ВОПРОСЫ
для подготовки к зачету по дисциплине
«Защита компьютерной информации»

1. Криптография: основные термины. Простейшие шифры
2. Криптоанализ. Безопасность данных
3. Криптосистемы. Требования к секретности и достоверности. Классификация криптосистем
4. Математические основы криптографии. Целые числа. Алгоритмы получения простых чисел. Составные числа
5. Математические основы криптографии. Алгоритм Евклида. Бинарный алгоритм
6. Математические основы криптографии. Сравнения. Свойства сравнений. Лемма
7. Математические основы криптографии. Алгоритм возведения в степень. Алгоритм быстрого возведения в степень
8. Математические основы криптографии. Понятие вычета. Теорема Ферма. Функция Эйлера. Теорема Эйлера
9. Математические основы криптографии. Линейные сравнения. Решение линейных сравнений
10. Математические основы криптографии. Элементы теории информации. Энтропия. Код Хаффмана
11. Математические основы криптографии. Частотный анализ. Абсолютная секретность
12. Математические основы криптографии. Одноразовый блокнот (шифратор Вермана)
13. Простейшие алгоритмы шифрования
14. Метод говорящих часов
15. Полибианский квадрат
16. Шифратор Цезаря
17. Омофонные шифраторы
18. Шифратор Виженера
19. Роторная машина
20. Устройства роторной машины. Ключи роторных машин
21. Электронный ротор. Реализация механизма вращения
22. Шифратор *LUCIFER*
23. Алгоритм *DES*. Таблица перестановки *DES*
24. Алгоритм *DES*. Функция *F* (подстановка + перестановка)
25. Алгоритм *DES*. *S*–бокс
26. Алгоритм *DES*. Вычисление ключа K_i
27. Алгоритм *DES*. Декодирование (дешифрование)
28. Алгоритм *DES*. Слабые ключи *DES*
29. Алгоритм *DES*. Модификации *DES*
30. Алгоритм шифрования данных *IDEA*. Общие сведения
31. Алгоритм шифрования данных *IDEA*. Операции над данными

32. Алгоритм шифрования данных *IDEA*. Процедура шифрования
33. Симметричный блочный шифратор *BLOWFISH*. Общие сведения. Преимущества *BLOWFISH*
34. Стандарт *AES*. Общие сведения. Основные параметры
35. Стандарт *AES*. Группы, кольца и поля. Поля Галуа
36. Стандарт *AES*. Математические операции. Умножение полиномов
37. Потоковые шифры
38. Потоковые шифры. Общая структура синхронного потокового шифратора
39. Потоковые шифры. Генераторы криптографических ключей
40. Потоковые шифры. Конгруэнтные генераторы
41. Потоковые шифры. LFSR. Характеристические полиномы LFSR
42. Потоковые шифры. Генераторы нелинейных последовательностей
43. Криптографические системы с открытым ключом. Алгоритм RSA
44. Криптостойкость алгоритма RSA
45. Электронная цифровая подпись. Функция хеширования
46. Электронная цифровая подпись. Классическая схема создания цифровой подписи
47. Алгоритм цифровой подписи RSA