Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Основы защиты информации

Практическое задание №7

«Криптографическая защита информации»

Подготовил: студент ФИТ 2 курса 5 группы Древотень Е.В.

Проверил: асс. Берников В.О.

Цель: изучить и закрепить умение реализации ЭЦП на примере RSA.

Задание на выполнение

Оба участника имеют открытый и закрытый ключи по алгоритму RSA.

Первый пользователь сначала шифрует сообщение своей закрытой экспонентой – подписывает сообщение: .

После этого он шифрует своё подписанное сообщение при помощи открытой экспоненты второго пользователя: .

Итоговое зашифрованное подписанное сообщение передаётся второму пользователю.

Второй пользователь сначала использует для расшифровки свою закрытую экспоненту: .

Для получения исходного сообщения и проверки подписи используется открытая экспонента первого пользователя: .

Электронная цифровая подпись – реквизит электронного документа, предназначенный для защиты данного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа ЭЦП и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.

Специальные схемы:

* схема "конфиденциальной" (неотвергаемой) подписи – подпись не может быть проверена без участия сгенерировавшего ее лица;
* схема подписи "вслепую" ("затемненной" подписи) – отправитель не знает подписанного им сообщения;
* схема "мультиподписи" – вместо одного отправителя сообщение подписывает группа из нескольких участников;
* схема "групповой" подписи – получатель может проверить, что подписанное сообщение пришло от члена некоторой группы отправителей, но не знает, кем именно из членов группы оно подписано. В тоже время, в случае необходимости, отправитель может быть определен.

Вывод: изучил и закрепил умение реализации ЭЦП на примере RSA.