ПРОГРАММА КУРСА ЛЕКЦИЙ
"Теоретико - числовые алгоритмы"
для специализации "Математические методы защиты информации"
(годовой)

1. Арифметическая сложность алгоритмов. Алгоритм Евклида, оценка его сложности (теорема Ламе). Квадратичные сравнения. Малая теорема Ферма. Символ Лежандра и его свойства. Вычисление символа Лежандра. Символ Якоби. Быстрый алгоритм для вычисления символа Якоби.

2. Быстрый алгоритм возведения в степень. Вычисление членов линейных рекуррентных последовательностей.

3. Вероятностные алгоритмы. Первообразные корни и их вычисление. Алгоритм Шенкса решения квадратичных сравнений и оценка его сложности при известном квадратичном невычете. Вероятностный алгоритм нахождения квадратичных невычетов.

4. Числа Кармайкла, псевдопростые числа. Вероятностные методы отсеивания составных чисел (тесты Миллера–Рабина, Соловея – Штрассена).

5. Алгоритм Берлекэмпа для разложения многочленов на неприводимые множители над конечным полем. Сведение задачи разложения многочлена на множители к нахождению корней. Нахождение корней многочленов в полях малой характеристики. Вероятностные алгоритмы для нахождения корней многочленов в полях большой характеристики.

6. Условный алгоритм Миллера для доказательства простоты чисел. Детерминированные $n \pm 1$-методы проверки простоты чисел. Простота чисел Ферма и Мерсенна. Построение больших простых чисел.

7. Полиномиальный детерминированный алгоритм проверки чисел на простоту.

8. Алгоритм Адлемана-Ленстры-Коена доказательства простоты чисел.

9. Факторизация чисел с экспоненциальной сложностью: метод Ферма, алгоритмы Ленстры и Шермана - Лемана, ρ —метод Полларда, $p-1$ — метод Полларда, алгоритм Полларда - Штрассена.

10. Субэкспоненциальные методы факторизации. Алгоритм Диксона, дополнительные стратегии. Алгоритм Бриллхарта - Моррисона. Квадратичное решето.

11. Решето числового поля на примере факторизации числа Ферма F_9.

12. Алгоритмы дискретного логарифмирования по простому модулю: метод Гельфонда, алгоритм Поллига - Хеллмана, алгоритм Адлемана, алгоритм Копперсмитта - Одлыжко - Шреппеля.

13. Дискретное логарифмирование и решето числового поля.

14. Решетки и их свойства. L^3 - алгоритм построения приведенного базиса решетки.

15. Факторизация многочленов в $\mathbf{Z}[x_1, \ldots, x_m]$ с полиномиальной сложностью.

16. Построение совместных рациональных приближений и нахождение минимумов квадратичных форм с помощью L^3-алгоритма.