1. Подмена шифрованного сообщения предусматривает...

2. Моделирование процедуры расшифрования предусматривает …

3. Моделирование процедуры дешифрования предусматривает ...

4. Под шифром обычно понимается ...

5. Неверно, что активная атака, проводимая противником, предусматривает ...

6. Пассивная атака, проводимая противником, связана с ...

7. Важнейшим компонентом шифра является ...

8. В шифре простой замены каждому символу исходного сообщения соответствует ...

9. При скремблировании речевого сигнала изменяются ...

10. Спектром сигнала называется эквивалентный сигналу...

11. Форманта – это области спектра, ...

12. Фонема – это ...

13. Средняя продолжительность взрывного звука составляет ...

14. Средняя продолжительность фрикативного звука составляет ...

15. С увеличением полосы пропускания канала возможность голосовой идентификации ...

16. Неверно, что при искусственном формировании речевого сигнала используется такая его характеристика, как …

17. В поточных шифрах в один момент времени процедура шифрования производится над ...

18. Неверно, что к достоинствам поточных систем относится ...

19. Неверно, что к достоинствам блочных систем относятся ...

20. Зашифрованное сообщение должно поддаваться чтению ...

21. Число операций, необходимых для определения использованного ключа шифрования по фрагменту шифрованного сообщения и соответствующего ему открытого текста, должно быть ..

22. Использование симметричного криптоалгоритма использование различных ключей для шифрования и расшифрования …

23. Знание противником алгоритма шифрования ...

24. Длина шифрованного текста должна быть ...

25. При проведении словарной атаки ...

26. Элемент одноразового блокнота представляет из себя ...

27. Осмысленные открытые тексты, полученные в результате дешифрования криптограммы, сформированной с использованием одноразового блокнота ...

28. Одноразовый блокнот проверку целостности сообщения …

29. В совершенном (идеальном) шифре апостериорные вероятности открытых текстов (вычисленные после получения криптограммы)...

30. При рассмотрении практической стойкости шифров предполагается, что для рассматриваемого шифра, обычно будет существовать ...

31. Рабочая характеристика шифра – это Средний объем работы W(N), необходимый для определения …

32. Наиболее надежной считается оценка практической стойкости шифра, если количество символов ключа ...

33. Имитовставка предназначена для проверки ...

34. Содержание имитовставки должно зависеть ...

35. Противник, производя подмену или имитацию сообщения исходит из предположения, что ...

36. При моделировании активных действий противника, его обычно ставят ...

37. Мерой имитостойкости шифра является вероятность успешного …

38. Код аутентификации сообщения обеспечивает ...

39. Идеальная безопасность обеспечивается, когда длина ключа ...

40. Одноразовое шифрование наиболее приемлемо для обработки ...

41. Максимальное количество раундов шифрования по стандарту ГОСТ 28147-89 составляет ...

42. При зашифровании по стандарту шифрования ГОСТ 28147-89 полное рассеивание входных данных происходит после ...

43. В симметричной системе получатель и отправитель используют для шифрования и расшифрования сообщения ...

44. Передача симметричного ключа по незащищенным каналам в открытой форме …

45. Основой для формирования алгоритмов симметричного шифрования является предположение, что …

46. В симметричной системе шифрования для независимой работы N абонентов требуется ...

47. Неверно, что к достоинствам симметричных систем шифрования относятся ...

48. Неверно, что к недостаткам симметричных систем шифрования относятся ...

49. В асимметричной системе шифрования для независимой работы N абонентов требуется ...

50. Надежность алгоритма RSA основывается ...

51. Открытый и закрытый ключи в асимметричной системе ...

52. В асимметричной криптосистеме RSA ...

53. Достоинством асимметричных систем шифрования (по сравнению с симметричными системами) является ...

54. Недостатком асимметричных систем шифрования является ...

55. Неверно, что к недостаткам асимметричных криптосистем относится ...

56. Неверно, что к недостаткам асимметричных криптосистем относится ...

57. Ренегатство – это ...

58. Подмена – это ...

59. Повтор – это ...

60. Электронная цифровая подпись – это …

61. При формировании цифровой подписи используется ...

62. При проверке цифровой подписи используется ...

63. Алгоритмы формирования и проверки электронной цифровой подписи ...

64. Параметр q отечественного стандарта цифровой подписи ГОСТ Р 34.10-94 имеет размерность ...

65. Для первоначального распределения ключей ...

66. Результатом генерации исходной информации при предварительном распределении ключей является ...

67. Протокол Диффи-Хеллмана является протоколом...

68. Протокол Диффи-Хеллмана ...

69. Метод разделения секрета используется, в первую очередь для снижения рисков ...

70. В системе открытого распределения ключей Диффи-Хеллмана используется ...

71. Защита информации в системе Диффи-Хеллмана основана на сложности...

72. Практическая реализация алгоритма Диффи-Хеллмана ...