### Министерство науки и высшего образования Российской Федерации

1. Санкт-Петербургский политехнический университет Петра Великого
2. —
3. Институт компьютерных наук и кибербезопасности
4. Высшая школа кибербезопасности

**ЛАБОРАТОРНАЯ РАБОТА № 6**

1. **«Протокол электронной цифровой подписи**
2. **ГОСТ P 34.10–2018»**
3. по дисциплине «Криптографические методы защиты информации»
4. Выполнил
5. студент гр. 5151001/00201 Устюгов А. А.

<*подпись*>

1. Проверил:
2. старший преподаватель, к.т.н. Тулинова А. В.

<*подпись*>

1. Санкт-Петербург
2. 2024

# Цель работы

Изучение протокола электронной цифровой подписи ГОСТ Р 34.10–2018, безопасность которого основана на задаче дискретного логарифмирования в группе точек эллиптической кривой.

# Порядок выполнения работы

Разработать программу П-1, реализующую протокол подписи согласно ГОСТ Р 34.10–2018. Параметры криптосистемы соответствуют варианту задания и приведены в Приложении Д. Программа должна поддерживать функции формирования и проверки подписи, а также допускать возможность использования различных ключей.

# Ход работы

В соответствии с вариантом были получены следующие параметры криптосистемы:

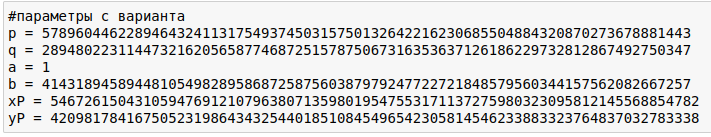


Рисунок 1 – параметры криптосистемы

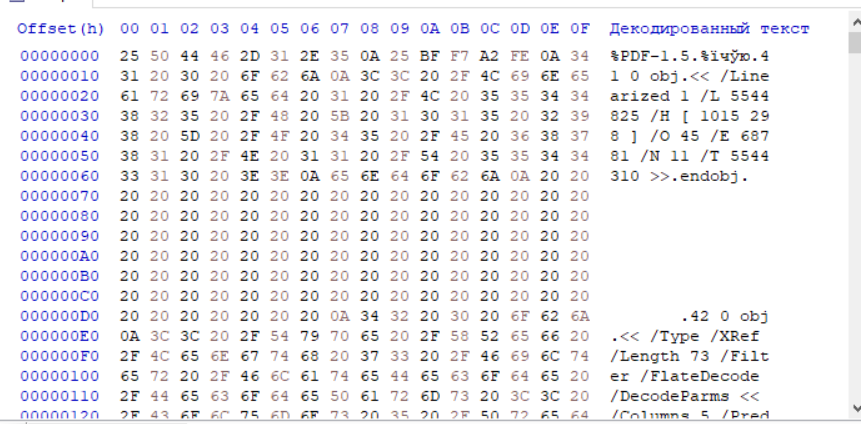


Рисунок 2 – подписываемый файл

В качестве функции хэширования используется отечественный стандарт ГОСТ Р 34.11–2012, «Стрибог».

Полученное содержимое файла подписи в соответствии с форматом ASN.1:

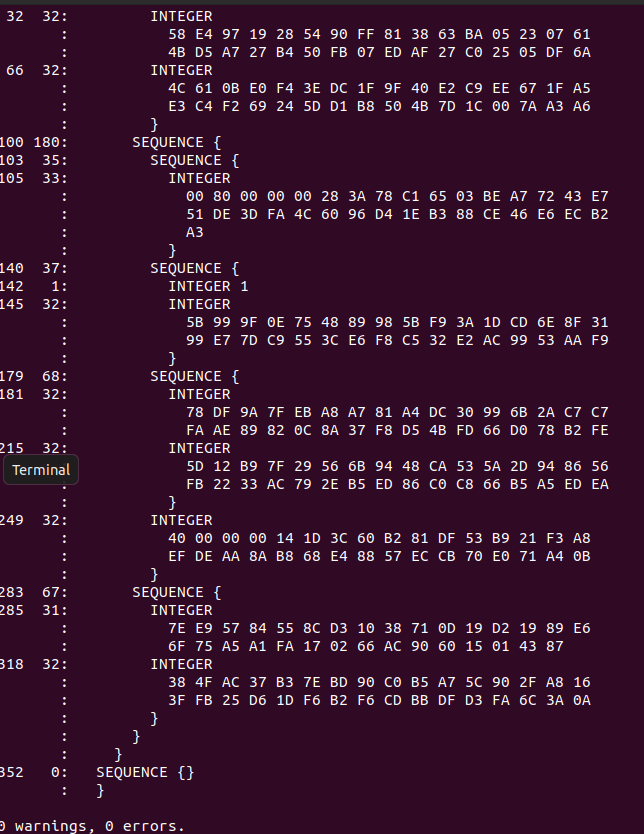


Рисунок 3 – файл подписи

# Ответы на контрольные вопросы

**1. Перечислите преимущества криптосистем на эллиптических**

**кривых по сравнению с другими криптосистемами.**

На сегодняшний момент задача дискретного логарифмирования для эллиптических кривых считается «сложнее» по сравнению с другими схожими задачами, используемыми в криптографии. Шифрование на основе эллиптических кривых обеспечивает тот же уровень безопасность при меньшей длине ключа, что делает ее более эффективной с точки зрения требований к вычислениям и пропускной способности.

**2. Почему в стандарте ГОСТ Р 34.10–2018 введено требование**

**#𝐸(𝔽𝑝) ≠ 𝑝?**

Обратим внимание на требование к делителю порядку группы

где m = #𝐸(𝔽𝑝)

Таким образом если число m = p, где p – простое число. То выбор q будет однозначным q = p. При выполнении этого равенства группа точек порядка q становится изоморфной аддитивной группе поля 𝔽𝑝, где изоморфизм вычисляется с помощью логарифмической производной.

Таким образом, задачу дискретного логарифмирования на кривых сводится к задаче дискретного логарифмирования в конечном поле, для решения которой существуют более эффективные алгоритмы.

**3. Если нарушитель имеет возможность обращать хэш-функцию, как он может подделать сообщение и подпись?**

Возможность обращать хэш-функцию создает серьезную уязвимость для системы цифровой подписи, так как злоумышленник может осуществлять атаку на основе поиска коллизий для двух сообщений. Если два сообщения имеют одинаковый хэш, то можно использовать оригинальную подпись для фальшивого сообщения или же наоборот, использовать фальшивую подпись для оригинального сообщения.

**4. Почему случайный показатель 𝑘 не должен повторяться в течение времени жизни ключа?**

Пусть k повторяется. Тогда для двух разных сообщений и одном k получается:

, откуда спокойно находится k, а зная k, восстанавливается закрытый ключ.

# Вывод

В данной лабораторной работе был реализован протокол цифровой подписи в соответствии с отечественным стандартом ГОСТ P 34.10–2018. Исследованы особенности задачи дискретного логарифмирования на эллиптических кривых.