	"Средняя прибыль при высокой цене" – Zp_5									
g по Zp_5	0	7137	15485	25114	36094	338607	381935	427241	474531	523814
μ(g)	0	0,25	0.5	0.75	1	1	0,75	0.5	0,25	0

Следующим шагом является поиск максимальной прибыли, т.е. перед нами стоит задача сравнения нечетких чисел. Сравнение будет осуществляться на основе представления нечетких чисел в виде упорядоченных совокупностей α-уровней и сравнения четких интервалов на соответствующих α-уровнях. [4]

Проведя последовательное сравнение нечетких чисел Zp_1, Zp_2, Zp_3, Zp_4, Zp_5 находим, что максимальная средняя прибыль достигается при довольно высокой цене (нечеткое число Zp_4), именно она является искомой оптимальной ценой. Однако в качестве решения, которое должно быть осуществлено, нужно выбрать одно количественное значение. Таким образом, проблема состоит в том, чтобы нечеткое подмножество преобразовать в скаляр. [5]

Поскольку мы имеем дело с трапециевидным нечетким числом, максимальная принадлежность достигается в нескольких значениях базовой переменной. Для нахождения требующегося значения мы берем среднюю точку между теми конечными точками, в которых достигается максимум функции принадлежности:

$x_{опт}$ = (62170 + 65280)/2 = 63725. Именно эта цена, исходя из проведенных расчетов, принесет фирме максимальную прибыль.

Литература:

1. Борисов, А.Н. Принятие решений на основе нечетких моделей / А.Н. Борисов, О.А. Крумберг, И.П. Федоров – Рига: Зинатне, 1990. – 184 с.
2. Дубров, А. М. Моделирование рисковых ситуаций в экономике и бизнесе: учеб. пособие / А.М. Дубров, Б.А. Лагоша, Е.Ю. Хрусталев. - М.: Финансы и статистика, 1999. - 176 с.
3. Недосекин, А. Нечеткий финансовый менеджмент [Электронный ресурс] / А. Недосекин. – [2006]. – Режим доступа: http://www.finansy.ru/book/inv/001.htm
4. Дилигенский, Н.В. Моделирование, многокритериальная оптимизация и оценки качества функционирования производственно-экономических и медико-экологических систем в условиях неопределенности [Электронный ресурс] / Н.В. Д Дилигенский, Л.Г. Дымова, П.В. Севастьянов. – [2006]. – Режим доступа: http://sedok.narod.ru/s_files/poland/Wwedenie
5. Ринкс Д.Б. Эвристический подход к обобщенному календарному планированию производства с использованием лингвистических переменных: методология и применение // Нечеткие множества и теория возможностей. Последние достижения: Пер. с англ. / под ред. Ягера Р.Р. – М., Радио и связь, 1986. – с. 349-370.
6. Пивкин, В.Я. Нечеткие множества в системах управления. [Электронный ресурс] / В.Я. Пивкин, Е.П. Бакулин, Д.И. Кореньков. – [2006]. – Режим доступа: http://www.kstu.ru/oldsite/int_rus-1.htm

Аль-Хадша Фарес Али, *магистрант,*
Волгоградский государственный технический университет

Исследование сертификационного центра на базе веб-сервера

Аннотация. *В статье рассматриваются вопросы практического применения безопасных алгоритмов и протоколов современными серверами web.*

Abstract. *Using of secure protocols and algorithms on the base of modern web servers is presented in this work.*

В целях обеспечения безопасности передачи документов многие Web-приложения требуют подкрепления электронного документа цифровой подписью. Существующие веб-форумы, позволяют заходить с помощью логина и пароля, но с развитием Интернета можно заменить этот способ на цифровую подпись, и данная публикация, посвящена этой теме.

Электронная подпись и цифровые сертификаты

Метод цифровой подписи основан на использовании алгоритмов асимметричного шифрования. Такие алгоритмы (RSA, Diffie-Hellman) подразумевают наличие пары ключей — открытого (публичного) и закрытого (секретного, приватного). Предположим, необходимо переслать документ по безопасной электронной почте и поставить под ним цифровую подпись. Для этого документ обрабатывается специальной хэш-функцией, а полученное в результате значение (условно его можно назвать «контрольной суммой» или сверткой, далее: хэш-значение) зашифровывается закрытым ключом отправителя и пересылается вместе с документом. Это и есть цифровая подпись.

Получатель использует открытый ключ отправителя для того, чтобы извлечь хэш-значение из цифровой подписи. Подпись считается подлинной, если извлеченное из нее хэш-значение совпадет с результатом повторного хэширования полученного документа.

Также, если необходимо закрыть информацию от несанкционированного просмотра при передаче через Интернет, передаваемый документ кодируется с использованием открытого ключа получателя, и раскодировать его сможет только получатель — владелец закрытого ключа. Таким образом, необходимо передавать открытые ключи пользователей неискаженными.

Чтобы удостовериться в том, что открытый ключ не искажен и действительно принадлежит тому, за кого выдает себя отправитель, существует механизм цифровых сертификатов. Доверенное третье лицо уполномоченный по выдаче сертификатов (Certification Authority CA) заверяет электронной подписью соответствие между открытым ключом и именем (идентификатором) его владельца. Подписанные таким образом данные (открытый ключ, идентификатор владельца и некоторые другие связанные с ним атрибуты) и представляют собой цифровой сертификат. Генерация цифровых сертификатов регламентируется стандартом X.509.

Необходимо сразу отметить, что у владельца сертификат с открытым ключом (далее: цифровой сертификат) может храниться в персональном компьютере вместе с закрытым ключом. Такой сертификат будет называться персональным цифровым сертификатом. В программах электронной почты персональные цифровые сертификаты и закрытые ключи часто называют «цифровыми удостоверениями».

Любой цифровой сертификат пользователя или сертификат web-узла сопоставляет некоторые идентификационные данные с открытым ключом. Закрытый ключ, дающий возможность расшифровать послание или поставить цифровую подпись только его владельцу, хранится в персональном цифровом сертификате. Посылая свой сертификат посторонним лицам, пользователь фактически передает им свой открытый ключ, благодаря чему они могут посылать указанному пользователю зашифрованную информацию, расшифровать и прочитать которую может только владелец персонального цифрового сертификата (закрытого ключа).

Цифровая подпись, которой подписана какая-либо информация, является электронной идентификационной картой этой информации и пользователя, пославшего ее. Она сообщает получателю, что данная информация действительно пришла от определенного пользователя и не была испорчена или «подделана» посторонними лицами.

Чтобы получить возможность посылать зашифрованные или подписанные цифровой подписью сообщения, пользователю нужно получить персональный цифровой сертификат и настроить web-браузер на работу с этим сертификатом. Защищенный web-узел (название которого начинается с «https») при посещении его пользователем автоматически посылает ему свой сертификат.

Сертификаты представляют собой цифровые документы, которые позволяют и серверам, и клиентам проверить подлинность друг друга. Они необходимы для установления между сервером и браузером на компьютере клиента соединения по протоколу SSL, при котором информация передается в зашифрованном виде. Для работы протокола SSL необходимы серверный и клиентский сертификаты. Эти сертификаты могут быть получены от доверенной для обеих сторон независимой организации, называемой службой сертификации.

Существуют два типа сертификата:

1.1 Сертификаты сервера

Чтобы активизировать на веб-сервере средства безопасности SSL (Secure Sockets Layer), необходимо получить и установить действительный сертификат сервера. Сертификаты сервера являются цифровыми идентификаторами, содержащими сведения о веб-сервере и организации, поддерживающей содержимое веб-узлов на сервере. Сертификат позволяет пользователям проверять подлинность сервера и подлинность содержимого веб-узлов, а также устанавливать защищенные подключения.

Сертификат сервера также содержит открытый ключ, который используется для установления безопасного соединения между клиентом и сервером.

Сертификаты сервера позволяют пользователю подтвердить подлинность веб-узла. Сертификат сервера содержит подробные сведения для идентификации: название организации, связанной с содержимым сервера, название организации-поставщика сертификата, а также открытый ключ, используемый для установления безопасного соединения между клиентом и сервером. Эти сведения служат для пользователей гарантией подлинности содержимого веб-сервера и целостности системы безопасности подключения HTTP.

1.2 Клиентские сертификаты

При использовании SSL веб-сервер также имеет возможность проверить подлинность пользователей по содержимому клиентских сертификатов.

Сертификаты клиента представляют собой электронные документы, содержащие сведения о клиентах. Эти сертификаты, как и сертификаты сервера, содержат только эти сведения, но не содержат ключи шифрования, которые формируют часть средств безопасности SSL . Эти ключи, или шифровальные коды, из сертификатов клиента и сервера образуют Пару ключей , которая и обеспечивает шифрование и дешифрование данных, передаваемых через открытую сеть (Интернет).

Типичный сертификат клиента содержит следующие данные: идентификатор пользователя, идентификатор службы сертификации, Открытый ключ, используемый для установления защищенных подключений, а также проверочные данные, такие как срок действия и порядковый номер.

Проверка подлинности клиентских сертификатов совместно с шифрованием SSL позволяет реализовать защищенный метод проверки подлинности пользователей.

Протокол защещенный SSL

Протокол SSL предназначен для решения традиционных задач обеспечения защиты информационного взаимодействия:

- пользователь и сервер должны быть взаимно уверены, что они обмениваются информацией не с подставными абонентами, а именно с теми, которые нужны, не ограничиваясь паролевой защитой;
- после установления соединения между сервером и клиентом весь информационный поток между ними должен быть защищен от несанкционированного доступа;
- при обмене информацией стороны должны быть уверены в отсутствии случайных или умышленных искажений при ее передаче.

Протокол SSL позволяет серверу и клиенту перед началом информационного взаимодействия аутентифицировать друг друга, согласовать алгоритм шифрования и сформировать общие криптографические ключи. С этой целью в протоколе используются двухключевые (ассиметричные) криптосистемы, в частности, RSA.

Конфиденциальность информации, передаваемой по установленному защищенному соединению, обеспечивается путем шифрования потока данных на сформированном общем ключе с использованием симметричных криптографических алгоритмов (например, RC4_128, RC4_40, RC2_128, RC2_40, DES40 и др.). Контроль целостности передаваемых блоков данных производится за счет использования так называемых кодов аутентификации сообщений (Message Autentification Code, или MAC), вычисляемых с помощью хэш-функций (например MD5).

Протокол SSL включает два этапа взаимодействия сторон защищаемого соединения:

- установление SSL-сессии;
- защита потока данных.

На этапе установления SSL-сессии осуществляется аутентификация сервера и (опционально) клиента, стороны договариваются об используемых криптографических алгоритмах и формируют общий "секрет", на основе которого создаются общие сеансовые ключи для последующей защиты соединения. Этот этап называют также "процедурой рукопожатия".

На втором этапе (защита потока данных) информационные сообщения прикладного уровня нарезаются на блоки, для каждого блока вычисляется код аутентификации сообщений, затем данные шифруются и отправляются приемной стороне. Приемная сторона производит обратные действия: расшифрование, проверку кода аутентификации сообщения, сборку сообщений, передачу на прикладной уровень.

В SSL используется криптография с открытым (публичным) ключом, также известная как асимметричная криптография. Она использует два ключа: один - для шифрования, другой - для расшифровывания сообщения. Два ключа математически связаны таким образом, что данные, зашифрованные с использованием одного ключа, могут быть расшифрованы только с использованием другого, парного первому. Каждый пользователь имеет два ключа - открытый и секретный (приватный). Пользователь делает доступным открытый ключ любому корреспонденту сети. Пользователь и любой корреспондент, имеющий открытый ключ, могут быть уверены, что данные, зашифрованные с помощью открытого ключа, могут быть расшифрованы только с использованием секретного ключа.

SSL на сегодня является наиболее распространенным протоколом, используемым при построении систем электронной коммерции. С его помощью осуществляется 99% всех транзакций. Широкое распространение SSL объясняется в первую очередь тем, что он является составной частью всех браузеров и Web-серверов. Другое достоинство SSL - простота протокола и высокая скорость реализации транзакции.

В то же время, SSL обладает рядом существенных недостатков:

- покупатель не аутентифицируется;
- продавец аутентифицируется только по URL;
- цифровая подпись используется только при аутентификации в начале установления SSL-сессии.

Протокол безопасности SSL- это протокол, который защищает данные, пересылаемые между Web-браузерами и Web-серверами.

Secure Sockets Layer protocol (SSL) - протокол уровня передачи данных, который может служить промежуточным слоем между протоколом сетевого уровня (прим. TCP/IP) и протоколом уровня приложения (те HTTP).

SSL предлагает защищенный канал передачи данных между клиентом и сервером с использованием аутентификации, цифровых подписей и шифрования. Протокол разработан с поддержкой большого числа специальных алгоритмов, используемых для криптования, создания дайджестов и подписей. Он позволяет делать выбор алгоритмов с учетом требуемой надежности, соответствия принятому законодательству и . факторам, а так же расширение новыми алгоритмами. Выбор происходит во время начала протокольной сессии между клиентом и сервером

SSL также предоставляет возможность, что данные, получаемые с узла Web, приходят именно с предполагаемого узла и во время передачи они не были искажены. Любой Web-узел, чей адрес начинается с https, поддерживает SSL.Чаще всего SSL применяется для защищенного обмена данными между Web-браузерами и Web-серверами. Основное назначение протокола защиты состоит в следующем:

- Аутентификация сервера, гарантирующая пользователям, что они попали именно на тот узел Web, который хотели посетить;
- Создание такого защищенного канала, что информация может передаваться между браузером и сервером в закодированном виде, с тем чтобы никто не смог исказить данные во время пересылки.

Пользователи Web могут распознать узел, который поддерживает SSL, по тому, что адрес Web-страницы начинается с https.

Таким образом, использование электронной цифровой подписи и защищенных соединений по проколу SSL позволяет существенно повысить безопасность при обмене данными пользователя с Веб-сервером.