Вопросы к экзамену
по дисциплине «методы алгебраической геометрии в криптографии»
для специальности «Компьютерная безопасность»
составил: д.ф-м.н., профессор Рацеев Сергей Михайлович
10-й семестр

Примерный перечень вопросов к экзамену

1. Кольца. Мультипликативная группа кольца. Подкольца. Критерий подкольца.
2. Идеал кольца. Фактор-кольцо. Кольца вычетов.
3. Морфизмы колец. Ядро и образ гомоморфизма. Теорема о гомоморфизме колец. Кольца главных идеалов.
4. Китайская теорема об остатках для идеалов колец. Разложение кольца вычетов в прямую сумму примарных колец.
5. Поле: определение и основные свойства. Подполе. Критерий подполя. Критерий конечного подполя.
6. Простые и максимальные идеалы.
7. Поле частных.
8. Простые поля. Характеристика поля.
9. Расширение поля. Теорема о башне полей.
10. Алгебраические и трансцендентные элементы поля. Простые расширения полей. Теорема о классификации простых расширений полей.
11. Поле разложения многочлена.
12. Конечные поля. Построение конечного поля.
13. Образующие элементы конечного поля.
14. Неприводимые многочлены над конечными полями.
15. Блочный шифр «Кузнечик» из ГОСТ Р 34.12-2015.
16. Шифр AES.
17. Рюкзачная криптосистема Шора-Ривеста на основе конечных полей.
18. Построение ортогональных таблиц над конечными полями.
19. Совершенные шифры на основе ортогональных таблиц.
20. Аффинные алгебраические многообразия. Примеры алгебраических многообразий и их идеалов.
21. Неприводимые аффинные многообразия.
22. Проективная плоскость.
23. Пифагоровы тройки.
24. Эллиптические кривые: определение, общая форма Вейерштрасса эллиптической кривой.
25. Сложение точек эллиптической кривой над полем **R.**
26. Сложение точек эллиптической кривой над произвольным полем.
27. Группа точек эллиптической кривой.
28. Модификация системы Диффи-Хеллмана на эллиптических кривых.
29. Модификация протокола Шнорра на эллиптических кривых.
30. Модификация протокола Окамото на эллиптических кривых.
31. Модификация протоколов MTIна эллиптических кривых.
32. Электронная подпись ГОСТ Р 34.10-2012.
33. Электронная подпись ECDSA.