Кокшаров Роман Андреевич
студент
Сулейманов Рустам Нафисович
студент
Кротова Елена Львовна
канд. физ.-мат. наук, доцент
ФГБОУ ВПО «Пермский национальный
исследовательский политехнический университет»
г. Пермь, Пермский край

КРИПТОГРАФИЧЕСКИЙ ПРОТОКОЛ ФЕЙГА – ФИАТА – ШАМИРА (FFS)

Аннотация: *в статье рассмотрен метод шифрования данных с нулевым разглашением. В работе представлен принцип работы, его стойкость, а также выделены достоинства и недостатки.*

Ключевые слова: *криптографический протокол, протокол с нулевым разглашением, криптостойкость, идентификация, аутентификация.*

Начнем с определения криптографического протокола – это такой протокол, в котором используются криптографические методы и средства для достижения определенных целей.

Криптографический протокол, позволяющий одной из сторон убедится в достоверности секретной информации другого лица, не предъявляя при этом ни единого бита информации называется протоколом с нулевым разглашением.

Один из протоколов с нулевым разглашением это – протокол Фейга – Фиата – Шамира, который был доработан из более раннего протокола Фиата – Шамира в 1986 году.

Стойкость данного протокола основывается в первую очередь на проблеме извлечения квадратного корня по модулю значительно большого числа n, на простые множители.

Данный протокол выполняет задачу идентификации и аутентификации.

Идентификация необходима нам для присвоения субъектам и объектам идентификатора или сравнения идентификатора с присвоенными идентификаторами [2]. А аутентификация отвечает за процедуру проверки подлинности идентификаторов. Для того что бы аутентифицировать некого субъекта, верификатор должен задать некоторое количество вопросов претенденту. Претендент в свою очередь отвечает на поставленные вопросы на основании секретной информации. На основании этих ответов, верификатор определяет, действительно ли он обладает секретными сведениями.

Протокол FFS реализуется следующим образом. Существует три лица: претендент, верификатор и центр управления и распределения ключей(ЦУиРК).

1. ЦУиРК формирует модуль, который является общим для всех пользователей: $n = pq$, где p и q – простые числа.

При этом необходимо выполнить следующие условия:

$$p \equiv 3 \; mod \; 4 \text{ и } q \equiv 3 \; mod \; 4 \text{ [1, с. 7].}$$

Благодаря данному условию появляется вспомогательная защита протокола, т.к. нам сложнее факторизовать модуль n.

После вычисления модуля, ЦУиРК определяет k и t, где k – размер вектора; t – число раундов проверки. Это секретные параметрами системы.

2. Каждый претендент А проделывает определенные действия:

Проверяет векторную строку случайных чисел S = (s_1, s_2, …, s_k), где все значения {si} принадлежат диапазону 1≤ s_i ≤ (n – 1) и подвергает, что бы выполнить равенство НОД(s_i, n) = 1;

Определяет векторную строку рандомных бит B = (b_1, …, b_k);

Рассчитывает множество значений:

$$v_i = (\text{-}1)^{b_i} \; (s_i^2)^{\text{-}1} s_i mod \; n, \text{для } 1 \leq \; i \; \leq k \text{ [1, с. 7].}$$

Устанавливает связь и происходит процесс идентификации и авторизации в ЦУиРК, после чего следует регистрация в центре своего ключа V = (v_1, …,v_k);

Центр управления и распределения ключей проверяет правильность значений представленного ключа, высчитывая символ Якоби J(v_i) mod n. Если символ Якоби будет равен +1, то ключ верен, в противном случае ключ не фиксируется.

Вектор s является секретным ключом претендента, который не следует разглашать.

3. Претендент А и верификатор В в каждом раунде обмениваются данными по алгоритму:

Претендент А определяет случайное число r, $1 \leq r \leq (n-1)$. Отбирает рандомным образом бит из вектора b, а после чего вычисляет число:

$$v_i x = (-1)^{b_i} r^2 mod\ n,$$

посылаемое верификатору В: А → В: $x = \pm r^2 \bmod n$

В качестве ответа верификатор В определяет случайным образом и передает претенденту А вектор $e = (e_1, \ldots, e_k)$, содержащий в себе k бит информации:

$$A \leftarrow B: e = (e_1, \ldots, e_k)\ e_i \{0,1\}$$

Претендент А определяет и передает обратно верификатору В число y

$$y = r \cdot s_i \prod_{i=1}^{k} s_i^{e_i} mod\ n,$$ [1, с. 8].

Далее проходит сверка с ранее принятым числом x. Если

$$z = \pm x \text{ и } z \neq 0,$$

то на данном раунде достоверность рассматриваемого идентификатора подтверждается. Полагается, что претендент убедил верификатора насчет наличия у него требуемых знаний, для выбранной длины вектора k. Для того чтобы претендент успешно прошел аутентификацию, он должен в течении заданного количества раундов подтверждать достоверность представляемого идентификатора.

Успешная криптографическая атака, на основе подмены с помощью открытых текстов, выполняется с вероятностью 2^{-kt} в течении t циклов. Но для увеличения скорости аутентификации претендента и уменьшении вероятности обмана верификатора необходимо какое-то компромиссное количество раундов. И в качестве условия доказательства с нулевым разглашением знаний и допустимый уровень защищенности выполняются, если $k = O(\log \log n)$ и $t = \Theta(\log n)$.

Достоинства и недостатки протокола FFS будем рассматривать относительно аналогичных протоколов, такие как протокол Шнора и Гиллоу – Куискутера.

Достоинствами данного протокола можно выделить следующее:

– высокий уровень безопасности по сравнению с аналогичными протоколами. В них количество операций в 3 раза больше при вычислениях;

– время работы протокола существенно ниже;

– простой в реализации.

Недостатки:

– большое число итераций;

– большое требование к объему хранимой секретной информации.

Данный протокол FFS является одним из основных протоколов с нулевым разглашением. Как мы видим у него есть достоинства и недостатки. Самое важное при организации защиты информации в коммерции, является наличие высокого уровня безопасности при простой реализации.

Список литературы

1. Википедия: свободная электронная энциклопедия: на русском языке [Электронный ресурс]. – Режим доступа: http://ru.wikipedia.org (дата обращения: 22.05.2016).

2. Саломатин С.Б. Методические указания к лабораторной работе криптографические протоколы по курсу «Защита информации» для студентов специальности 39 01 02 «Радиоэлектронные системы». Мн.: БГУИР, 2002. – 22 с. [Электронный ресурс]. – Режим доступа. – http://www.studfiles.ru/preview/1437861/ (дата обращения: 22.05.2016).