1. Спецкурс, полугодовой: **Еллиптические кривые в алгоритмах**.

2. Преподаватель: с.н.с. Р.Р.Айдагулов.

3. Аннотация курса: Еллиптические кривые в форме Вейрштрасса, сложение точек на кривой, ранг, дискриминант и j-инвариант эллиптической кривой, диофантовые уравнения, приводящие к нахождению рациональных точек на эллиптической кривой, порядок эллиптической кривой над полем $Z\_{p}$, базовый алгоритм ECM, методы Шенкса-Местре, Шуфа и Аткина-Морейна, тесты на простоту, доказательство простоты при помощи эллиптических кривых, факторизация с использованием эллиптических кривых.

4. Тематическое содержание курса:

|  |  |
| --- | --- |
| **Тема 1.** | Основы теории эллиптических кривых. Арифметика эллиптических кривых. ТеоремыХассе, Дойринга и Ленстры. |
| **Тема 2.** | Диофантовые задачи, приводящие к нахождению рациональных точек на эллиптической кривой.. |
| **Тема 3.** | Эллиптические кривые над конечными полями и их порядок. Базовый алгоритм ECM.  |
| **Тема 4.** | Подсчет числа точек на эллиптической кривой. Методы Шенкса-Местре, Шуфа и Аткина-Морейна  |
| **Тема 5.** | Тесты на простоту Гольдвассер-Килиана и Аткина-Морейна.  |
| **Тема 6.** | Быстрое доказательство простоты при помощи эллиптических кривых.  |
| **Тема 7.** | Факторизация больших чисел при помощи эллиптических кривых. |

5. Типовые контрольные задания или иные материалы, необходимые для оценки результатов обучения, характеризующих этапы формирования компетенций.

Эллиптические кривые.

Приведение к форме Вейрштрасса.

Сложение на эллиптической кривой.

ТеоремыХассе, Дойринга и Ленстры.

Диофантовые задачи, приводящие к нахождению рациональных точек на кривой.

Эллиптические кривые над конечным полем и их порядок.

Базовый алгоритм ЕСМ.

Методы подсчета числа точек на эллиптической кривой.

Тесты на простоту.

Доказательства простоты.

Алгоритм факторизации.

Примеры задач для самостоятельного решения.

1. Вычислить количество точек на кривой$y^{2}=x^{3}-x$ над $Z\_{p}$, p=17 и p=19.

2. Найти порядок эллиптической кривой $y^{2}=x^{3}-5x+3$ над $Z\_{p},$ р=23.

3. Доказать простоту числа 89 используя эллиптические кривые.

4.Разложить на множители n=1363 используя эллиптические кривые.

6. Перечень основной и дополнительной учебной литературы:

А. Основная литература

 1. Р. Крендал, К. Померанс. Простые числа. Криптографические и вычислительные аспекты.

 2. Henry Cohen. Number Theory/ Volume 1, Volume 11.

Б. Дополнительная литература

 3. Henry Cohen and / Handbook of Elliptic and Hyperelliptic curve Cryptography.

 4. А.А. Болотов, С.Б. Гашков, А.Б. Фролов. Элементарное введение в эллиптическую криптографию.

 5. А.А. Болотов, С.Б. Гашков, А.Б. Фролов. Протоколы криптографии на эллиптических кривых.

**Программа утверждена на заседании кафедры теоретической информатики**

**Протокол №**