Вопросы к зачету
по дисциплине «теоретико-числовые методы в криптографии»
для специальности «Компьютерная безопасность»
составил: д.ф-м.н., профессор Рацеев Сергей Михайлович

6-й семестр

Примерный перечень вопросов к зачету

1. Сравнения произвольной степени по простому модулю.
2. Сравнения по составному модулю.
3. Степенные вычеты. Показатель числа.
4. Первообразные корни по простому модулю.
5. Первообразные корни по составному модулю.
6. Индексы (дискретные логарифмы).
7. Сравнения второй степени. Квадратичный вычет. Критерий квадратичного вычета по простому модулю.
8. Квадратичный невычет. Критерий квадратичного невычета по простому модулю.
9. Символ Лежандра и его свойства.
10. Символ Якоби и его свойства.
11. Вычисление квадратного корня. Алгоритм Тонелли-Шенкса.
12. Тест на простоту на основе малой теоремы Ферма.
13. Тест Соловея-Штрассена.
14. Тест Миллера-Рабина.
15. Методы дискретного логарифмирования. Метод Шенкса.
16. Метод исчисления порядка.
17. Основные алгоритмы факторизации экспоненциальной сложности (метод Ферма, $P-1$-метод Полларда, ро-метод Полларда, метод Шермана – Лемана, метод Шенкса).
18. Основные алгоритмы факторизации субэкспоненциальной сложности (алгоритм Диксона и дополнительные стратегии к данному алгоритму, алгоритм Бриллхарта–Моррисона, метод квадратичного решета Померанса).
19. Определение и основные свойства дискретного преобразования Фурье.
20. Алгоритм быстрого преобразования Фурье.
21. Дискретное преобразование Фурье для перемножения многочленов.
22. Алгоритм Монтгомери.