Вопросы

по дисциплине «Криптографические методы защита информации» – (2022 г)

1. Сущность проблемы информационной безопасности систем. Характеристики и параметры ИС и ИВС.
2. Характеристика угроз безопасности современным ИС и ИВС.
3. Политика безопасности современных ИС и ИВС
4. Энтропия источника сообщения. Энтропия Шеннона.
5. Энтропия источника сообщения. Энтропия Хартли.
6. Двоичный канал передачи информации.
7. Энтропия двоичного алфавита.
8. Условная энтропия. Энтропийная оценка потерь при передаче информации.
9. Базовые понятия криптографии. Основы теории больших чисел. Проблема дискретного логарифма.
10. Основная теорема арифметики. Алгоритм Евклида нахождения НОД
11. Основы модулярной арифметики. Вычеты.
12. Обратные вычисления по модулю в криптографии. Расширенный алгоритм Евклида.
13. Функция Эйлера в криптографии.
14. Хеш-функция и ее свойства. Области использования хеш-функций.
15. Общая характеристика алгоритмов хеширования классов MD и SHA.
16. Алгоритмы хеширования класса MD. Области использования.
17. Алгоритмы хеширования класса SHA. Области использования.
18. Общая классификация криптографических методов защиты информации.
19. Подстановочные шифры. Шифр Цезаря.
20. Особенности реализации шифровальной машины Энигма.
21. Шифр на основе аффинной системы подстановок Цезаря.
22. Система шифрования Цезаря с ключевым словом.
23. Шифр Виженера.
24. Перестановочные шифры.
25. Методы симметричного криптопреобразования. Стандарт DES. Общая характеристика.
26. Методы симметричного криптопреобразования. Стандарт DES. Структура одного цикла. Криптостойкость алгоритма.
27. Методы симметричного криптопреобразования. Стандарты 3DES. Реализация и криптостойкость.
28. Шифровальная машина Энигма. Устройство, функционирование, криптостойкость.
29. Сравнительная характеристика алгоритмов Lucifer, IDEA, ГОСТ 28147-89, Blowfish.
30. Криптографические системы с открытым (публичным) ключом. Задача об укладке ранца.
31. Управление криптографическими ключами. Алгоритм рукопожатия.
32. Распределение ключей на основе симметричных систем.
33. Алгоритм передачи ключа по Диффи-Хеллману.
34. Алгоритм шифрования RSA. Реализация и криптостойкость.
35. Алгоритм шифрования Эль-Гамаля. Реализация и криптостойкость.
36. Потоковое шифрование. Типы. Гаммирование в потоковом шифровании.
37. Генерация ключевой информации для потокового шифрования. Генераторы ПСП на основе регистров сдвига.
38. Особенность шифра Вернама.
39. Стеганографические методы защиты информации. Классификация и области использования. Метод наименее значащих бит.
40. Текстовая стеганография. Многоключевая модель стеганографической системы.
41. Понятие эллиптичекой кривой. Принципы построения криптосистемы на эллиптических кривых
42. Представление и описание эллиптической кривой на основе алгебраической геометрии
43. Арифметические операции в эллиптической криптографии
44. Система согласования криптографических ключей на основе эллиптической кривой
45. ЭЦП. Назначение и свойства.
46. ЭЦП. Основные методы генерации. Атаки на ЭЦП
47. ЭЦП на основе симметричной криптографии
48. ЭЦП на основе алгоритма RSA
49. ЭЦП на основе симметричной криптосистемы и посредника
50. ЭЦП DSS.
51. ЭЦП на основе алгоритма Эль-Гамаля
52. ЭЦП на основе эллиптической кривой.
53. Алгоритм К. Шнорра. Стандарт ЭЦП в РБ.
54. Протокол Kerberos.
55. Деструктивные программы. Классификация и методы нейтрализации.
56. Оценка безопасности парольной защиты.