3 Забезпечення комп'ютерної безпеки в державних, банківських та інших інформаційних системах

УДК 681.3.06

ЭФФЕКТИВНОСТЬ СМЕШАННЫХ АЛГОРИТМОВ ШИФРОВАНИЯ

Галина Козина, Владимир Журавлев
Запорожский национальный технический университет

Аннотация: **Предложен алгоритм шифрования информации, предусматривающий возможность адаптации (с изменением криптостойкости и имитостойкости) скорости работы системы под конкретную аппаратуру пользователя и обеспечивающий работу в реальном маштабе времени.**
Summary: **Adaptive on-line encryption algorithm is proposed. Algorithm is used mixed cipher blocks and mixed (symmetric and asymmetric) keys.**
Ключевые слова: **Информация, информационная безопасность, техническая защита информации, режим работы в реальном маштабе времени.**

I Введение

Во всем комплексе общепринятых требований к применяемым в настоящее время криптографическим алгоритмам и устройствам наиболее весомыми являются показатели криптостойкости, имитостойкости и скорости обработки (шифрования и дешифрования) информации, которые можно рассматривать с позиций работы пользователя в реальном масштабе времени [1].

Можно выделить следующие установившиеся положения [2]:

- асимметричные (с открытым ключом) либо двухключевые алгоритмы шифрования обладают исключительной возможностью переопределения нижнего предела криптостойкости, что и предопределило их всестороннее применение в коммуникационных устройствах с разделением времени передачи и обработки конфиденциальных сообщений;
- симметричные либо одноключевые алгоритмы шифрования, в отличие от алгоритмов с открытым ключом, обладают хорошими скоростными показателями обработки (шифрования и дешифрования) информации, что является основой для применения их в криптографических системах, предназначенных для работы в реальном масштабе времени.

II Основная часть

Для достижения указанных характеристик, по нашему мнению, наиболее целесообразен комбинированный подход, при котором асимметричные алгоритмы шифрования применяются совместно с симметричными, а объем их применения определяется пользователем исходя из субъективной оценки возможности работы в реальном масштабе времени.

Комбинированная реализация криптоалгоритмов предусматривает наличие двух модулей шифрования: симметричного и асимметричного.

Так как при засекречивании информации в реальном масштабе времени двухключевые шифры находят ограниченное применение, то наиболее эффективными могут быть гибридные криптосистемы, в которых информация шифруется с помощью одноключевых алгоритмов, а распределение сеансовых ключей для шифрации информационных блоков осуществляется по открытому каналу с помощью двухключевых алгоритмов.

При реализации рассматриваемой криптографической системы должны быть решены следующие задачи:

- разработка и исследование алгоритма смешанного шифрования;
- определение оптимального количества и параметров блоков шифрования одноключевыми алгоритмами для обеспечения работы пользователя в реальном масштабе времени;
- разработка программы–оболочки, облегчающей пользователю адаптацию алгоритма смешанного шифрования под конкретный аппаратный состав рабочей станции.

Возможный вариант структурной схемы системы приведен на рис. 1.

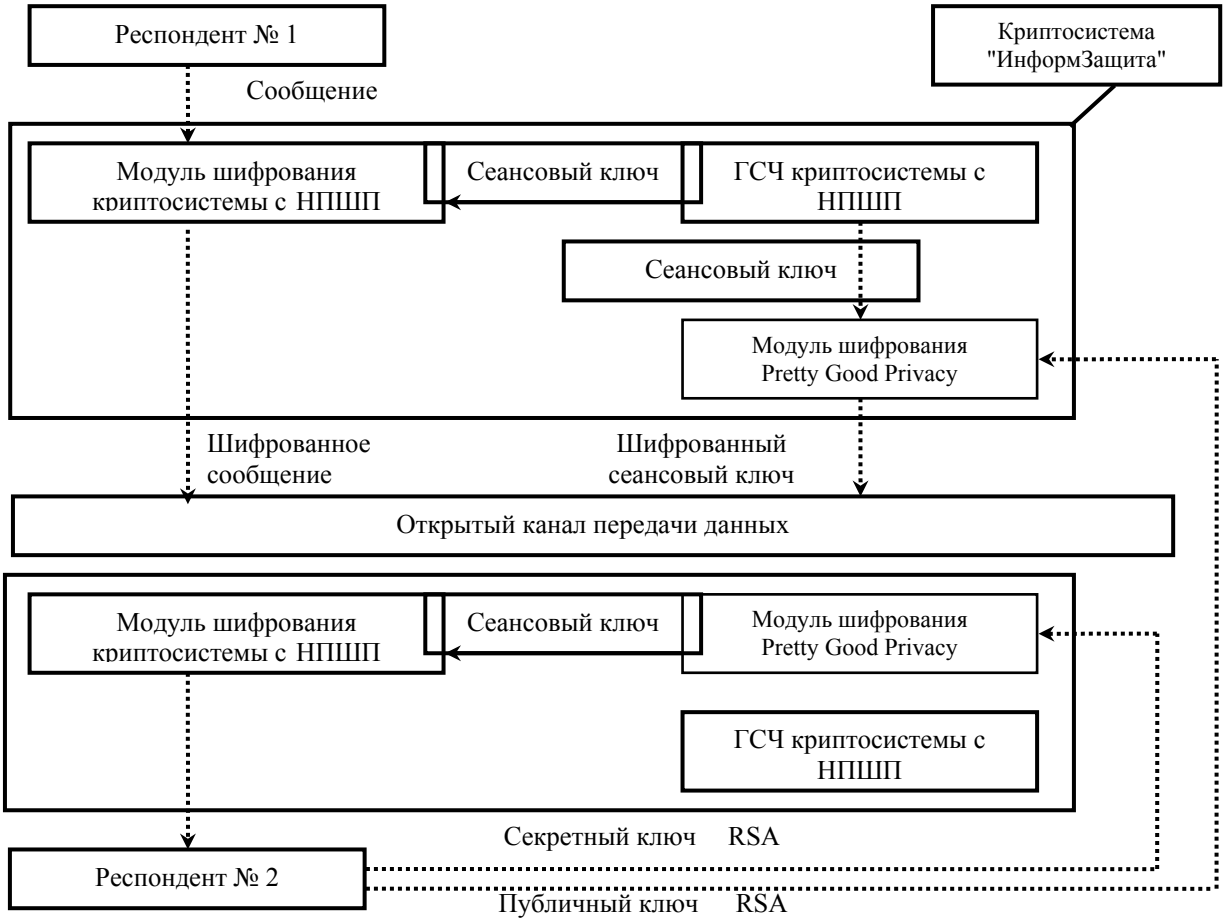

Рисунок 1 – Структурная схема криптосистемы с НПШП

Данная реализация предусматривает наличие двух модулей криптосистемы: модуль криптосистемы с неопределенной перестановкой шифрующих процедур (НПШП) и модуль асимметричной системы RSA.

Модуль НПШП представляет собой переменный набор одноключевых алгоритмов шифрования, ключевые параметры, количество, порядок следования и число проходов которых определяется сеансовым ключом системы. В модуле производится шифрование блоков сообщения в соответствии с сеансовым ключом системы.

Модуль асимметричной системы RSA предназначен для шифрования секретного сеансового ключа системы с НПШП публичным ключом респондента.

Последовательность действий, проводимых криптографической системой при шифровании сообщения:

- с помощью адаптивного к структуре системы генератора формируется ключ, который определяет параметры, порядок следования и количество проходов одноключевых алгоритмов шифрования;
- в соответствии с данным ключом производится операция шифрования секретного сообщения и формируется выходная последовательность зашифрованных данных, которая передается по открытому каналу передачи данных;
- ключ шифруется с помощью открытого ключа респондента и передается в открытый канал передачи данных;
- на приемном конце респондент с помощью своего секретного ключа RSA восстанавливает сеансовый ключ системы.

Алгоритм с НПШП использует несколько блоков шифрующих одноключевых алгоритмов, каждый из которых обеспечивает один шаг шифрования блока исходного текста сообщения.

Программа шифрующей процедуры должна поддерживать блочное и поточное шифрование в соответствии с последовательно расположенными блоками, каждый из которых обеспечивает вычисления, необходимые на каком-то одном шаге криптографических преобразований.

На подготовительном этапе, в зависимости от выбранного пользователем пароля, осуществляется построение ключевого поля, вычисление необходимых ключевых констант-операндов и формирование некоторой перестановки целых чисел 1, 2, 3, …, N, которые являются номерами блоков. Данная перестановка в рассматриваемой криптосистеме является типом ключевого элемента.

Алгоритмы шифрующих процедур криптосистемы с НПШП базируются на стандартных методах шифрования и кодирования.

Если принять, что длина блока исходного текста сообщения равна D, количество одноключевых алгоритмов, применяемых в системе с НПШП, равно N, длина ключа соответствующего алгоритма равна Ki (i=1, N), производительность алгоритма при заданной длине ключа Ai (i=1, N), а число проходов перешифрования для соответствующего алгоритма равно Pi, (i=1, N) то количество операций Кор на реализацию шифрования одного криптоблока можно оценить следующим выражением:

$$Кор=f(N, Ki , Ai, Pi, D). \quad (1)$$

Пусть у пользователя (респондента) эксплуатируется рабочая станция с нижеследующими параметрами, определяющими основную производительность работы системы с НПШП:

О – коэффициент качества операционной системы для данного типа приложений;

С – обобщенный показатель производительности материнской платы;

П – производительность процессора для данных приложений;

М – коэффициент влияния объема оперативной памяти на производительность;

Н – производительность файла подкачки жесткого диска при работе с операционными системами Windows;

КН – производительность каналообразующего модуля;

Л – коэффициент качества канала связи при заданной производительности КН.

Тогда интегральную производительность (количество операций в единицу времени) рабочей станции пользователя можно оценить следующим выражением:

$$Прс=g(О, С, П, М, Н, КН, Л). \quad (2)$$

Определяя из зависимостей (1), (2) величину Тш=Кор/Прс – время дешифрации одного блока шифротекста, субъективное для каждого респондента, можно определить оптимальные пользовательские параметры алгоритма НПШП.

Затем, при необходимости, можно решить обратную задачу: расчета криптостойкости и имитостойкости полученной системы при определенных на предыдущем шаге параметрах алгоритма НПШП. При неудовлетворительных показателях криптостойкости можно повторить вычисления, варьируя пользовательский параметр Тш.

III Выводы

В заключение отметим некоторые характеристики рассмотренной криптосистемы.

При минимальной длине ключа RSA раскрытие исходного текста может быть достигнуто только при прямом переборе всех возможных вариантов секретного ключа, что в настоящее время для существующих вычислительных мощностей маловероятно. Стойкость криптосистемы определяется перебором всех возможных ключей. Даже при знании шифрующих процедур криптосистемы подбор секретного сеансового ключа не представляется возможным, так как при тридцати шифрующих процедурах в криптосистеме количество возможных вариантов составляет приблизительно 2^{1032}.

Высокая эффективность предложенного алгоритма шифрования достигается тем, что в роли шифрующих процедур выступают быстрые одноключевые алгоритмы шифрования.

Двухключевой алгоритм RSA применяется для шифрования незначительного по объему сеансового ключа криптосистемы.

Отличительная особенность предложенного алгоритма заключается в том, что при изменении количества проходов перешифрования и длины ключей криптоалгоритмов имеется возможность адаптации (с изменением криптостойкости и имитостойкости) скорости работы системы под конкретную аппаратуру пользователя, обеспечивая режим работы в реальном маштабе времени.

Литература: 1. Домарев В. В. Защита информации и безопасность компьютерных систем. – К.: Изд. «ДиаСофт», 1999. – 480 с. 2. Романец Ю. Ф., Тимофеев П. А., Шаньгин В. Ф. Защита информации в компьютерных системах и сетях. – М.: Радио и связь, 1999.