По умолчанию для Криптография и криптографические протоколы (09.04.01, 2021)/ПК-30, ПК-30.1

1. **SP-сеть является комбинацией**
    a. Таблиц сдвигов и замен
    b. Задачи дискретного логарифмирования и факторизации
    c. Сети Фейстеля

    SP-сеть является комбинацией (Множественный выбор / Только один ответ)

---

2. **Акустическая атака является**
    a. Активной атакой
    b. Пассивной атакой
    c. Агрессивной атакой

    Акустическая атака является (Множественный выбор / Только один ответ)

---

3. **Алгоритм A5 является алгоритмом**
    a. Блочного шифрования
    b. Поточного шифрования
    c. Гибридной криптосистемой

    Алгоритм A5 является алгоритмом (Множественный выбор / Только один ответ)

---

4. **Алгоритм A5 является алгоритмом**
    a. Симметричного шифрования
    b. Хэш-функцией
    c. Асимметричного шифрования

    Алгоритм A5 является алгоритмом (Множественный выбор / Только один ответ)

---

5. **Алгоритм AES является алгоритмом**
    a. Блочного шифрования
    b. Поточного шифрования
    c. Гибридной криптосистемой

    Алгоритм AES является алгоритмом (Множественный выбор / Только один ответ)

---

6. **Алгоритм AES является алгоритмом**
    a. Симметричного шифрования
    b. Асимметричного шифрования
    c. Хэш-функцией

    Алгоритм AES является алгоритмом (Множественный выбор / Только один ответ)

---

7. **Алгоритм AES работает с блоками длины**

a. 64
b. 128
c. 256

Алгоритм AES работает с блоками длины (Множественный выбор / Только один ответ)

---

8. Алгоритм DES является алгоритмом

a. Блочного шифрования
b. Поточного шифрования
c. Гибридной криптосистемой

Алгоритм DES является алгоритмом (Множественный выбор / Только один ответ)

---

9. Алгоритм DES является алгоритмом

a. Симметричного шифрования
b. Асимметричного шифрования
c. Хэш-функцией

Алгоритм DES является алгоритмом (Множественный выбор / Только один ответ)

---

10. Алгоритм DES работает с блоками длины

a. 64
b. 128
c. 256

Алгоритм DES работает с блоками длины (Множественный выбор / Только один ответ)

---

11. Алгоритм MD4 работает с блоками длины

a. 128
b. 256
c. 512

Алгоритм MD4 работает с блоками длины (Множественный выбор / Только один ответ)

---

12. Алгоритм MD5 является алгоритмом

a. Симметричного шифрования
b. Хэш-функцией
c. Асимметричного шифрования

Алгоритм MD5 является алгоритмом (Множественный выбор / Только один ответ)

---

13. Алгоритм MD5 работает с блоками длины

a. 128
b. 256
c. 512

Алгоритм MD5 работает с блоками длины (Множественный выбор / Только один ответ)

---

14. Алгоритм RSA является алгоритмом

a. Симметричного шифрования
b. Асимметричного шифрования
c. Хэш-функцией

Алгоритм RSA является алгоритмом (Множественный выбор / Только один ответ)

---

15. Алгоритм RSA основывается на задаче

a. факторизации
b. Рюкзак
c. Дискретного логарифмирования

Алгоритм RSA основывается на задаче (Множественный выбор / Только один ответ)

---

16. Алгоритм SHA1 работает с блоками длины

a. 128
b. 160
c. 512

Алгоритм SHA1 работает с блоками длины (Множественный выбор / Только один ответ)

---

17. Алгоритм SHA2 работает с блоками длины

a. 128
b. 160
c. 256

Алгоритм SHA2 работает с блоками длины (Множественный выбор / Только один ответ)

---

18. Алгоритм SHA3 является алгоритмом

a. Симметричного шифрования
b. Хэш-функцией
c. Асимметричного шифрования

Алгоритм SHA3 является алгоритмом (Множественный выбор / Только один ответ)

---

19. Алгоритм ГОСТ «Кузнечик» работает с блоками длины

a. 64
b. 128
c. 256

Алгоритм ГОСТ «Кузнечик» работает с блоками длины (Множественный выбор / Только один ответ)

---

20. Алгоритм ГОСТ «Кузнечик» является алгоритмом

a. Блочного шифрования
b. Поточного шифрования
c. Гибридной криптосистемой

Алгоритм ГОСТ «Кузнечик» является алгоритмом (Множественный выбор / Только один ответ)

---

21. Алгоритм ГОСТ «Кузнечик» является алгоритмом

a. Симметричного шифрования
b. Хэш-функцией
c. Асимметричного шифрования

Алгоритм ГОСТ «Кузнечик» является алгоритмом (Множественный выбор / Только один ответ)

---

22. Алгоритмы DSA используется для

a. Постановки подписи
b. Для создания хэш-функции
c. Для шифрования

Алгоритмы DSA используется для (Множественный выбор / Только один ответ)

---

23. Алгоритмы DSA основывается на

a. Задаче факторизации
b. Задаче рюкзак
c. Задаче дискретного логарифмирования

Алгоритмы DSA основывается на (Множественный выбор / Только один ответ)

---

24. Асимметричное шифрование базируется на

a. Задачах ловушках
b. На SP сетях
c. На задаче рюкзаке

Асимметричное шифрование базируется на (Множественный выбор / Только один ответ)

---

25. Атака зондированием является

a. Активной атакой
b. Не агрессивная атака
c. Агрессивной атакой

Атака зондированием является (Множественный выбор / Только один ответ)

---

26. Атака по времени является

a. Активной атакой
b. Пассивной атакой
c. Агрессивной атакой

Атака по времени является (Множественный выбор / Только один ответ)

---

27. Атака по ошибкам вычисления является

a. Активной атакой
b. Пассивной атакой
c. Простая атака

Атака по ошибкам вычисления является (Множественный выбор / Только один ответ)

---

28. Атака по энергопотреблению является

a. Активной атакой
b. Пассивной атакой
c. Агрессивной атакой

Атака по энергопотреблению является (Множественный выбор / Только один ответ)

---

29. Атака, возможная на алгоритм MD4

a. Атака малых экспонент
b. Атака «Человек по середине»
c. Атака «Дней рождений»

Атака, возможная на алгоритм MD4 (Множественный выбор / Только один ответ)

---

30. Атака, возможная на алгоритм RSA

a. Атака малых экспонент
b. Атака «Человек по середине»
c. Атака «Дней рождений»

Атака, возможная на алгоритм RSA (Множественный выбор / Только один ответ)

---

31. Атака, возможная на алгоритм SHA1

a. Атака «Малых экспонент»
b. Атака «Человек по середине»
c. Атака «Дней рождений»

Атака, возможная на алгоритм SHA1 (Множественный выбор / Только один ответ)

---

32. Атака, возможная на алгоритм Диффи-Хэллмана

a. Атака малых экспонент
b. Атака «Человек по середине»
c. Атака «Дней рождений»

Атака, возможная на алгоритм Диффи-Хэллмана (Множественный выбор / Только один ответ)

---

33. Атаки по сторонним каналам применимы к

a. Асимметричному шифрованию
b. Симметричному шифрованию
c. Всему

Атаки по сторонним каналам применимы к (Множественный выбор / Только один ответ)

---

34. Аутентифкация используется для

a. шифрования
b. сжатия
c. проверки подлинности

Аутентифкация используется для (Множественный выбор / Только один ответ)

---

35. Блочное шифрование работает с данными

a. Без задержки в реальном времени
b. Разделяя их на блоки фиксированной длины
c. В смешанном режиме

Блочное шифрование работает с данными (Множественный выбор / Только один ответ)

---

36. В алгоритме RSA открытый ключ

a. (d, N)
b. (N, E)
c. (p, q, d)

В алгоритме RSA открытый ключ (Множественный выбор / Только один ответ)

---

37. В алгоритме RSA секретный ключ

a. (p, q, N)
b. (p, q, E)
c. (p, q, d)

В алгоритме RSA секретный ключ (Множественный выбор / Только один ответ)

---

38. В алгоритме Диффи-Хэллмана открытый ключ

a. Числа Алисы и Боба
b. Общий модуль P и открытые данные G
c. Открытые данные G

В алгоритме Диффи-Хэллмана открытый ключ (Множественный выбор / Только один ответ)

---

39. В алгоритме Диффи-Хэллмана секретный ключ

a. Числа Алисы и Боба
b. Общий модуль P
c. Открытые данные G

В алгоритме Диффи-Хэллмана секретный ключ (Множественный выбор / Только один ответ)

---

40. В алгоритме рюкзак открытый ключ

a. Сверхвозрастающая последовательность
b. Простая последовательность
c. Обе последовательности

В алгоритме рюкзак открытый ключ (Множественный выбор / Только один ответ)

---

41. В алгоритме рюкзак секретный ключ

a. Сверхвозрастающая последовательность
b. Простая последовательность
c. Обе последовательности

В алгоритме рюкзак секретный ключ (Множественный выбор / Только один ответ)

---

42. Гибридное шифрование использует для создания ключа

a. Симметричный алгоритм шифрования
b. Асимметричный алгоритм шифрования
c. Хэш-функцию

Гибридное шифрование использует для создания ключа (Множественный выбор / Только один ответ)

---

43. Гибридное шифрование использует для шифрования

a. Симметричный алгоритм шифрования
b. Асимметричный алгоритм шифрования
c. Хэш-функцию

Гибридное шифрование использует для шифрования (Множественный выбор / Только один ответ)

---

44. Задача Диффи-Хэллмана сводится к

a. Задаче факторизации
b. Задаче дискретного логарифмирования
c. Задаче рюкзак

Задача Диффи-Хэллмана сводится к (Множественный выбор / Только один ответ)

---

45. Задача ловушка дискретного логарифмирования используется в

a. RSA
b. Криптосистема Эль-Гамаль
c. AES

Задача ловушка дискретного логарифмирования используется в (Множественный выбор / Только один ответ)

---

46. Задача ловушка дискретного логарифмирования используется в

a. Криптосистеме рюкзак
b. Протоколе Диффи-Хэллмана
c. RSA

Задача ловушка дискретного логарифмирования используется в (Множественный выбор / Только один ответ)

---

47. Задача ловушка дискретного логарифмирования используется в

a. RSA
b. AES
c. Криптосистема Рабина

Задача ловушка дискретного логарифмирования используется в (Множественный выбор / Только один ответ)

---

48. Задача ловушка факторизация используется в

a. RSA
b. AES
c. DES

Задача ловушка факторизация используется в (Множественный выбор / Только один ответ)

---

49. Задача ловушка факторизация используется в

a. Криптосистеме рюкзак
b. Протоколе Диффи-Хэллмана
c. RSA

Задача ловушка факторизация используется в (Множественный выбор / Только один ответ)

---

50. Криптосистема RC4 является алгоритмом

a. Симметричного шифрования
b. Хэш-функцией
c. Асимметричного шифрования

Криптосистема RC4 является алгоритмом (Множественный выбор / Только один ответ)

---

51. Криптосистема рюкзак является алгоритмом

a. Симметричного шифрования
b. Хэш-функцией
c. Асимметричного шифрования

Криптосистема рюкзак является алгоритмом (Множественный выбор / Только один ответ)

---

52. Криптосистема Эль-Гамаль является алгоритмом

a. Симметричного шифрования
b. Хэш-функцией
c. Асимметричного шифрования

Криптосистема Эль-Гамаль является алгоритмом (Множественный выбор / Только один ответ)

---

53. Криптосистему AES можно использовать для

a. Шифрования
b. Постановки подписи
c. Шифрования и постановки подписи

Криптосистему AES можно использовать для (Множественный выбор / Только один ответ)

---

54. Криптосистему DES можно использовать для

a. Шифрования
b. Постановки подписи
c. Шифрования и постановки подписи

Криптосистему DES можно использовать для (Множественный выбор / Только один ответ)

---

55. Криптосистему RSA можно использовать для

a. Шифрования
b. Постановки подписи
c. Шифрования и постановки подписи

Криптосистему RSA можно использовать для (Множественный выбор / Только один ответ)

---

56. Криптосистему Диффи-Хэллмана можно использовать для

a. Шифрования
b. Постановки подписи
c. Создания общего ключа

Криптосистему Диффи-Хэллмана можно использовать для (Множественный выбор / Только один ответ)

---

57. Криптосистему Рабина можно использовать для

a. Шифрования
b. Постановки подписи
c. Шифрования и постановки подписи

Криптосистему Рабина можно использовать для (Множественный выбор / Только один ответ)

---

58. Криптосистему рюкзак можно использовать для

a. Шифрования
b. Постановки подписи
c. Шифрования и постановки подписи

Криптосистему рюкзак можно использовать для (Множественный выбор / Только один ответ)

---

59. Криптосистему Эль-Гамаль можно использовать для

a. Шифрования
b. Постановки подписи
c. Шифрования и постановки подписи

Криптосистему Эль-Гамаль можно использовать для (Множественный выбор / Только один ответ)

---

60. Криптосистемы асимметричного шифрования работают

a. Быстрее симметричного
b. Медленнее симметричного
c. Одинаково

Криптосистемы асимметричного шифрования работают (Множественный выбор / Только один ответ)

---

61. Криптосистемы асимметричного шифрования решают проблему

a. Коллизий
b. Передачи ключа
c. Скорости шифрования

Криптосистемы асимметричного шифрования решают проблему (Множественный выбор / Только один ответ)

---

62. Линейный криптоналаиз применим к

a. Асимметричному шифрованию
b. Симметричному шифрованию
c. К хэш-функциям

Линейный криптоналаиз применим к (Множественный выбор / Только один ответ)

---

63. Минусом симметричного шифрования является

a. Скорость
b. Затратная реализация
c. Передача ключа

Минусом симметричного шифрования является (Множественный выбор / Только один ответ)

---

64. Моноалфовитный шифр

a. Более стойкий чем полиалфовитный
b. Менее стойкий чем полиалфовитный
c. Такой же стойкий как полиалфовитный

Моноалфовитный шифр (Множественный выбор / Только один ответ)

---

65. На первом шаге создания хэш-функции используются

a. Сдвиги
b. Добавление констант
c. Переменные сцепления

На первом шаге создания хэш-функции используются (Множественный выбор / Только один ответ)

---

66. Недостаток криптосистем с открытом ключом

a. Ключ не надо передавать
b. Скорость
c. Простота

Недостаток криптосистем с открытом ключом (Множественный выбор / Только один ответ)

---

67. Недостаток криптосистем с открытом ключом

a. Ключ не надо передавать
b. Трудно внести изменения в систему
c. Простота

Недостаток криптосистем с открытом ключом (Множественный выбор / Только один ответ)

---

68. Плюсом асимметричного шифрования является

a. Решена проблема передачи ключа
b. Скорость
c. Легкая реализация

Плюсом асимметричного шифрования является (Множественный выбор / Только один ответ)

---

69. Подпись Шнорра на

a. Задаче факторизации
b. Задаче рюкзак
c. Задаче дискретного логарифмирования

Подпись Шнорра на (Множественный выбор / Только один ответ)

---

70. Поточное шифрование применяется в

a. Протоколах гибридного шифрования
b. В подписях
c. В симметричном шифровании

Поточное шифрование применяется в (Множественный выбор / Только один ответ)

---

71. Поточное шифрование применяется для

a. Передачи аудио и видео сигнала
b. В алгоритмах асимметричного шифрования
c. В банковских транзакциях

Поточное шифрование применяется для (Множественный выбор / Только один ответ)

---

72. Поточное шифрование применяется для

a. Ключ не надо передавать
b. Скорость
c. Простота

Преимущества криптосистем с открытом ключом (Множественный выбор / Только один ответ)

---

73. Преимущества криптосистем с открытом ключом

a. Безопасность относительно симметричного шифрования
b. В больших системах меньше ключей надо хранить
c. Скорость работы

Преимущества криптосистем с открытом ключом (Множественный выбор / Только один ответ)

---

74. При постановке подпись используется

a. Алгоритм Диффи-Хэллмана
b. Хэш-функция
c. Алгоритмы поточного шифрования

При постановке подпись используется (Множественный выбор / Только один ответ)

---

75. Проблемы хэш-функций в

a. Скорости
b. Наличие коллизий
c. Передачи ключа

Проблемы хэш-функций в (Множественный выбор / Только один ответ)

---

76. Самый перспективный вид криптонализа сейчас это

a. Линейный криптонализ
b. Дифференциальный криптоанализ
c. Атаки по сторонним каналам

Самый перспективный вид криптонализа сейчас это (Множественный выбор / Только один ответ)

---

77. Сеть Фейстеля делит блок

a. На три части
b. На n частей
c. На две части

Сеть Фейстеля делит блок (Множественный выбор / Только один ответ)

---

78. Симметричное блочное шифрование можно использовать для

a. Создания подписи
b. Создания хэш-функций
c. Создания общего ключа

Симметричное блочное шифрование можно использовать для (Множественный выбор / Только один ответ)

---

79. Структура Меркла-Дамгарда используется при

a. Создании подписи
b. Создании хэш-функций
c. Блочном шифровании

Структура Меркла-Дамгарда используется при (Множественный выбор / Только один ответ)

---

80. Функции ловушки используются в

a. Симметричном шифровании
b. Асимметричном шифровании
c. В поточном шифровании

Функции ловушки используются в (Множественный выбор / Только один ответ)

---

81. Хэш-функци обеспечивают

a. Сжатие данных
b. Перестановку
c. подлинность

Хэш-функци обеспечивают (Множественный выбор / Только один ответ)

---

82. Хэш-функции подвержаны

a. Коллизиям
b. Атакам малых экспонент
c. Атаке общий модуль

Хэш-функции подвержаны (Множественный выбор / Только один ответ)

---

83. Цифровая подпись обеспечивает

a. Скорость
b. Целостность сообщения
c. Простоту передачи ключа

Цифровая подпись обеспечивает (Множественный выбор / Только один ответ)

---

84. Цифровая подпись обеспечивает

a. Оригинальность сообщения
b. Отсутствие коллизий
c. Шифрование данных

Цифровая подпись обеспечивает (Множественный выбор / Только один ответ)

---

85. Цифровая подпись обеспечивает

a. Защиту от атаки «Дней Рождений»
b. Защиту от атаки «Малых экспонент»
c. Невозможность отказа от сообщения

Цифровая подпись обеспечивает (Множественный выбор / Только один ответ)

---

86. Что является самым слабым видом криптоанализа

a. Полный перебор
b. Тест Касиского
c. Частотный анализ

Что является самым слабым видом криптоанализа (Множественный выбор / Только один ответ)

---

87. Шифр Вижнера подвержен атаке

a. Полный перебор
b. Тест Касиского
c. Частотный анализ

Шифр Вижнера подвержен атаке (Множественный выбор / Только один ответ)

---

88. Шифр сдвига и замены подвержен атаке

a. Полный перебор
b. Тест Касиского
c. Частотный анализ

Шифр сдвига и замены подвержен атаке (Множественный выбор / Только один ответ)

---

89. Шифр Цезаря подвержен атаке

a. Полный перебор
b. Тест Касиского
c. Дней Рождений

Шифр Цезаря подвержен атаке (Множественный выбор / Только один ответ)

---

90. Шифр Цезаря производил

a. Перестановку
b. Сдвиг
c. Смещение

Шифр Цезаря производил (Множественный выбор / Только один ответ)

---

91. **Шифр Цезаря является**
    a. Моноалфовитным
    b. Полиалфовитным
    c. Шифром перестановки

Шифр Цезаря является (Множественный выбор / Только один ответ)

По умолчанию для Криптография и криптографические протоколы (09.04.01, 2021)/ПК-30.2

1. **P- блок является таблицей**
    a. Сдвиг
    b. Подстановка
    c. Перестановка

P- блок является таблицей (Множественный выбор / Только один ответ)

---

2. **S- блок является таблицей**
    a. Сдвиг
    b. Подстановка
    c. Перестановка

S- блок является таблицей (Множественный выбор / Только один ответ)

---

3. **Алгоритм Rijndael является**
    a. Настраиваемым шифром
    b. Поточным алгоритмом шифрования
    c. Хэш-функцией

Алгоритм Rijndael является (Множественный выбор / Только один ответ)

---

4. **Алгоритм двойного храповика используется в**
    a. Мессенджерах
    b. Гибридных криптосистемах
    c. Поточном шифровании

Алгоритм двойного храповика используется в (Множественный выбор / Только один ответ)

---

5. **Атаки по сторонним каналам основаны на**
    a. Математических уязвимостях алгоритма
    b. На физических уязвимостях реализации алгоритма
    c. На дифференциальном и линейном криптоанализе

Атаки по сторонним каналам основаны на (Множественный выбор / Только один ответ)

---

6. **Безопасность поточного шифрования обеспечивается с помощью**
    a. Роторов

b. Операции XOR
c. Генератора ключевого потока

Безопасность поточного шифрования обеспечивается с помощью (Множественный выбор / Только один ответ)

---

7. В алгоритме Rijndael операция MixColumns использует

a. Неприводимый многочлен 8 степени
b. Неприводимый многочлен 7 степени
c. Неприводимый многочлен 4 степени

В алгоритме Rijndael операция MixColumns использует (Множественный выбор / Только один ответ)

---

8. В алгоритме Rijndael операция ShiftRows обеспечивает

a. Сложение с ключом
b. Работу с колонками
c. Замену по S-блокам

В алгоритме Rijndael операция ShiftRows обеспечивает (Множественный выбор / Только один ответ)

---

9. В алгоритме Rijndael операция SubButes использует

a. Неприводимый многочлен 8 степени
b. Неприводимый многочлен 7 степени
c. Неприводимый многочлен 4 степени

В алгоритме Rijndael операция SubButes использует (Множественный выбор / Только один ответ)

---

10. В алгоритме Rijndael операция SubButes обеспечивает

a. Сложение с ключом
b. Работу с колонками
c. Замену по S-блокам

В алгоритме Rijndael операция SubButes обеспечивает (Множественный выбор / Только один ответ)

---

11. В криптографическом протоколе задействованы

a. Субъекты
b. Объекты
c. Персоны

В криптографическом протоколе задействованы (Множественный выбор / Только один ответ)

---

12. Взлом это

a. Успешная криптоатака
b. Метод криптоанализа
c. Способ криптоанализа

Взлом это (Множественный выбор / Только один ответ)

---

13. Данный алгоритм использует сеть Фейстеля

a. DSA
b. AES
c. DES

Данный алгоритм использует сеть Фейстеля (Множественный выбор / Только один ответ)

---

14. Данный алгоритм использует сеть Фейстеля

a. RSA
b. MD4
c. ГОСТ «Кузнечик»

Данный алгоритм использует сеть Фейстеля (Множественный выбор / Только один ответ)

---

15. Деление на блоки не возможно при работе с

a. Большими данными
b. Аудио и видео сигналом
c. Малыми текстами

Деление на блоки не возможно при работе с (Множественный выбор / Только один ответ)

---

16. Для обеспечения аутентификации Вы выберете алгоритм

a. SHA1
b. AES
c. DSA

Для обеспечения аутентификации Вы выберете алгоритм (Множественный выбор / Только один ответ)

---

17. Для обеспечения быстрого шифрования текста Вы выберете алгоритм

a. A5
b. 3DES
c. MD4

Для обеспечения быстрого шифрования текста Вы выберете алгоритм (Множественный выбор / Только один ответ)

---

18. Для обеспечения конфиденциальности Вы выберете алгоритм

a. SHA1
b. AES
c. DSA

Для обеспечения конфиденциальности Вы выберете алгоритм (Множественный выбор / Только один ответ)

---

19. Для обеспечения целостности Вы выберете алгоритм

a. SHA1
b. AES
c. DSA

Для обеспечения целостности Вы выберете алгоритм (Множественный выбор / Только один ответ)

---

20. Для решения проблему передачи ключа Вы выберете алгоритм

a. A5
b. RSA
c. MD4

Для решения проблему передачи ключа Вы выберете алгоритм (Множественный выбор / Только один ответ)

---

21. Если Вам необходимо использовать в системе абсолютно стойкий алгоритм шифрования Вы выберет

a. Шифр Вернама
b. Шифр Вижнера
c. Алгоритм 3DES

Если Вам необходимо использовать в системе абсолютно стойкий алгоритм шифрования Вы выберет (Множественный выбор / Только один ответ)

---

22. Какие криптографические уязвимости позволяют быстрее взломать систему

a. Математических уязвимостях алгоритма
b. Физические уязвимости в реализации алгоритма
c. Дифференциальный и линейный криптоанализ

Какие криптографические уязвимости позволяют быстрее взломать систему (Множественный выбор / Только один ответ)

---

23. Какой из алгоритмов симметричного шифрования отказался от сети Фейстеля

a. Rijndael
b. DES
c. RC4

Какой из алгоритмов симметричного шифрования отказался от сети Фейстеля (Множественный выбор / Только один ответ)

---

24. Какой из предложенных алгоритмов построен н задаче дискретного логарифмирования

a. Протокол передачи ключей Диффи-Хэллмана
b. Алгоритм Rijndael
c. Криптосистема DES

Какой из предложенных алгоритмов построен н задаче дискретного логарифмирования (Множественный выбор / Только один ответ)

---

25. Какой из режимов шифрования трансформирует блочный шифр в поточный

a. Electronic Code Book
b. Cipher Blok Chaining
c. Cipher Feed Back

Какой из режимов шифрования трансформирует блочный шифр в поточный (Множественный выбор / Только один ответ)

---

26. Какой из режимов шифрования является самым быстрым

a. Electronic Code Book
b. Cipher Blok Chaining

c. Cipher Feed Back

Какой из режимов шифрования является самым быстрым (Множественный выбор / Только один ответ)

---

27. Криптографическая подпись

a. Неподдельна
b. Может быть использована повторно
c. Не меняется при изменении сообщения

Криптографическая подпись (Множественный выбор / Только один ответ)

---

28. Криптографический протокол состоит из

a. Сеансов
b. Циклов
c. Таблиц

Криптографический протокол состоит из (Множественный выбор / Только один ответ)

---

29. Лавинный эффект обеспечивается с помощью

a. Сдвига
b. Подстановки
c. Перестановки

Лавинный эффект обеспечивается с помощью (Множественный выбор / Только один ответ)

---

30. Наименьшая длина блока у алгоритма

a. DES
b. AES
c. 3DES

Наименьшая длина блока у алгоритма (Множественный выбор / Только один ответ)

---

31. Первым алгоритм асимметричного шифрования является алгоритм

a. RSA
b. DES
c. Диффи-Хэллмана

Первым алгоритм асимметричного шифрования является алгоритм (Множественный выбор / Только один ответ)

---

32. Передача ключа может быть осуществлена с помощью

a. Протоколов с доверенным лицом
b. Блочного шифрования
c. Поточного шифрования

Передача ключа может быть осуществлена с помощью (Множественный выбор / Только один ответ)

---

33. Перестановочный шифр подвержен

a. Частотному анализу

b. Атаке с выбором открытого текста
c. Полному перебору

Перестановочный шифр подвержен (Множественный выбор / Только один ответ)

---

34. Подпись можно создать с помощью алгоритма

a. RSA
b. DES
c. Диффи-Хэллмана

Подпись можно создать с помощью алгоритма (Множественный выбор / Только один ответ)

---

35. После постановки криптографической подписи сообщение

a. Нельзя менять
b. Можно менять
c. Можно отказаться

После постановки криптографической подписи сообщение (Множественный выбор / Только один ответ)

---

36. Поточное шифрование применяется в обработке

a. Больших данных
b. Аудио и видео сигнала
c. Малых текстов

Поточное шифрование применяется в обработке (Множественный выбор / Только один ответ)

---

37. При аутентификации Вы будете использовать алгоритм

a. DSA
b. AES
c. DES

При аутентификации Вы будете использовать алгоритм (Множественный выбор / Только один ответ)

---

38. При использовании RSA для постановки подписи

a. Открытый ключ используется для подписания документа
b. Закрытый ключ используется для подписания документа
c. Оба ключа используется для постановки подписи

При использовании RSA для постановки подписи (Множественный выбор / Только один ответ)

---

39. При применении гибридной криптосистемы передачу ключа Вы будете обеспечивать с помощью

a. AES
b. MD4
c. Диффи-Хэллман

При применении гибридной криптосистемы передачу ключа Вы будете обеспечивать с помощью (Множественный выбор / Только один ответ)

---

40. При применении гибридной криптосистемы шифрование Вы будете обеспечивать с помощью

a. AES
b. MD4
c. Диффи-Хэллман

При применении гибридной криптосистемы шифрование Вы будете обеспечивать с помощью (Множественный выбор / Только один ответ)

---

41. При шифровании аудио сигнала Вы выберете алгоритм

a. A5
b. RSA
c. MD4

При шифровании аудио сигнала Вы выберете алгоритм (Множественный выбор / Только один ответ)

---

42. При шифровании аудио сигнала Вы выберете алгоритм

a. SHA1
b. RC4
c. AES

При шифровании аудио сигнала Вы выберете алгоритм (Множественный выбор / Только один ответ)

---

43. При шифровании текста Вы выберете алгоритм

a. A5
b. RSA
c. MD4

При шифровании текста Вы выберете алгоритм (Множественный выбор / Только один ответ)

---

44. При шифровании текста Вы выберете алгоритм

a. SHA1
b. RC4
c. AES

При шифровании текста Вы выберете алгоритм (Множественный выбор / Только один ответ)

---

45. Принцип Керкгофсса утверждает

a. Система должна быть в секрете
b. Система должна быть общедоступной
c. Система должна быть гибридной

Принцип Керкгофсса утверждает (Множественный выбор / Только один ответ)

---

46. Рассеивание обеспечивается с помощью

a. Сдвига
b. Подстановки
c. Перестановки

Рассеивание обеспечивается с помощью (Множественный выбор / Только один ответ)

47. Регистр сдвига с линейной обратной связью используется в

a. Блочном шифровании
b. Асимметричном шифровании
c. Поточном шифровании

Регистр сдвига с линейной обратной связью используется в (Множественный выбор / Только один ответ)

---

48. РСЛОС применяются в

a. Асимметричном шифровании
b. Блочном шифровании
c. Поточном шифровании

РСЛОС применяются в (Множественный выбор / Только один ответ)

---

49. Сеть Фейстеля используется в алгоритме

a. DES
b. AES
c. GSM

Сеть Фейстеля используется в алгоритме (Множественный выбор / Только один ответ)

---

50. Стандарт GSM использует в своей работе алгоритм

a. Блочного шифрования
b. Асимметричного шифрования
c. Поточного шифрования

Стандарт GSM использует в своей работе алгоритм (Множественный выбор / Только один ответ)

---

51. Целостность данных можно обеспечить с помощью

a. Асимметричного шифрования
b. Хэш-функции
c. Алгоритма RSA

Целостность данных можно обеспечить с помощью (Множественный выбор / Только один ответ)

---

52. Что является здесь лишним

a. Асимметричное шифрование
b. Хэш-функции
c. Алгоритм RSA

Что является здесь лишним (Множественный выбор / Только один ответ)

---

53. Что является здесь лишним

a. Асимметричное шифрование
b. Блочное шифрование
c. Поточное шифрование

Что является здесь лишним (Множественный выбор / Только один ответ)

54. Шифр Вернама производился с помощью

a. Операции XOR
b. Перестановки
c. Замены

Шифр Вернама производился с помощью (Множественный выбор / Только один ответ)

---

55. Шифр Вижнера производился с помощью

a. Операции XOR
b. Перестановки
c. Замены

Шифр Вижнера производился с помощью (Множественный выбор / Только один ответ)

---

56. Шифр Цезаря производился с помощью

a. Сдвига на 3
b. Перестановки
c. Замены

Шифр Цезаря производился с помощью (Множественный выбор / Только один ответ)

---

57. Шифром блокнот является

a. Шифр Вернама
b. Алгоритм Rijndael
c. Криптосистема DES

Шифром блокнот является (Множественный выбор / Только один ответ)

---

58. Электромеханические шифовальные устройств использую

a. Регистры сдвигов
b. Роторы
c. Таблицы замен

Электромеханические шифовальные устройств использую (Множественный выбор / Только один ответ)

---

59. ЭЦП используется для

a. Обеспечения целостности данных
b. Обеспечения аутентификации данных
c. Обеспечения конфиденциальности данных

ЭЦП используется для (Множественный выбор / Только один ответ)
