Экзаменационные вопросы.
Защита информации.

1. Криптографическая стойкость
2. Классы сложности. Иерархия классов сложности
3. Тенденции развития и проблемы защиты информации
4. Шифры
5. Блочные шифры
6. Сеть (схема) Фейстеля
7. Шифр DES
8. Шифр DES — режим ECB
9. Шифр DES — режим CBC
10. Шифр DES — режим CFB
11. Шифр DES — режим OFB
12. Шифр Triple DES
13. Полиномы. Общие алгебраические структуры. Группы
14. Поля GF(2n). Полином с коэффициентами из GF(2)
15. Шифр AES
16. AES. Преобразование SubBytes
17. AES. Преобразование ShiftRow
18. AES. Преобразование MixColomn
19. AES. Преобразование AddRoundKey
20. Анализ AES
21. Режимы блочного шифрования Electronic Code Book
22. Режимы блочного шифрования Cipher Block Chaining
23. Режимы блочного шифрования Cipher Feedback Mode
24. Режимы блочного шифрования Output Feedback Mode
25. Алгоритм Евклида. Расширенный алгоритм Евклида.
26. Криптосистемы с открытым ключом (Public - key cryptosystems)
27. Односторонние функции.Ооднонаправленные хэш-функции
28. Использование асимметричных алгоритмов для шифрования
29. Цифровая подпись на основе алгоритмов с открытым ключом
30. Формирование секретных ключей с использованием асимметричных алгоритмов
31. Требования к алгоритмам шифрования с открытым ключом
32. Алгоритмы с открытым ключом
33. Алгоритм на основе задачи об укладке ранца
34. Алгоритм RSA. Генерация ключей. Зашифровывание и расшифровывание
35. Практическое использованияе алгоритма RSA
36. Шифрование, дешифрование и генерация ключей в криптосистеме Рабина
37. Безопасность криптографической системы Рабина
38. Генерация ключей, шифрование, и дешифрование в криптосистеме Эль-Гамаля
39. Инфраструктура управления открытыми ключами (Public key infrastructure)
40. Цифровые сертификаты
41. Стандарты
42. MAC