Исследование функциональных возможностей асимметричных алгоритмов шифроования

Орлов Павел Олегович
магистр «НИУ ИТМО»
г. Санкт-Петербург

Аннотация: в статье описана обобщенная математическая модель для исследования функциональных возможностей асимметричных алгоритмов шифрования. В качестве примера возьмем криптоалгоритмы RSA и Elgamal. Данная статья будет полезна для выбора асимметричного криптоалгоритма в прикладной практике исходя из исследованных функциональных возможностей.

Ключевые слова: криптография, криптографические системы с открытым ключом, криптографические средства защиты информации, уязвимость, угроза, электронная цифровая подпись, криптографический ключ.

Разработанная для исследования математическая модель может быть использована в качестве основы при проектировании более совершенных криптосистем в будущем, которые предназначены для шифрования и расшифрования конфиденциальной и любой другой информации.

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ

Разрабатываемая модель предназначена для исследования функциональных возможностей асимметричных криптосистем.

Для начала необходимо задать общее исходное описание модели.

K - Пространство ключей;

C - Пространство шифртекстов;

M - Пространство сообщений;

e и d - Ключ шифрования и расшифрования соответственно;

E_e - Функция шифрования для произвольного ключа $e \in K$, такая что $E_e(m)=c$;

D_d - Функция расшифрования, с помощью которой можно найти исходное сообщение m, зная шифртекст c: $D_d(c)=m$;

$E_e(D_d(c))=c$ и $D_d(E_e(m))=m$

$\{E_e : e \in K\}$ - Набор для шифрования;

$\{D_d : d \in K\}$ - Соответствующий набор для расшифрования;

Каждая пара (E, D) имеет свойство:

Если известно E_e, невозможно решить уравнение $E_e(m)=c$. Отсюда следует, что по данному e невозможно определить ключ расшифрования d.

Вся модель состоит из четырех элементов:

1. Генерация ключей;
2. Аутентичный канал передачи открытых ключей по открытому каналу;
3. Шифрование;
4. Расшифрование.

Рисунок 1 - Общая схема модели

ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ

Ссылаясь на обобщенную модель, были изучены функциональные возможности асимметричных криптоалгоритмов. Каждый из двух алгоритмов может быть использован не только для решения классической задачи криптографии, то есть для шифрования и расшифрования, но и для электронной цифровой подписи. Размер ключа каждого алгоритма может достигать 4096 бит. Была проанализирована скорость шифрования. Скорость полностью зависит от входных параметров алгоритма. Исходя из модели, скорость работы алгоритма El-Gamal медленнее, чем у алгоритма RSA. Криптостойкость работы алгоритма El-Gamal выше, чем у RSA, потому что криптосистема El-Gamal является асимметричным вероятностным алгоритмом шифрования и чем больше значений рандомизатора, тем лучше.

Рассмотренные алгоритмы обладают следующими функциональными возможностями: решают задачу ключевого управления (отсутствует обмен секретами между участниками защищенного взаимодействия), обеспечивают невозможность отказа от авторства и обеспечивают контроль целостности электронных документов, благодаря возможности реализации механизма ЭЦП.

Основным недостатком являются высокие вычислительные затраты, если сравнивать с симметричными криптоалгоритмами.

Список использованных источников

1. Бутакова Н.Г.,Семененко В.А., Федоров Н.В. Криптографическая защита информации: учебное пособие для вузов. – М. : Изд-во МГИУ, 2011 . – 316 с. – ISBN 978-5-2760-1503-3.
2. Алгоритмы: построение и анализ, 2-е издание. :Пер с англ. - М.: Издательский дом «Вильямс» ISBN 5-8459-0857-4 (рус.)
3. В.Г.Потемкин "Введение в Matlab".
4. ГОСТ 28147-89 — советский и российский стандарт симметричного шифрования, введённый в 1990 году, также является стандартом СНГ.