1. Спецкурс, полугодовой: **Основные алгоритмы в алгебре и теории чисел**.

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

3. Аннотация курса: мастер теорема, сортировка слиянием, алгоритм Евклида, модулярная арифметика, примеры использования мультимодулярных вычислений, умножение больших чисел, использование преобразования Фурье для умножения больших чисел, бигрупповая алгебра и умножение больших матриц, криптография RSA, тесты на простоту, алгоритм AKS, экспоненциальные и субэкспоненциальные методы факторизации больших чисел.

4. Тематическое содержание курса:

|  |  |
| --- | --- |
| **Тема 1.** | Эффективность алгоритмов. О- большое нотация. Принцип разделяй и властвуй. Сортировка делением пополам и разбиением по значениям.  |
| **Тема 2.** | Китайская теорема об остатках. Алгоритм Евклида. Модулярные и мультимодулярные выяисления. Квадратные корни. |
| **Тема 3.** | Представление больших чисел и умножение по Карацуба. Фильтрованные и градуированные вычисления. Преобразование Фурье и быстрый метод умножения. Умножение матриц методом Штрассена. |
| **Тема 4.** | Групповая и бигрупповая алгебра и изоморфизм последних с алгеброй матриц. Быстрое умножение больших матриц. |
| **Тема 5.** | Основы криптографии RSA. Максимальный порядок в группе Эйлера, Числа и функция Кармайкла. Тесты на простоту Ферма, Эйлера и Рабина-Миллера.  |
| **Тема 6.** | Псевдопростые числа Фибоначчи и Люка. Тест Фробениуса. |
| **Тема 7.** | n-1 и n+1 методы доказательства простоты. Критерии простоты чисел Мерсена и чисел Ферма. |
| **Тема 8.** | Полиномиальный алгоритм AKS, доказывающий простоту или составность большого числа. |
| **Тема 9.** | Экспоненциальные методы факторизации. |
| **Тема 10.** | Метод квадратичного решета в задаче факторизации. |
| **Тема 11.** | Методы числового поля NFS. |

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

О- большое нотация.

Сравнение эффективности разных алгоритмов.

Мастер теорема.

Алгоритмы сортировки.

Китайская теорема об остатках.

Алгоритм Евклида.

Модулярные и мультимодулярные вычисления.

Вычисление произведения больших чисел и матриц.

Криптография RSA.

Тесты на простоту.

Доказательства простоты.

Экспоненциальные алгоритмы факторизации.

Субэкспоненциальные алгоритмы факторизации.

Примеры задач для самостоятельного решения.

1. Сравнить эффективность алгоритмов сортировки слиянием и ранжированием.

2. Сравнить эффективность мультимодулярного вычисления последовательным вычислением остатков и методом бинарного дерева.

3. Найти минимальную мультипликативную образующую по модулю 41.

3.Найти минимальную пару натуральных чисел a,b, удовлетворяющую уравнению 89a-46b=1.

4. Найти x, удовлетворяющую соотношению $x^{2}=17 mod 256\*43$.

5. Разложить на множители 10057 методом Лемана.

6. Разложить на множители 5207 ро методом.

6. Перечень основной и дополнительной учебной литературы:

А. Основная литература

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

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

Б. Дополнительная литература

 3. П. Ноден, К. Китте. Алгебраическая алгоритмика», Москва, «Мир», 1999 г.

 4. Р. Грэхем, Д. Кнут, О. Паташник. «Конкретная математика.» Москва, «Мир», 1998.

5. С. Дасгупта, Х. Пападимитриу, У. Вазирани. «Алгоритмы». Москва, Изд-во МЦНМО, 2014 г.

**Программа утверждена на заседании кафедры теоретической информатики**

**Протокол №**