Реализация протокола обмена ключами Диффи-Хеллмана

Если рассматривать стойкость симметричного и асимметричного шифрования, то при одинаковой длине ключа сравнение будет не в пользу последних. Более того, для ассиметричного шифрования требуется времени на порядки больше, чем симметричных. Однако для эффективного симметричного шифрования необходимо произвести обмен секретными ключами между участниками. Наиболее популярным алгоритмом обмена ключами является алгоритм Диффи-Хеллмана.

Этот алгоритм, предложенный в 1976 г., стал первым в истории алгоритмом с открытым ключом. Алгоритм, как и алгоритм Эль-Гамаля, основан на проблеме дискретного логарифмирования в конечных абелевых группах.

Задание: создать приложение на языке C++/C#, моделирующее обмен секретными ключами между двумя участниками по алгоритму Диффи-Хеллмана.

Алгоритм.

1. Один из участников (A или B) генерирует простое число n типа *unsigned int* в интервале от 0 до $2^{32}-1$. Для генерации простого числа использовать вероятностный тест Ферма.
2. Тот же участник вычисляет первообразный корень g по модулю n. Для вычисления g использовать алгоритм, описанный в лекциях. Для факторизации значения функции Эйлера $\varphi(n)$, необходимой в алгоритме, использовать метод перебора делителей, либо метод факторизации Ферма.
3. Числа n и g передаются по открытому каналу другому участнику.
4. Участник A генерирует случайное число x типа *unsigned int* в интервале от 0 до $2^{32}-1$.
5. Участник A вычисляет значение $X = g^x \pmod n$ и отправляет результат по открытому каналу участнику B.
6. Участник B генерирует случайное число y типа *unsigned int* в интервале от 0 до $2^{32}-1$.
7. Участник B вычисляет значение $Y = g^y \pmod n$ и отправляет результат по открытому каналу участнику A.
8. Участник A вычисляет секретный ключ по формуле $k = Y^x \pmod n$
9. Участник B вычисляет секретный ключ по формуле $k' = X^y \pmod n$

Для реализации возведения в степень по модулю использовать рекурсивный алгоритм.

Критерий корректности работы программы – равенство получившихся ключей: $k = k' = g^{xy} \pmod n$.

Замечания по реализации

Моделирование обмена данными по открытому каналу предлагается реализовать следующим образом. Запускаются два экземпляра приложения, один из которых соответствует участнику A, второй – участнику B. В каждом приложении должны быть

кнопки «Отправить данные» и «Принять данные». По нажатию кнопки «Отправить данные» данные, подлежащие отправке, сохраняются в текстовый или бинарный файл. По нажатию кнопки «Принять данные» необходимые для работы числа считываются из файла.

Пример алгоритма передачи модуля n и основания g:

1. В приложении 1 числа n и g генерируются согласно алгоритму и отображаются в текстовых полях.
2. По нажатию кнопки «Отправить данные» в приложении 1 числа записываются в текстовый или бинарный файл.
3. По нажатию кнопки «Принять данные» в приложении 2 числа n и g считываются из файла.
4. Числа n и g отображаются в текстовых полях приложения 2.

Приложение должно содержать 5 текстовых полей, в которых отображаются следующие числа в десятичном формате:

- Модуль системы n
- Основание системы g
- Выбранное число x для участника A, y - для участника B
- Принятое число Y для участника A, X - для участника B
- Вычисленный ключ