Лабораторная работа №1
СТБ 34.101.45

Дедлайн: 08.10.2024

1 Введение

В данной лабораторной работе вам необходимо программно реализовать криптографические алгоритмы из СТБ 34.101.45 для уровня стойкости $l = 128$. Дополнительную информацию об этой криптосистеме вы можете получить в стандарте, лекции а также в книгах по криптографии.

2 Условие лабораторной работы

Основные алгоритмы

Обязательно должны быть реализованы:

1. алгоритм задания параметров (p, a, b, q) эллиптической кривой (минимум один из списка):
   - *(2 балла)* стандартные параметры (СТБ 34.101.45, приложение Б);
   - *(2 балла)* собственные параметры;
2. *(2 балла)* алгоритм вычисления базовой точки эллиптической кривой (СТБ 34.101.45, п. 6.1.3, шаг 8);
3. алгоритм вычисления кратной точки (минимум один из списка):
   - *(2 балла)* бинарный метод (лекция, п. 36.1);
   - *(8 баллов)* с использованием якобиановых координат (лекция, п. 36.5);
   - *(12 баллов)* с использованием кривой Эдвардса (лекция, п. 36.5);
   - *(4 балла)* с использованием аддитивных цепочек (лекция, п. 36.6);
   - *(6 баллов)* с использованием оконного метода (лекция, п. 36.7);

- *(6 баллов)* с использованием метода скользящего окна (лекция, п. 36.7);
- *(6 баллов)* с использованием NAF (лекция, п. 36.9);

4. *(2 балла)* алгоритм генерации пары ключей (СТБ 34.101.45, п. 6.2.2);
5. *(2 балла)* алгоритм проверки открытого ключа (СТБ 34.101.45, п. 6.2.3).

Вспомогательные алгоритмы

Дополнительно могут быть реализованы:

1. *(12 баллов)* алгоритм генерации параметров эллиптической кривой (СТБ 34.101.45, п. 6.1.3);
2. *(6 баллов)* алгоритм проверки параметров эллиптической кривой (СТБ 34.101.45, п. 6.1.4);
3. *(10 баллов)* алгоритм генерации одноразового личного ключа (СТБ 34.101.45, п. 6.3.3);
4. *(6 баллов)* алгоритм выработки электронной цифровой подписи (СТБ 34.101.45, п. 7.1.3);
5. *(6 баллов)* алгоритм проверки электронной цифровой подписи (СТБ 34.101.45, п. 7.1.4).

Алгоритмы из СТБ 34.101.31

При реализации некоторых приведенных выше алгоритмов вам понадобятся алгоритмы из СТБ 34.101.31. Вы можете как реализовать их самостоятельно, так и воспользоваться готовой библиотекой, которую можно взять здесь. За самостоятельную реализацию соответствующих функции можно получить следующие баллы:

1. *(8 баллов)* belt-block: зашифрование блока (СТБ 34.101.31, п. 6.1.3);
2. *(12 баллов)* belt-hash: хэширование (СТБ 34.101.31, п. 7.8.3).

Особенности реализации лабораторной работы

- Под реализацией следует понимать программу, написанную на одном из языков программирования: C, C++, C#, Java, Python, Go.
- Если существует возможность задания собственных параметров эллиптической кривой, то они обязательно должны быть проверены по алгоритму проверки параметров эллиптической кривой (СТБ 34.101.45, п. 6.1.4).
- В алгоритме проверки электронной цифровой подписи (СТБ 34.101.45, п. 7.1.4) можно использовать трюк Шамира (лекция, п. 36.10), что принесет дополнительные 4 балла.
- Помимо указанных алгоритмов, в реализации должен присутствовать функционал, демонстрирующий работоспособность каждого из реализованных алгоритмов, другими словами необходимо написать тесты, которые покрывают весь ваш исходный код.
- Реализация должна иметь проверку корректности входных данных для всех алгоритмов (см. требования к входным данным в СТБ 34.101.45).
- Допускается использование любого стандартного источника случайности, который присутствует в выбранном языке программирования.

3 Порядок сдачи лабораторной работы

- Вам необходимо создать архив формата «.zip», название которого должно иметь вид «Ivanov_1.zip», где «Ivanov» – ваша фамилия латинскими буквами. В архиве должен быть исходный код вашей реализации.
- Не позже, чем за 24 часа до сдачи лабораторной работы преподавателю, вы должны отправить архив по одному из контактов, указанных в ответе на вопрос №3 в файле «FAQ.pdf».