ПРИМЕНЕНИЕ БЕЗОПАСНОЙ ПЕРЕДАЧИ ДАННЫХ В ДИСТАНЦИОННОМ ОБУЧЕНИИ

В.Н. Зинькевич

Белорусский государственный университет информатики и радиоэлектроники, Минск, Беларусь, zislava@yandex.ru

Abstract. Remote learning means interaction between teacher and student mostly via network technology. Various learning materials are presented in the form of files. Cryptography helps to address security and authorship issues in organization of data transfer through public Internet channel. This article concerns secure files exchange and access to them after.

Различные цифровые материалы, например, литературные источники, исходные коды лабораторных заданий, тестовые данные для проверки корректности выполнения работы, отчеты и прочее передаются в обе стороны по открытому каналу сети Интернет, что означает отсутствие гарантии авторства источника данных, а также того, что данные были не модифицированы в ходе передачи.

С одной стороны, может казаться, что в вопросе образования нет необходимости обеспечивать секретность передаваемой информации, ведь никакой опасности при раскрытии или получении файлов лабораторной работы или литературных источников нет, в отличие от передачи экономических данных, секретных переписок и т.д. Однако существуют ситуации, когда литературные источники представляют собой ценные материалы, которые по условиям соглашения, не могут поставляться третьим лицам. То же касается различных данных по заданиям, тестовых материалов и другой интеллектуальной собственности. Гарантия авторства источника данных кроме достоверности, что общение происходит именно с тем человеком, может быть использована и для других целей.

При получении результатов работы студента в виде файла, данные могут быть подписаны уникальным цифровым ключом [1]. Таким образом можно гарантировать, что именно студент был адресантом данного файла, с зафиксированным временем подписания и отправки. В случае каких-либо вопросов по содержимому, его авторству, каким-либо разночтениям данная подпись подтверждает, что ответственным является конкретный студент/преподаватель. Таким образом исключается возможность ситуации, известной как «отказ от ответственности» [1]. Дополнительным достоинством является автоматическая проверка модификации данных после подписания. Из этого следует, что подменить данные после подписания любой из сторон будет невозможно.

Однако цифровая подпись не гарантирует секретности подписанных данных и не может предотвратить лиц получение доступа к информации несанкционированных лиц.

Одним из недостатков прямого взаимодействия преподавателя и студента по сети является необходимость обоих присутствовать в процессе общения, будь то простой обмен сообщениями либо передача заданий. Проблема общения может быть решена средствами электронной почты, однако пересылку файлов не всегда удобно делать почтой. Некоторые сервисы накладывают достаточно строгие ограничения на объем файлов, доступ к ним не всегда удобный и необходимо помнить в каких письмах какие файлы были приложены и хранить всю переписку. Простым, удобным и нетребовательным решением может быть использование папки с общим доступом, например, на одной из машин университета. Уязвимостью в этом случае, однако, как раз и является возможность общего доступа любого студента/преподавателя к этим папкам. Настраивать различные права и уровни доступа к разным иерархиям для

разных студентов может быть достаточно долго, неудобно и неэффективно. Возможным решением в этом случае может выступить шифрование хранимых данных общим для преподавателя и студента ключом. Получение этого ключа на основе уникальных секретных ключей студентов и преподавателя выполнять с помощью алгоритма распределения криптографических ключей Диффи-Хеллмана [2]. Общая схема работы алгоритма представлена на рисунке 1. Значения параметров:

a,b – секретные числа Алисы и Боба соответственно;

g,p – некоторые заранее выбранные, необязательно секретные, известные и Алисе, и Бобу числа.

A,B – вычисляемые значения, на основе которых каждая из сторон получает общее значение секретного ключа K.

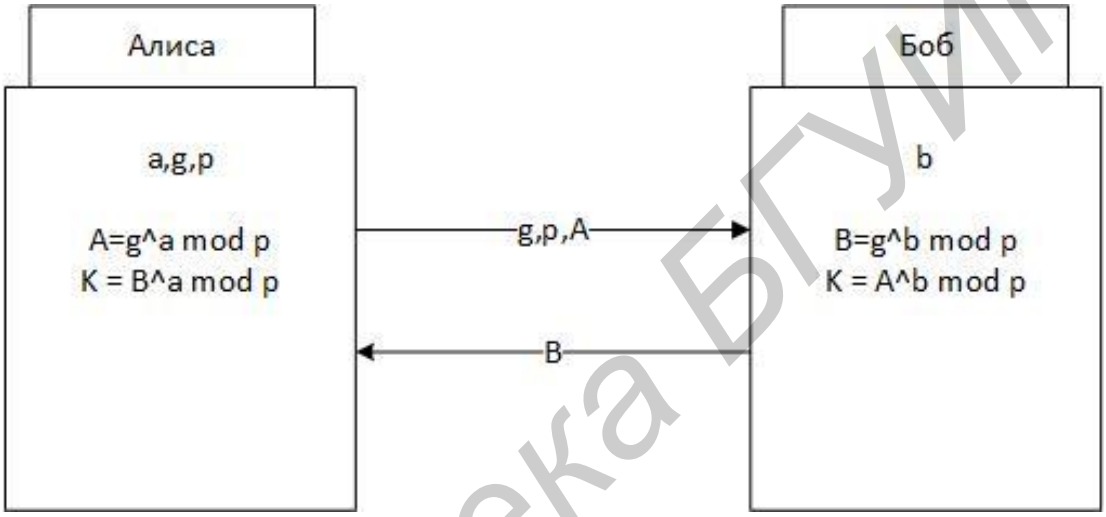

Рисунок 1 – Общая схема распределения ключей Диффи-Хеллмана

На данный момент существует ряд готовых решений, способных помочь при реализации описанного процесса без необходимости внедрять криптографические алгоритмы вручную. Примерами таких решений являются протоколы SFtp и Ftps, которые позволяют осуществлять безопасную и проверяемую передачу файлов в удаленное хранилище. Однако вопрос конечного шифрования переданных файлов для ограничения доступа посторонних лиц они не затрагивают.

Таким образом применение криптографических решений может существенно помочь при осуществлении дистанционного обучения, влияя не только на сохранность и доступность данных, но также на общее поведение участников процесса и удобство осуществление этого процесса.

Литература

1. Ярмолик, В. Н. Теория информации: методическое пособие для студентов специальности I – 40 01 01 «Программное обеспечение информационных технологий» дневной и дистанционной форм обучения / В. Н. Ярмолик. – Мн.: БГУИР, 2004. – 118 с.: ил.

2. Stallings, W. Cryptography and Network Security Principles and Practices, Fourth Edition / W. Stallings. – Prentice Hall, Ca, 2005.