Экзам. Вопросы по «Криптографические методы защиты информации»

1. Основные методы информационной безопасности
2. Общая идея симметричного шифрования, принципы Керкхоффа
3. Моно- и много- алфавитные шифры подстановки, суть и отличия
4. Афинное шифрование, общий и частные случаи
5. Статистическая атака, тест Казиски
6. Шифр Вижинера и его криптоанализ
7. Шифры Хилла и его криптоанализ
8. Шифр Плейфеера и одноразовый блокнот
9. Роторный шифр, основные блоки шифровальной машины Энигмы и их назначение.
10. Особенности шифрования и криптостойкость шифрования на Энигма
11. Основные принципы шифра перестановки
12. Ключевые шифры перестановки, использование матриц
13. Блочные и поточные шифры принципы и отличия
14. Особенности современного блочного шифра
15. Компоненты современного блочного шифра
16. Основные типы Р-блоков
17. Основные типы S-блоков
18. Свойства операции XOR
19. Операции сдвига и замены, разбиения и объединения
20. Составной шифр, принципы рассеивания и перемешивания, раунды, смысл и назначение
21. Идея (первая) Файстеля и схема ее усовершенствования.
22. Два раунда шифрования и дешифрования шифром Файстеля
23. FSR –регистр сдвига с обратной связью, типы, назначение, структура и особенности
24. Общая структура DES, начальная и конечные перестановки
25. Раунды и функция DES
26. P- и S-блоки DES
27. Генерация ключей DES
28. Слабости DES
29. Особенности 2-х и 3-х кратного DES
30. Обшая структура AES и его разновидности
31. Данные в AES, матрица состояний
32. Общая структура раунда AES
33. Подстановки в AES
34. Перстановки в AES
35. Смешивание в AES
36. Добавление ключей в AES
37. Расширение ключей в AES-128
38. Общие принципы ассиметричного шифрования и отличия от симметричного шифрования
39. Ранцевая криптосистема, генерация ключей, шифрование, дешифрование и лазейка
40. Криптосистема RSA, идея процедур, шифрование/дешифрование и генерация ключей
41. Криптосистема Рабина, процедура, шифрование/дешифрование и генерация ключей
42. Криптосистема Эль-Гамаля, процедура, шифрование/дешифрование и генерация ключей
43. Криптосистема на методе эллиптических кривых, кривые в вещественных числах
44. Общая схема проверки целостности «сообщения»
45. Общая схема использования цифровой подписи с ключом и без ключа
46. Особенности ключей и их пименения в цифровой подписи
47. 10 распространенных правил зарубежной практики обеспечения безопасности ПО
48. Типичные уязвимости ПО
49. Стандарты тестирования безопасности ПО
50. Виды тестирования безопасности ПО см.презент. Очир Абушинова
51. Инструменты тестирования безопасности ПО
52. Этапы тестирования безопасности ПО
53. Меры по разработке безопасного ПО, реализуемые при выполнении анализа требований к ПО

Из Российского Стандарта

1. Меры по разработке безопасного ПО, реализуемые при выполнении проектирования архитектуры программы
2. Меры по разработке безопасного ПО, реализуемые при выполнении конструирования и комплексирования ПО
3. Меры по разработке безопасного ПО, реализуемые при выполнении квалификационного тестирования ПО
4. Меры по разработке безопасного ПО, реализуемые при выполнении инсталляции программы и поддержки приемки ПО
5. Меры по разработке безопасного ПО, реализуемые при выполнении при решении проблем в программном обеспечении в процессе эксплуатации
6. Меры по разработке безопасного ПО, реализуемые в процессе менеджмента документацией и конфигурацией программы