МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«МИРЭА – Российский технологический университет»

РТУ МИРЭА

Задание по практике

Методы обеспечения целостности информации

(наименование дисциплины (модуля) в соответствии с учебным планом)

Уровень: бакалавриат
(бакалавриат, магистратура, специалитет)

Форма обучения: очная
(очная, очно-заочная, заочная)

Направление подготовки: 09.03.02 «Информационные системы и технологии»
(код(-ы) и наименование(-я))

Институт: Кибербезопасности и цифровых технологий (ИКБ)
(полное и краткое наименование)

Кафедра: «Разработка программных решений и системное программирование»
(полное и краткое наименование кафедры, реализующей дисциплину (модуль))

Лектор: к.т.н. Ермакова Алла Юрьевна
(сокращенно – ученая степень, ученое звание; полностью – ФИО)

Используются в данной редакции с учебного года 2023/24
(учебный год цифрами)

Проверено и согласовано «____» _____2023_г. _____ _____
(подпись директора Института/Филиала с расшифровкой)

Москва 2023 г.

Практическая работа 5.

Разработка криптографического протокола ЭЦП.

Цель работы: изучение способа построения и разработка криптографического протокола.

Протокол – совокупность правил, регламентирующих последовательность шагов, предпринимаемых двумя или большим количеством сторон для совместного решения некоторой задачи, а также регламентирующих форматы сообщений, пересылаемых между участниками обмена, и действия при возникновении сбоев.

Наиболее распространенными криптографическими протоколами являются:

- протоколы электронной подписи: RSA, DSA, DSS, Эль-Гамаля, ГОСТ-34.10-94, ГОСТ-34.10-2001, ГОСТ-34.10-2012.

- протоколы контроля целостности;

- протоколы электронных платежей.

Задание

Задание расписано на примере реализации протокола электронной подписи.

Реализовать на любом машинном языке (написать программу):

1. Процедуру генерации простых чисел. Результат должен вводится в окне программы.
2. Алгоритм проверки чисел на простоту. Результат должен вводится в окне программы. Проверку осуществить 2-3 тестами.
3. Алгоритм генерации ключей. Переслать участникам переписки (обмена) ключи для шифрования исходного документа и ключи для подписания документа. Исходный текст для шифрования должен вводится в окне программы.
4. Алгоритм зашифрования исходного сообщения и подписания его на секретном ключе. Зашифрованный текст должен выводится в окне программы.
5. Процедуру пересылки подписанного и зашифрованного сообщения получателю. Зашифрованный текс с подписью должен выводится в окне программы.

6. Алгоритм проверки правильности ЭЦП. Восстановленный исходный текс сообщения выводится в окне программы.
7. Сохранить в отчете экранные формы демонстрирующие: процесс генерации простых чисел и их проверку на простоту, процесс генерации и распространения ключей, процесс шифрования исходного документа и постановки ЭЦП, процесс восстановления исходного документа и проверки правильности ЭЦП, выводится в окне программы.
8. Вызывать любые встроенные библиотеки запрещено!!!

Под окном программы следует понимать пользовательский интерфейс.

Протоколы обмена ключами

Для передачи секретной информации по открытым каналам связи абонентам необходимо иметь ключи. Либо единый ключ в случае использования симметричного шифрования, либо пару ключей для каждого абонента при асимметричном шифровании. Использование одного и того же ключа при многократном общении между абонентами позволяет противнику накопить богатый материал для криптоанализа. Поэтому в целях повышения безопасности обмена секретной информации широко используются сеансовые ключи. **Сеансовый (сессионный) ключ** – ключ, используемый абонентами в рамках одного сеанса (сессии, раунда) общения. Более того, в некоторых криптосистемах предусматривается многократная смена ключа в рамках одного сеанса, временные метки[1], некоторая дополнительная информация, усиливающие безопасность криптосистемы. Использование сеансовых ключей позволяет решить также и вторую проблему - ограничить размер ущерба при компрометации ключа.

Возможны следующие разновидности протоколов обмена ключами **в зависимости от стороны, вырабатывающей сеансовый ключ**:

- ключ вырабатывается одним из абонентов и высылается второму для последующего информационного обмена;

- совместная выработка ключа абонентами;

- ключ вырабатывается и предоставляется абонентам третьей стороной (доверенным центром).

Кроме этого, обмен ключами может выполняться как с помощью симметричного, так и асимметричного шифрования.

Вызывать встроенные библиотеки запрещается.

Алгоритм генерации простых чисел и тесты проверки чисел на простоту разрабатывается самостоятельно. Тестов проверки чисел на простоту должно быть минимум два.

Реализация простейших алгоритмов: шифрования и генерации общего секретного ключа оценивается как «удовлетворительно».