ЛАБОРАТОРНАЯ РАБОТА 5

ПРОТОКОЛ ИДЕНТИФИКАЦИИ С НУЛЕВОЙ ПЕРЕДАЧЕЙ ДАННЫХ

Цель работы: формирование умений проверки подлинности удаленных пользователей с помощью протокола идентификации с нулевой передачей данных.

Теоретические сведения

Широкое распространение интеллектуальных карт (смарт-карт) для разнообразных коммерческих, гражданских и военных применений (кредитные карты, карты социального страхования, карты доступа в охраняемое помещение, компьютерные пароли и ключи, и т. п.) потребовало обеспечения безопасной идентификации таких карт и их владельцев. Во многих приложениях главная проблема заключается в том, чтобы при предъявлении интеллектуальной карты оперативно обнаружить обман и отказать обманщику в допуске, ответе или обслуживании.

Для безопасного использования интеллектуальных карт разработаны протоколы идентификации с нулевой передачей знаний. Секретный ключ владельца карты становится неотъемлемым признаком его личности. Доказательство знания этого секретного ключа с нулевой передачей этого знания служит доказательством подлинности личности владельца карты.

Схему идентификации с нулевой передачей знаний предложили в 1986 г. У. Фейге, А. Фиат и А. Шамир. Она является наиболее известным доказательством идентичности с нулевой передачей конфиденциальной информации.

Прежде всего, в схеме идентификации с нулевой передачей знаний выбирают случайное значение модуля n, который является произведением двух больших простых чисел. Модуль n должен иметь длину 512...1024 бит. Это значение n может быть представлено группе пользователей, которым придется доказывать свою подлинность. В процессе идентификации участвуют две стороны:

сторона A, доказывающая свою подлинность;

сторона B, проверяющая представляемое стороной А доказательство.

Для того чтобы сгенерировать открытый и секретный ключи для стороны A, доверенный арбитр (Центр) выбирает некоторое число V, которое является квадратичным, вычетом по модулю n. Иначе говоря, выбирается такое число V, что сравнение

$x^2 = V(mod\ n)$ имеет решение, и существует целое число $V^{-1} mod\ n$.

Выбранное значение V является открытым ключом для A. Затем вычисляют наименьшее значение S, для которого

$S = \sqrt{(V^{-1})}(mod\ n)$.

Это значение S является секретным ключом для A.

Теперь можно приступить к выполнению протокола идентификации

1. Сторона *A* выбирает некоторое случайное число *r*, $r < n$. Затем она вычисляет

$x = r^2$ **mod** *n* и отправляет *x* стороне *B*.

2. Сторона *B* посылает *A* случайный бит *b*.

3. Если $b = 0$, тогда *A* отправляет *r* стороне *B*. Если $b = 1$, то *A* отправляет стороне *B*:

$y = r$**Smod** *n*

4. Если $b = 0$, сторона *B* проверяет, что $x = r^2$ **mod** *n* чтобы убедиться, что *A* знает

√ (x). Если $b = 1$, сторона *B* проверяет, что $x = y^2 \cdot V$ **mod** *n*, чтобы быть уверенной, что A знает $\sqrt{(V-1)}$.

Эти шаги образуют один цикл протокола, называемый *аккредитацией*. Стороны *A* и *B* повторяют этот цикл *t* раз при разных случайных значениях *r* и *b* до тех пор, пока *B* не убедится, что *A* знает значение *S*.

Если сторона *A* не знает значения *S*, она может выбрать такое значение *r*, которое позволит ей обмануть сторону *B*, если *B* отправит ей $b = 0$, либо *A* может выбрать такое *r*, которое позволит обмануть *B*, если *B* отправит ей $b = 1$. Но этого невозможно сделать в обоих случаях. Вероятность того, что *A* обманет *B* в одном цикле, составляет 1/2. Вероятность обмануть *B* в *t* циклах равна $(1/2)^t$.

Для того чтобы этот протокол работал, сторона *A* никогда не должна повторно использовать значение *r*. Если *A* поступила бы таким образом, а сторона *B* отправила бы стороне *A* на шаге 2 другой случайный бит *b*, то *B* имела бы оба ответа *A*. После этого *B* может вычислить значение *S*, и для *A* все закончено.

Содержание заданий

Разработайте программу, имитирующую функционирование упрощенной схемы идентификации с нулевой передачей данных.

Значения необходимых параметров должны выбираться случайным образом.

Выходная информация должна быть следующей:

Значение n;

Открытый ключ;

Секретный ключ;

Процесс идентификации

Сторона A;

Сторона B;

Сторона A;

Сторона B;

…

П р и м е ч а н и я

1. Модуль n определяется как произведение двузначных чисел p и q.
2. Сравнение $x^2 = V$(**mod** n) равнозначно выражению x^2 **mod** $n = V$.
3. Сравнение $z = V^{-1}$(**mod** n) равнозначно выражению $z \bullet V$ **mod** $n = 1$.

Контрольные вопросы

1. Что такое идентификация пользователей и для чего она нужна?
2. Какая рекомендуемая длина модуля?
3. Сколько итераций алгоритма нужно провести для уверенности в подлинности пользователя?

Отчетность по лабораторной работе

Подготовить отчет с кодом программы с подробными его комментариями и результатами выполнения программы.

ЛАБОРАТОРНАЯ РАБОТА 6

ПАРАЛЛЕЛЬНАЯ СХЕМА ПРОТОКОЛА ИНТЕНСИФИКАЦИИ С НУЛЕВОЙ ПЕРЕДАЧЕЙ ДАННЫХ

Цель работы: формирование умений проверки подлинности удаленных пользователей с помощью параллельной схемы протокола идентификации с нулевой передачей данных.

Теоретические сведения

Параллельная схема идентификации позволяет увеличить число аккредитаций, выполняемых за один цикл, и тем самым уменьшить длительность процесса идентификации.

Сначала генерируется число n как произведение двух больших чисел. Для того, чтобы сгенерировать открытый и секретный ключи для стороны *A*, сначала выбирают *K* различных чисел $V_1, V_2, ..., V_K$, где каждое V_i является квадратичным вычетом по модулю *n*. Иначе говоря, выбирают значение *Vi* таким, что сравнение $x^2 = V_i$ **mod** *n* имеет решение, и существует число V^{-1}_i **mod** *n*. Полученная строка $V_1, V_2, ..., V_K$ является открытым ключом.

Затем вычисляют такие наименьшие значения *Si*, что

$Si = \sqrt{(V^{-1}_i)}$(**mod** *n*).

Эта строка $S_1, S_2, ..., S_K$ является секретным ключом стороны *A*.

Протокол процесса идентификации имеет следующий вид:

1. Сторона *A* выбирает некоторое случайное число *r*, $r < n$.

Затем она вычисляет $x = r^2$ **mod** *n* и посылает *x* стороне *B*.

2. Сторона *B* отправляет стороне *A* некоторую случайную двоичную строку из *K* бит: $b_1, b_2, ..., b_K$.

3. Сторона *A* вычисляет

$y = r(S_1^{b_1} \times S_2^{b_2} \times ... \times S_K^{b_K})$ **mod** *n*.

Перемножаются только те значения *Si*, для которых $b_1 = 1$. Например, если $b_1 = 1$, то сомножитель *S* входит в произведение, если же $b_1 = 0$, то S_1 не входит в произведение, и т. д. Вычисленное значение y отправляется стороне *B*.

4. Сторона *B* проверяет, что

$x = y(V_1^{b_1} \times V_2^{b_2} \times ... \times V_K^{b_K})$**mod** *n*.

Фактически сторона *B* перемножает только те значения *Vi*, для которых *bi* = 1. Стороны *A* и *B* повторяют этот протокол *t* раз, пока *B* не убедится, что *A* знает S_l, S_2, ..., S_K.

Вероятность того, что *A* может обмануть *B*, равна $(1/2)^{Kt}$. Рекомендуется в качестве контрольного значения брать вероятность обмана *B* равной $(1/2)^{20}$ при $K = 5$ и $t = 4$.

Содержание заданий

Разработайте программу, имитирующую функционирование параллельной схемы идентификации с нулевой передачей данных.

Значения необходимых параметров должны выбираться случайным образом.

Выходная информация должна быть следующей:

Значение n;

Открытые ключи;

Секретные ключи;

Процесс идентификации

Сторона A;

Сторона B;

Сторона A;

Сторона B.

Контрольные вопросы

1. Что такое идентификация пользователей и для чего она нужна?

2. В чем отличие протокола идентификации с нулевой передачей знания и параллельной схемы протокола идентификации с нулевой передачей знания?

3. Какая вероятность того, что одному из пользователей удастся обмануть другого?

Отчетность по лабораторной работе

Подготовить отчет с кодом программы с подробными его комментариями и результатами выполнения программы.