УДК 621.391.052
А.О. Горьева
Севастопольский национальный технический университет
ул. Университетская 33, г. Севастополь, Украина, 99053
E-mail: kvt@sevgtu.sebastopol.ua

СТРУКТУРНОЕ ОПИСАНИЕ КРИПТОГРАФИЧЕСКОЙ СИСТЕМЫ СВЯЗИ

Рассматривается задача построения структуры криптографической системы связи с учетом поставленных целей и необходимых функций, которые она должна реализовывать. Решена задача векторной оптимизации и приведен численный пример.

Задача надежной защиты авторских прав, прав интеллектуальной собственности или конфиденциальных данных от несанкционированного доступа является одной из старейших и до конца не решенных на сегодняшний день. В связи с интенсивным развитием и распространением технологий цифровой обработки различных типов сигналов, вопрос защиты информации, представленной в цифровом виде, является чрезвычайно актуальным.

Преимущества представления и передачи данных в цифровом виде (легкость восстановления, высокая помехоустойчивость, перспективы использования универсальных аппаратных и программных решений) могут быть перечеркнуты с легкостью, с которой возможно их похищение и модификация. Поэтому актуальным является вопрос разработки методов защиты информации организационного, методологического и технического характера. Среди них — методы криптографии и стеганографии.

Существующие методы криптографии решают указанные проблемы лишь частично. К сожалению, в настоящее время нет четких рекомендаций к обоснованному применению тех или иных методов, не формализовано описание для многих криптосистем, нет единого математического аппарата для решения большинства криптографических задач, является открытым вопрос о том, какую информацию считать общедоступной, а какую — конфиденциальной. Инженерам и разработчикам программного обеспечения приходится решать поставленную задачу обеспечения безопасности данных, не имея четких рекомендаций, какой из алгоритмов эффективнее в той или иной ситуации [1].

Целью данной работы является разработка методики построения оптимальной структуры криптографической системы связи. Существующие модели не позволяют адекватно и полно описать информационные процессы, происходящие в системах передачи информации. Требуется детальная проработка аспектов поведения таких систем на различных уровнях функционирования.

Содержательное описание задачи. Клиенты обмениваются сообщениями посредством серверного узла. Число клиентов в данной системе равно N. Каждый клиент является и отправителем и получателем. Структура описанной системы изображена на рисунке 1.

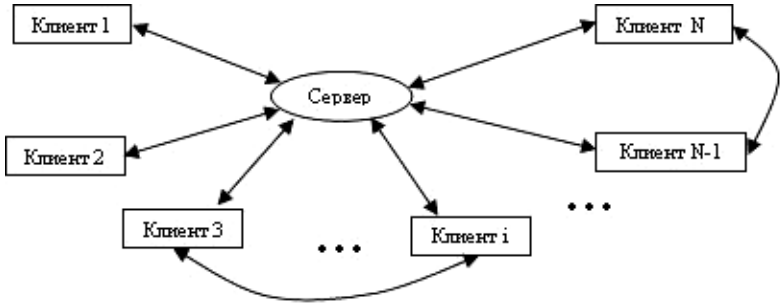

Рисунок 1 — Структурная схема системы связи

Каналы связи между клиентом и сервером являются дуплексными. Как видно из рисунка 1, между клиентами существуют каналы связи минуя сервер. Сообщения передаются только в зашифрованном виде.

Введем следующие обозначения:

M — открытый текст, который может представлять собой двоичные данные, текст, звуковое сообщение, видеопоток и т.д.;

C — шифротекст, которые представляет собой зашифрованное сообщение M, в зависимости от функции шифрования размер C может быть равен, больше или меньше размера M;

E — функция шифрования, которая воздействует на M, создавая C:

$$E(M) = C; \tag{1}$$

D — функция дешифрования, которая воздействует на шифротекст C, восстанавливая M:

$$D(C) = M\ . \tag{2}$$

Конечной целью является восстановление первоначального текста M, поэтому должно выполнятся следующее равенство:

$$D(E(M)) = M \ . \tag{3}$$

В системе шифрование и дешифрование, в соответствии с рисунком 2, может выполняться со стороны сервера и стороны клиента. Дисциплина функционирования такова, что $E(M)$ и $D(C)$ должны реализовывать один и тот же алгоритм шифрования/дешифрования для сервера и для клиента K_i.

Рассмотрим случай, когда сообщение передается от клиента к серверу. На стороне клиента сообщение шифруется при помощи функции $E(M)$, далее по каналу связи передается сообщение C, на которое со стороны сервера воздействует функция $D(C)$. Это самый простой способ обеспечения конфиденциальности переписки. Функции $E(M)$ и $D(C)$ — это криптографические алгоритмы. В случае, если необходимо обеспечить более надежную защиту передаваемых данных, то необходимо использовать в системе криптографические алгоритмы с ключами, причем лучше использовать различные ключи для шифрования и дешифрования.

Обозначим ключ шифрования через k_1, а ключ дешифрования — k_2. Тогда функции (1) — (3) запишем следующим образом

$$\begin{aligned} &E_{k_1}(M) = C; \\ &D_{k_2}(C) = M; \\ &D_{k_2}(E_{k_1}(M)) = M. \end{aligned} \tag{4}$$

Согласно вышеизложенному, процесс криптографической защиты сообщений можно представить в виде, показанном на рисунке 2.

Рисунок 2 — Структура канала связи

Для обеспечения дополнительной защиты передачи данных введем в систему следующие функции.

1. Проверка подлинности. Получатель сообщения может проверить его источник, лицо, совершающее несанкционированный доступ, не сможет замаскироваться под кого-либо.

2. Целостность. Получатель сообщения может проверить, не было ли сообщение изменено в процессе доставки, нарушитель не сможет подменить правильное сообщение ложным.

3. Неотрицание авторства. Отправитель не сможет ложно отрицать отправку сообщения.

С использованием подобной дополнительной информации, всегда можно установить от кого было точно получено сообщение [2].

Изобразим описанную структуру на рисунке 3.

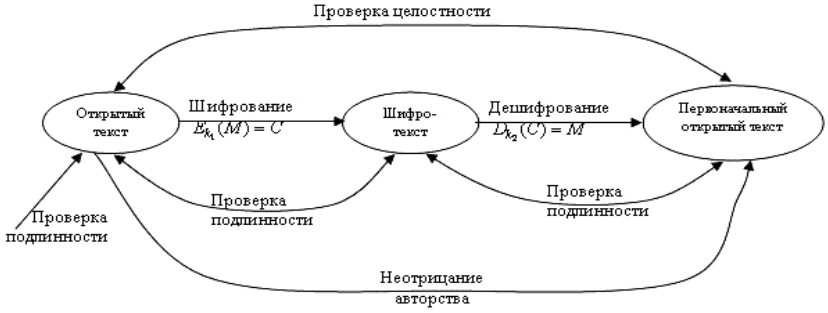

Рисунок 3 — Структура шифрования и дешифрования сообщения

Описываемая система призвана обеспечить выполнение следующих целей:

— защита конфиденциальных сообщений;

— установление автора сообщений;

— исключение ситуаций подмены и искажения сообщений.

В связи с указанным списком, целесообразно выделить функции, которые должна реализовывать криптосистема. Цель защиты конфиденциальности данных достигается с использованием криптографических алгоритмов на основе различных ключей шифрования и дешифрования. Запрет неотрицания авторства реализуется с использованием цифровой подписи или сигнатуры. Исключить подмену или модификацию сигнатур можно различными способами, например: контрольная сумма, различные криптографические хэш-функции и т.д. В нашем распоряжении имеется несколько структур криптографической системы связи, которые могут обеспечивать достижение указанных целей.

Для удобства формализации данной модели введем понятия субъекта и объекта системы, а также установим правила взаимодействия между ними.

Под субъектом (S_i) будем понимать передающую или принимающую стороны, т.е. конечные точки приема и передачи открытых и зашифрованных сообщений. В качестве объекта (O_i) рассматриваем непосредственно сообщение, которое может находиться в открытом или зашифрованном виде.

Рассмотрим множество состояний, в которых оказываются S_i и O_i при работе системы.

S_i при взаимодействии с S_j выполняет одно из следующих действий:

— передает информацию (PI);

— осуществляет проверку целостности информации (CI);

— проверяет подлинность сообщения (PS);

— не позволяет осуществлять отказ от авторства переданной информации (OAI).

Множество объектов O_i может находиться в двух состояниях:

— зашифрованная информация;

— открытая информация.

Процесс взаимодействия субъекта S_i и объекта O_j представлен схемой (рисунок 4):

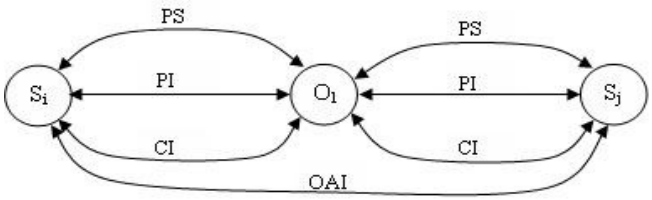

Рисунок 4 — Структурная схема процесса взаимодействия
между субъектами S_i и S_j и объектом O_l

В рассматриваемой системе число объектов и субъектов конечно и соответственно равно K и N.

На рисунке 4 изображен процесс передачи сообщения O_l от субъекта S_i субъекту S_j. Здесь возможны следующие варианты взаимодействия:

— субъект S_i проверяет целостность информации;

— передает объект O_l;

— проверяет подлинность сообщения;

— устанавливает авторство.

Описанные процессы являются двусторонними. Субъекты S_i и S_j могут взаимодействовать указанным способом одновременно либо независимо друг от друга в разные моменты времени.

Для реализации существующих процессов в описанной системе можно использовать следующие общепринятые понятия:

— для шифрования и дешифрования — выбор оптимального криптографического алгоритма;

— для проверки целостности использовать хэш-функции;

— для запрета неотрицания авторства — подписывать сообщения, используя протоколы цифровой сигнатуры;

— для проверки подлинности — аутентификация в системе.

Методика выбора оптимальной структуры криптографической системы связи. Пусть количество альтернативных структур криптосистемы равно n, число функций, реализуемых системой — m. Вектор критериев обозначим через $X = \{X_1, X_2 \dots X_k\}$. Построим оценочную матрицу A, где элемент матрицы α_{ij} — оценка j-ой структуры с точки зрения функции i и влияния критерия x_i. Несложно провести выбор оптимальной структуры, используя метод анализа иерархий, предложенный Т. Саати. В качестве критериев целесообразно использовать критерии, подходящие для оценки той или иной функции, например, при оценке качества шифрование/дешифрование логично руководствоваться критериями криптостойкости, надежности, быстродействия и т.д.

Для примера приведем следующую задачу. Имеются четыре альтернативные варианта структуры S_i криптографической системы (i=1...n, n=4), каждая из которых реализует один и тот же набор функций (m=4) различными методами: шифрование/дешифрование; проверка подлинности; целостность; неотрицание авторства. Структура S_1 использует следующие методы: шифрование/дешифрование с использованием алгоритма RSA; проверка подлинности — с использованием парольного доступа (постоянный пароль, требующий ввода при отправке сообщения); целостность — использование функции N-хэш; неотрицание авторства — сообщение подписывается с помощью протоколов цифровой сигнатуры. Опишем структуру S_2: шифрование/дешифрование с использованием алгоритма DES; проверка подлинности — с использованием SecurID (пароль вырабатывается специальным генератором на стороне клиента и при каждом входе в систему он новый); целостность — использование хэш-функции MD4; неотрицание авторства — сообщение подписывается с помощью протоколов цифровой сигнатуры. Структура S_3: шифрование/дешифрование — алгоритм DES; проверка подлинности — с использованием SmartID (пароль хранится на smart-карте или USB-устройстве); целостность — использование хэш-функции MD5; неотрицание авторства — сообщение

подписывается с помощью протоколов цифровой сигнатуры. В структуре S_4 шифрование/дешифрование осуществляется с использованием алгоритма RSA, проверка подлинности — технология MobilID (пользователю пароль высылается на мобильный телефон с использованием SMS); целостность — хэш-функция MD2; неотрицание авторства — сообщение подписывается с использованием протоколов цифровой сигнатуры.

Таким образом, данная задача относится к классу многокритериальных задач выбора оптимального решения и может быть решена методами теории принятия решений, в частности методом анализа иерархий (МАИ). МАИ является систематической процедурой для иерархического представления элементов, определяющих суть любой проблемы. Метод состоит в декомпозиции проблемы на более простые составляющие части и дальнейшую обработку суждений попарным сравнением [3].

В данной задаче решается проблема выбора структуры криптографической системы связи. Следовательно, целью решения будет выбор единственной из альтернативных структур. Определим критерии, по которым осуществляется выбор. К ним можно отнести, например, следующие:

1) функция шифрования/дешифрования всегда оценивается криптостойкостью алгоритма, т.е. временем, необходимым на расшифровку текста С, если криптоаналитику известен алгоритм шифрования, но неизвестен ключ;

2) эффективность средств аутентификации оценивается количественно исходя из стоимости реализации каждого метода;

3) качество хэш-функции оценивается количественно с точки зрения вероятности появления коллизий;

4) эффективность подписи с использованием цифровой сигнатуры можно оценить количественно с точки зрения критерия вероятности раскрытия сигнатуры третьим лицом.

Построим матрицу оценок для рассматриваемого случая. Будем использовать относительные значения оценок критериев в соответствии со следующим выражением:

$$V_i = \frac{V_{iф}}{V_б}, \tag{5}$$

где $V_{iф}$ — фактическое значение i-го критерия структуры S_i; $V_б$ — базовое значение.

Передавались текстовые сообщения, содержащие в себе банковскую информацию, размер сообщения — блок символов объемом 1024. Базовое значение для алгоритма RSA — 112 условных единиц времени, для DES — 98 условных единиц времени. Если $V_{iотн}$>>1, то алгоритм шифрования/дешифрования более надежный. Критерий 2 оценивается по относительной шкале от 0 до 10 (чем ниже стоимость реализации, тем выше оценка). Его базовое значение — 5 баллов. Для оценки хэш-функции принято считать, что чем меньше вероятность появления коллизий, тем качественнее ее реализация. Для этого критерия базовое значение равно 0,03. Чем меньше относительная оценка, тем эффективнее считается хэш-фенкция. Чем меньше вероятность раскрытия сигнатуры третьим лицом, тем надежнее цифровая подпись сообщения. Базовое значение критерия равно 0,07. Фактические значения для каждой структуры получены с использованием имитационного моделирования. Оценочная матрица приведена в таблице 2.

Таблица 2 — Матрица оценок для структур S_i

	S_1	**S_2**	**S_3**	**S_4**
Криптостойкость	2,5	1,9	1,4	2,7
Аутентификация	2,0	1,4	1,2	0,6
Хэш-функции	1,4	1,2	0,6	0,9
Цифровая сигнатура	1,1	0,8	1,3	0,9

Составляется иерархия с учетом поставленной цели — выбор оптимальной структуры. Далее разрабатываются матрицы попарных сравнений для критериев на каждом уровне иерархий. Затем проводится оценка полученных матриц с использованием методов МАИ, находятся векторы локальных приоритетов, после чего строится таблица соответствия локальных приоритетов второго уровня локальным приоритетам третьего уровня, вычисляются глобальные приоритеты. Проанализировав полученную таблицу, получаем, что структура S_4 предпочтительнее S_1, S_1 в свою очередь предпочтительнее S_2, а S_2 предпочтительнее S_3, т.е. $S_4 \succ S_1 \succ S_2 \succ S_3$.

В заключение отметим, что предложенный подход, т.е. структурное описание криптографической системы защиты с дальнейшей оценкой методов реализации каждой функции, позволит специалистам по компьютерной безопасности проектировать адекватные и эффективные системы безопасности.

Перспективами дальнейших исследований в данном направлении, например, могут быть следующие:

1. определение областей ограничения для объектов (длина, время передачи, разбивка на пакеты, и т.д);

2. анализ криптостойкости процессов на основе методов имитационного моделирования;

3. описание правил взаимодействия между субъектом и объектом на основе криптографических протоколов.

Библиографический список

1. Смарт Н. Криптография / Н. Смарт. — М.: Техносфера, 2006. — 528 с.

2. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. / Б. Шнайер. — К.: Триумф, 2002. — 816 с.

3. Саати Т. Принятие решений — метод анализа иерархий / Т. Саати. — М.: Радио и связь, 1993. — 320 с.

Поступила в редакцию 6.05.2008 г.