УДК 004.056.55

Особенности реализации алгоритма шифрования данных Диффи-Хеллмана в среде программирования Delphi

Прохорова Наталья Юрьевна
Приамурский государственный университет имени Шолом-Алейхема
Студент

Глаголев Владимир Александрович
Приамурский государственный университет имени Шолом-Алейхема
к.г.н. доцент кафедры информационных систем, математики и методик обучения

Аннотация
Данная статья посвящена разработке клиентского приложения, позволяющего обмениваться текстовыми сообщениями по защищенному каналу. Безопасность передачи данных строиться на алгоритме Диффи-Хеллмана, который позволяет двум сторонам получить общий секретный ключ, используя незащищенный от прослушивания, но защищённый от подмены канала связи. Этот ключ может быть использован для шифрования дальнейшего обмена с помощью алгоритма симметричного шифрования.
Ключевые слова: Криптография, алгоритм Диффи-Хеллмана, секретный ключ, шифрование сообщений, защищенный канал.

The particular implementation of the encryption algorithm Diffie-Hellman data in the programming environment Delphi

Prokhorova Natalya Yurievna
Sholom-Aleichem Priamursky State University
Student

Glagolev Vladimir Alexandrovich
Sholom-Aleichem Priamursky State University
Candidate of Geographical Sciences, Assistant Professor of the Department of Information Systems, Mathematics and teaching methods

Abstract
This article is devoted to the development of a client application that allows you to exchange text messages over a secure channel. The security of data transmission is based on the Diffie-Hellman algorithm, which allows two parties to obtain a common secret key, using unprotected from listening, but protected from the substitution of the communication channel. This key can be used to encrypt further exchange using the symmetric encryption algorithm.
Keywords: Cryptography, Diffie-Hellman algorithm, secret key, message encryption, secure channel.

Криптография - это наука о том, как обеспечить секретность сообщения. Она покрывает все практические аспекты секретного обмена сообщениями, становится одним из основных инструментов, обеспечивающих конфиденциальность, доверие, авторизацию, электронные платежи, корпоративную безопасность и бесчисленное множество других важных вещей.

Цель исследования заключается в создании программы с помощью инструментария среды Delphi, реализующей алгоритм шифрования данных Диффи-Хеллмана.

Задачей является разработка приложения, соответствующих интерфейсных форм для указания различных вариантов шифрования указанным методом.

Для разработки информационной системы была использована объектно-визуальная среда программирования RAD Studio Delphi 2010, предназначенная для быстрой разработки приложений под платформу Microsoft Windows. С её помощью можно создавать высокопроизводительные приложения для самой популярной платформы в мире, используя быстрое компилирование и высокоэффективную интегрированную среду разработки (IDE), и не прибегая к runtime-модулям для созданных приложений.

Сетевое взаимодействие обеспечивается двумя компонентами: TClientSocket и TServerSocket. Первый используется для подключения к удаленному приложению и передачи данных, а второй контролирует прием данных.

Опишем алгоритм Диффи-Хеллмана. Предположим, что обоим абонентам известны некоторые два числа g и p, которые не являются секретными и могут быть известны также другим заинтересованным лицам. Для того, чтобы создать неизвестный никому секретный ключ, оба пользователя генерируют большие случайные числа: первый абонент — число a, второй абонент — число b. Затем первый пользователь вычисляет значение $A = g^a \bmod p$ и пересылает его второму, а второй вычисляет $B = g^b \bmod p$ и передаёт первому (рис. 1).

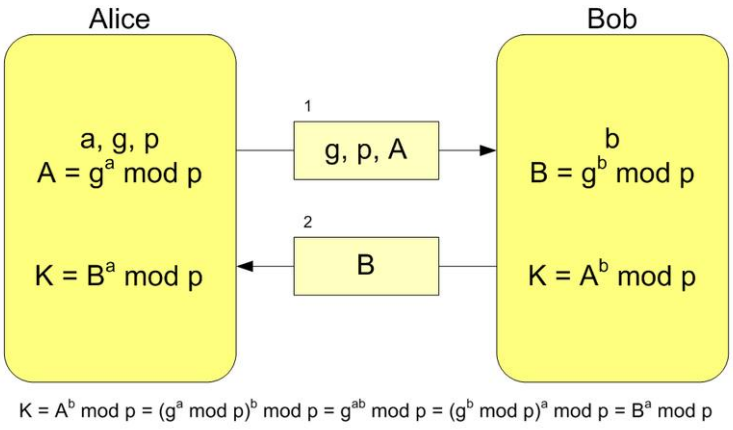


Рисунок. 1. – Схема алгоритма

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, первый пользователь на основе имеющегося у него числа a и полученного по сети числа B вычисляет значение $B^a \bmod p = g^{ab} \bmod p$, а второй пользователь на основе имеющегося у него числа b и полученного по сети числа A вычисляет значение $A^b \bmod p = g^{ab} \bmod p$. Тем самым, у обоих пользователей получилось одно и то же число: $K = g^{ab} \bmod p$. Его они и могут использовать в качестве секретного ключа, поскольку здесь злоумышленник встретится с практически неразрешимой (в течение некоторого времени) проблемой вычисления - $g^{ab} \bmod p$ по перехваченным $g^a \bmod p$ и $g^b \bmod p$, если числа p,a,b выбраны достаточно большими.

При запуске программы появляется главное окно приложения (рис. 2). Состоящее из меню, двух диалоговых окон для отображение обычного и зашифрованного текста, поля ввода сообщения и четырех кнопок.

Рисунок 2 – Главная форма приложения

Команда меню главного окна «Файл-Настройка» вызывает окно (рис. 3), в котором указываются параметры подключения и защиты передачи данных. Вводиться имя пользователя, порт прослушивания и подключения, адреса подключения и ключи сеанса.

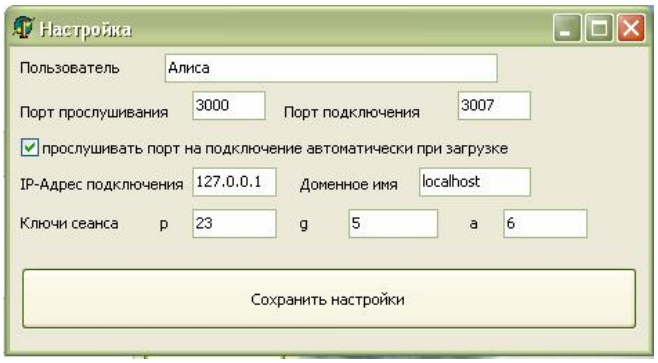
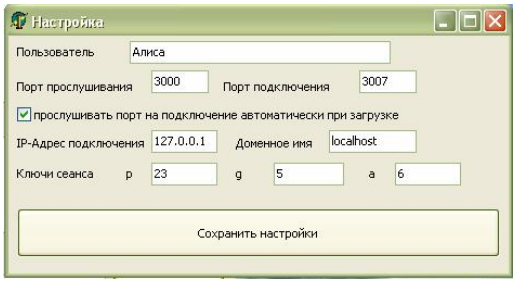


Рисунок 3 – Окно «Настройка»

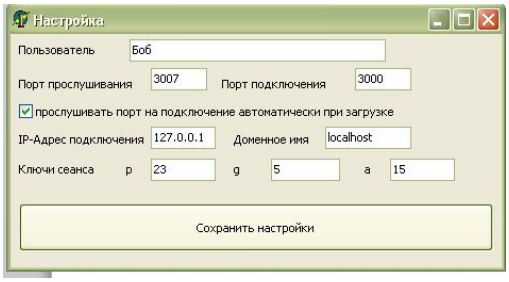
Команда меню «Безопасность – Шифровать канал» отправляет открытый ключ другому пользователю и производит шифрование сообщений. Ниже представлен пример шифрования, вверху зашифрованный текст, а внизу расшифрованный (рис. 4).

Рисунок 4 – Шифрование сообщений

Рассмотрим пример подключения двух пользователей (рис. 5). В начале необходимо сконфигурировать два клиента следующим образом.



a) Настройка клиента «Алиса»



b) Настройка клиента «Боб»

Рисунок 5 – Настройка двух клиентов

Затем каждый пользователь нажимает кнопку «Подключение». После успешного подключения, можно печатать и отправлять текст (рис. 6).

a) Отправка сообщения от Алисы

b) Отправка сообщения от Боба

Рисунок 6 – Отправка сообщений двух клиентов

Пользователи могут выбрать защищенный канал нажав в меню пункт «Безопасность-Шифровать канал», тогда каждый из пользователей получает одинаковый сеансовый ключ, например, 2. В приложение в строке статуса появляется сообщение об использование ключа (рис. 7).

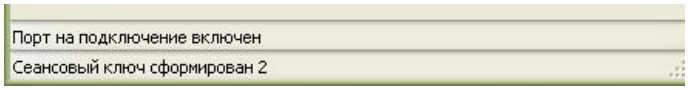


Рисунок 7 – Строка состояния

После этого происходит шифрование сообщений. Пользователи в дальнейшем могут отменить защищенный канал или разорвать соединение. Выбор параметров для формирования сеансового ключа рассмотрены в техническом задание, ниже приведены примерные значения переменных p,g,a,b, которые можно использовать в программе (табл. 1).

Таблица 1 – Переменные алгоритма Диффи-Хеллмана

№	p	g	a	b
1	47	3	8	10
2	23	5	6	15

В ходе выполнения данного исследования была выполнена поставленная цель – разработано приложение, реализующее защищенный канал передачи данных. Проведен вариант эксплуатации, разработанного приложения, позволяющего организовывать защищенный канал связи на основе сеансового ключа с использованием симметричных алгоритмов.

Библиографический список

1. Сергиенко А.Б. Цифровая обработка сигналов: Учеб. пос. для вузов. СПб.: Питер, 2002. 608 с.
2. Теория информации и кодирования/ Б.Б. Самсонов, Е.М. Плохое, А.И. Филоненко и др. Ростов н/Д: Феникс, 2002. 288 с.
3. Молдовян А.А. Криптография / А.А. Молдовян, Н.А. Молдовян, Б.Я. Советов. СПб.: Лань, 2001.
4. Архангельский А.Я. и др. Русская справка (HELP) no Delphi 5 и Object Pascal/ А.Я. Архангельский, В.Н. Ильин, М.А. Тагин: М.: БИНОМ, 2000. 32 с.
5. Мельников В.В. Безопасность информации в автоматизированных системах. М.: Финансы и статистика, 2003. 368 с.
6. Степанов Е.А., Корнеев И.К. Информационная безопасность и защита информации: Учеб. пос. М.: ИФРА, 2001. 304 с.
7. Соколов А.В., Степанюк О.М. Методы информационной защиты объектов и компьютерных сетей .М.: АСТ; СПб: Полигон, 2000. 272 с.