шифрования данных являются системы *DES* и *RSA*. Алгоритм системы *DES* является симметричным. Алгоритм *RSA* – асимметричный. Этот алгоритм (*RSA*) используется в программе *PGP – Pretty Good Privacy*, широко используемой для шифрования данных в *Internet.*

К отечественным стандартам относятся:

ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования»;

ГОСТ 34.11-94 «Криптографическая защита информации. Функция кэширования»;

ГОСТ 34.10-94 «Криптографическая защита информации. Процедура выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма».

ГОСТ Р 34.10-2001 Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи

Правовые и нормативные основы существования и развития криптографических средств защиты информации в Республике Молдова только начинают своё существование. Это основывается на данном этапе на следующих правовых документах:

- Закон Республики Молдова "Об информатизации и государственных информационных ресурсах" *№ 467-XV от 21.11.2003*
- Закон Республики Молдова "О доступе к информации*" № 982-XIV от 11.05.2000*
- Закон *PM ZPO264/2004* «Об электронном документе и цифровой подписи» *№ 264 от 15.07.2004*
- Постановление об утверждении Концепции Интегрированной системы электронного документооборота *N 844 от 26.07.2007*

Заключение:

Существует достаточно средств и стандартов для криптографической защиты информации, но применение этих средств в определённой системе – будь то политической, военной, экономической или информационной зависит во многом от специфики данной системы и от ее предрасположенности к использованию данных средств. Так, для эффективного внедрения криптографических механизмов информационной безопасности требуется достаточная правовая и нормативная база, в частности для Республики Молдова.

Литература:

1. «Защита компьютерной информации», А.В. Терехов, В.Н. Чернышов, ТГТУ, Тамбов 2003 г.
2. «Прикладная Криптография», А. Щербаков, А. Домашев, Москва 2003 г.
3. «Методы и средства защиты информации в компьютерных системах», Хорев П. Б., Академия, 2005.
4. «О современной криптографии», В. М. Сидельников, http://www.citforum.ru/security/cryptography/crypto/
5. «Криптографические основы безопасности», О.Р. Лапонина http://www.intuit.ru/department/security/networksec/
6. «Криптографические средства защиты информации», http://kiev-security.org.ua/box/1/15.shtml
7. Законы и нормативы http://www.mdi.gov.md/
8. Определения http://ru.wikipedia.org/