Задание выполнил Улитин Иван Владимирович, 531 группа

Протокол Диффи-Хеллмана

Работу алгоритма можно описать следующим образом. Предположим, существует два абонента: Алиса и Боб. Обоим абонентам известны некоторые два числа g и p, которые не являются секретными и могут быть известны также другим заинтересованным лицам. При этом g - первообразный корень по модулю p. Для того, чтобы создать неизвестный более никому секретный ключ, оба абонента генерируют большие случайные числа: Алиса — число a, Боб — число b. Затем Алиса вычисляет остаток от деления:

$$A = g^a \bmod p$$

и пересылает его Бобу, а Боб вычисляет остаток от деления

$$B = g^b \bmod p.$$

и передаёт Алисе. Предполагается, что злоумышленник может получить оба этих значения, но не модифицировать их (то есть, у него нет возможности вмешаться в процесс передачи).

На втором этапе Алиса на основе имеющегося у неё a и полученного по сети B вычисляет значение:

$$B^a \bmod p = g^{ab} \bmod p$$

Боб на основе имеющегося у него b и полученного по сети A вычисляет значение:

$$A^b \bmod p = g^{ab} \bmod p$$

Как нетрудно видеть, у Алисы и Боба получилось одно и то же число:

$$K = g^{ab} \bmod p$$

Особенности программной реализации

При запуске программы предлагается выбрать одну из опций: "сгенерировать g и p", "сгенерировать a и b", "вычислить K для Алисы", "вычислить K для Боба".

1. При выборе опции "сгенерировать g и p" нужно ввести длину простого числа p в битах, которое будет затем генерироваться. На его основе будет находится

некоторый примитивный корень g. После этого данная пара чисел (g, p) будет сохранена в файл `public_key.txt`.

2. При выборе "сгенерировать a и b" программа потребует ввести сначала длину степени a в битах, а затем длину степени b в битах. Затем, после генерации B и A будет произведено сохранение параметра A в файл `alice_remainder.txt`, параметра a в файл `alice_private_key.txt`, параметра B в файл `bob_remainder.txt`, параметра b в файл `bob_private_key.txt`.
3. При выборе "вычислить K для Алисы" будет производиться считывание данных из файлов `public_key.txt`, `bob_remainder.txt` и `alice_private_key.txt`, после которых осуществляться вычисление Алисой числа $K = B^a \bmod p$.
4. При выборе "вычислить K для Боба" будет производиться считывание данных из файлов `public_key.txt`, `alice_remainder.txt` и `bob_private_key.txt`, после которых осуществляться вычисление Бобом числа $K = A^b \bmod p$.