Лабораторная работа №1. Протоколы с нулевым разглашением.

1. Общие положения

Доказа́тельство с нулево́ым разглаше́нием (информа́ции) (англ. *Zero-knowledge proof*) — интерактивный вероятностный протокол, который позволяет доказать, что доказываемое утверждение верно, и Доказывающий знает это доказательство, в то же время не предоставляя никакой информации о самом доказательстве данного утверждения. Протокол должен обладать тремя свойствами:

- **Полнота**: если утверждение действительно верно, то Доказывающий убедит в этом Проверяющего с любой наперед заданной точностью;
- **Корректность**: если утверждение неверно, то любой, даже «нечестный», Доказывающий не сможет убедить Проверяющего за исключением пренебрежимо малой вероятности;
- **Нулевое разглашение**: если утверждение верно, то любой, даже «нечестный», Проверяющий не узнает ничего кроме самого факта, что утверждение верно.

В данной лабораторной работе рассматриваются два протокола с нулевым разглашением: протокол Фиата-Шамира и протокол Шнорра.

2. Примеры протоколов с нулевым разглашением

2.1. Протокол Фиата-Шамира

Протокол Фиата-Шамира – один из наиболее известных протоколов доказательства с нулевым разглашением, основанный на проблеме извлечения квадратного корня по модулю большого составного n.

Предварительный этап:

1. Доверенный центр T выбирает и публикует модуль схемы - число n, являющееся произведением двух больших простых чисел p и q.

2. Пользователь выбирает секретное S из интервала (1, n-1), взаимно простое с n. Затем вычисляется открытый ключ $V = s^2 (mod\ n)$. Значение V регистрируется доверенным центром в качестве открытого ключа пользователя, а число S является его закрытым ключом.

Рабочий этап:

1. A выбирает случайно r из интервала (1, n-1) и отсылает B значение $x = r^2 (mod\ n)$;
2. B случайно выбирает бит e (0 или 1) и отсылает его A.
3. A вычисляет $y = r * v^e (mod\ n)$ и отправляет его обратно к B.

4. Сторона B проверяет равенство $y^2 = x * v^e (mod\ n)$. Если оно верно, раунд считается завершенным корректно и осуществляется переход к следующему раунду. В противном случае доказательство не принимается.

Таким образом протокол состоит из этапа подготовки (достаточно осуществить один раз для каждого пользователя) и этапа доказательства, состоящего из t раундов.

В каждом раунде пользователь, не обладающий знанием секрета может угадать ответ с вероятностью ½. Для t раундов таким образом вероятность обмана составит 2^{-t}.

2.2. Протокол Гиллу-Кискатра

Протокол Гиллу-Кискатра является расширением **протокола Фиата-Шамира** и в сравнении с ним имеет меньшее число сообщений, которыми необходимо поменяться сторонам, и более низкие требования к памяти, используемой для хранения секретов пользователей.

Предварительный этап:

1. Доверенный центр T выбирает и публикует модуль схемы - число n, являющееся произведением двух больших простых чисел p и q.
2. T определяет и делает доступным для всех пользователей v, где v-открытая экспонента ($v > 2, \text{НОД}(v, \varphi(n)) = 1$), s – закрытая экспонента ($s = v^{-1}(mod\ \varphi(n))$;
3. Каждый участник A получает уникальный идентификатор, на основании которого по известной функции f вычисляется значение $J_A = f(I_A)$;
4. T возвращает участнику A секретное значение $s_A = {J_A}^{-s} (mod\ n)$.

Рабочий этап:

1. Участник A выбирает случайное секретное число r (0<r<n), вычисляет $x = r^v (mod\ n)$ и отправляет B пару чисел (I_A, x);
2. B генерирует случайное целое число e (0<e<(n+1)) и отправляет его участнику A;
3. A вычисляет и передаёт B $y = r * s_A^e (mod\ n)$;
4. B получает y, из I_A, используя функцию f получает $J_A = f(I_A)$, вычисляет $z = J_A^e * y^v (mod\ n)$ и принимает доказательство участника A, если z=x и z!=0.

2.3. Протокол Шнорра

Протокол Шнорра – протокол доказательства с нулевым разглашением, стойкость которого базируется на проблеме дискретного логарифмирования.

Этап 1: Выбор параметров протокола

1. Выбирается два простых числа p и q, причём q|(p-1).
2. Выбирается число t ($2^t < q$), являющееся параметром безопасности.
3. Выбирается элемент g, лежащий в пределах (1, p-1) и имеющий порядок q.
4. Каждая сторона протокола получает копию системных параметров (g,p,q), а также открытый ключ доверенного центра T, который позволяет проверить подпись сообщения m.

Этап 2: Выработка параметров пользователя

1. Каждая сторона протокола A получает уникальный идентификатор I_A;
2. Сторона A выбирает приватный ключ a (лежащий в пределах (1, q-1)) и вычисляет $v = g^{-a}(mod\ p)$;
3. Сторона A передаёт v доверенному центру T и получает сертификат $cert_A = \left(I_A, v, S_r(I_A, v)\right)$, который связывает v и I_A.

Этап 3: Доказательство

1. Доказывающая сторона A случайным образом выбирает число r (0<r<q), вычисляет $x = g^r(mod\ p)$ и отправляет проверяющей стороне B $(cert_A, x)$;
2. Сторона B делает вывод об аутентичности открытого ключа v доказывающей стороны A путём проверки подписи доверенного центра, после чего отправляет A случайное ранее не использовавшееся число e, $1 \leq e \leq 2^t$;
3. Сторона A проверяет $1 \leq e \leq 2^t$ и передаёт B $y = ae + r\ (mod\ q)$;
4. B вычисляет $z = g^y \cdot v^e (mod\ p)$ и принимает доказательство, если z=x.

3. Задания

3.1. Реализация протокола Фиата-Шамира

Целью данного задания является реализация протокола доказательства с нулевым разглашением Фиата-Шамира. В интерфейсе приложения должны быть наглядно представлены:

- Исходные данные протокола (модули, ключи, секретные данные и т.п.);
- Данные, передаваемые по сети каждой из сторон;
- Проверки, выполняемые каждым из участников.

Процесс взаимодействия между сторонами протокола может быть реализован как с применением сетевых технологий, так и при помощи буферных переменных. Также необходимо выделить каждый из этапов протоколов для того, чтобы его можно было отделить от остальных.

3.2. Реализация протокола Гиллу-Кискатра

Используя исходный код, полученный в процессе выполнения задания 5.1, необходимо создать реализацию протокола Гиллу-Кискатра, являющего модификацией протокола Фиата-Шамира. В интерфейсе приложения должны быть наглядно представлены:

- Исходные данные протокола (модули, ключи, секретные данные и т.п.);
- Данные, передаваемые по сети каждой из сторон;
- Проверки, выполняемые каждым из участников.

Процесс взаимодействия между сторонами протокола может быть реализован как с применением сетевых технологий, так и при помощи буферных переменных. Также необходимо выделить каждый из этапов протоколов для того, чтобы его можно было отделить от остальных.

3.3. Реализация протокола Шнорра

Целью данного задания является реализация протокола доказательства с нулевым разглашением Шнорра. В интерфейсе приложения должны быть наглядно представлены:

- Исходные данные протокола (модули, ключи, секретные данные и т.п.);
- Данные, передаваемые по сети каждой из сторон;
- Проверки, выполняемые каждым из участников.

Процесс взаимодействия между сторонами протокола может быть реализован как с применением сетевых технологий, так и при помощи буферных переменных. Также необходимо выделить каждый из этапов протоколов для того, чтобы его можно было отделить от остальных.