ВОПРОСЫ ЭКЗАМЕНАЦИОННЫХ БИЛЕТОВ
по курсу "Математические основы криптологии"

1. Классификация шифров: шифры простой и многозначной замены, матричные и дробные шифры, многоалфавитные шифры, шифры перестановок, гаммирования, блочные, поточные, с открытым и секретным ключом.
2. Исторические шифры: Цезаря, таблица Тритемия, шифры Виженера и Бофора, автоключ Виженера, решетка Кардано, шифр Ришелье, телеграфный шифр Вернама, роторные шифраторы («Энигма»)
3. Способы комбинирования секретных систем по К.Шеннону. Эндоморфные и идемпотентные системы. Чистые и смешанные шифры.
4. Совершенная секретность по К.Шеннону: необходимое и достаточное условие. Соотношение между количеством возможных сообщений и количеством ключей в совершенно секретной системе.
5. Ненадежность (equivocation) как мера теоретической секретности по К.Шеннону. Идеальные секретные системы.
6. Практическая секретность по К.Шеннону. Рабочие характеристики. Точка единственности. Перемешивание. Шифры типа $T_k FS_{\text{i}}$.
7. Принцип Керхоффа. Классификация криптоатак. Методы криптоанализа.
8. Алгоритм DES.
9. Режимы применения алгоритмов шифрования.
10. Программная реализация алгоритма DES на языке Си.
11. Алгоритм шифрования ГОСТ 28147-89 и его программная реализация.
12. Режимы шифрования по ГОСТ 28147-89 и их алгоритмы
13. Алгоритм шифрования Rijndael (AES)
14. Отображения множеств. Образы и прообразы. Сбалансированные отображения. Сюръекция, инъекция и биекция. Произведение отображений. Ассоциативность произведения множеств.
15. Группы, полугруппы, моноиды, подгруппы. Абелевы группы. Примеры групп.
16. Смежные классы, примеры смежных классов, индекс подгруппы, разложение группы по подгруппе, теорема Лагранжа.
17. Циклические группы и подгруппы, порядок элемента группы, образующий элемент. Теорема Эйлера.
18. Специальные функции на множестве групп: гомоморфизм, мономорфизм, эпиморфизмы, изоморфизм и автоморфизм. Примеры морфизмов.
19. Кольца. Делители нуля. Область целостности. Примеры колец. Кольца многочленов. Неприводимые многочлены. Идеал кольца. Факторкольцо.
20. Поля. Простейшие свойства полей. Примеры полей. Поле Галуа. Характеристика поля.
21. Теорема о бесконечности количества простых чисел. Генерация простых чисел. Решето Эратосфена. Плотность распределения простых чисел.
22. Числа Кармайкла. Тест Миллера-Рабина. Алгоритм AKS.
23. Дзета-функция Римана и ее свойства.
24. Свойства делимости. Критерий взаимной простоты двух чисел. НОК и НОД.
25. Свойства сравнений и вычетов.
26. Алгоритмы Эвклида для нахождения наибольшего общего делителя двух чисел и числа обратного заданному по модулю взаимно простого с ним числа.

27. Конгруэнтность. Классы вычетов. Приведенная система вычетов. Функция Эйлера доказательство ее мультипликативности.
28. Доказательство теоремы Эйлера. Малая теорема Ферма.
29. Китайская теорема об остатках.
30. Система RSA. Доказательство справедливости алгоритма RSA.
31. Первообразные (примитивные) корни по модулю натурального числа. Их свойство и существование.
32. Дискретные логарифмы. Система распределения ключей Диффи-Хеллмана.
33. Быстрый алгоритм возведения чисел в большую целую степень по модулю. Алгоритм шифрования Эль-Гамаля.
34. Лямбда-метод Полларда вычисления дискретных логарифмов.
35. Алгоритм цифровой подписи Эль-Гамаля. Доказательство справедливости алгоритма.
36. Хэш-функции: классификация, требования к хэш-функциям, подбор коллизий на основе "парадокса дня рождений", радужные таблицы.
37. Алгоритмы MD5, SHA и американский стандарт хэш-функций.
38. Алгоритм ГОСТ Р 34.11-94. Функция хэширования.
39. Алгоритм ГОСТ Р 34.11-2012. Функция хэширования.
40. Стандарты цифровой подписи DSS и ГОСТ 34.10-94 (2012).
41. Эллиптические кривые над полем действительных чисел и полем Галуа. Дискриминант кривой и условие невырожденности.
42. Группа точек эллиптической кривой, групповая операция сложения точек.
43. Теорема Хассе. Количество точек эллиптической кривой. Умножение точки на число. Дискретное логарифмирование на эллиптической кривой.
44. Алгоритм ГОСТ Р 34.10.2001. Формирование и проверка электронной подписи