1. **Неверно, что к недостаткам асимметричных криптосистем относится - отсутствие математического доказательства необратимости используемых в асимметричных алгоритмах функций**
2. **Алгоритмы формирования и проверки электронной цифровой подписи**
3. **В асимметричной криптосистеме RSA**
4. **В асимметричной системе шифрования для независимой работы N абонентов требуется …**
5. **В поточных шифрах в один момент времени процедура шифрования производится над**
6. **В симметричной системе получатель и отправитель используют для шифрования и расшифрования сообщения ...**
7. **В симметричной системе шифрования для независимой работы N абонентов требуется …**
8. **В системе открытого распределения ключей Диффи-Хеллмана используется**
9. **В совершенном (идеальном) шифре апостериорные вероятности открытых текстов (вычисленные после получения криптограммы)**
10. **В шифре простой замены каждому символу исходного сообщения соответствует**
11. **Важнейшим компонентом шифра является**
12. **Длина шифрованного текста должна быть ...**
13. **Для первоначального распределения ключей ...**
14. **Достоинством асимметричных систем шифрования (по сравнению с симметричными системами) является**
15. **Зашифрованное сообщение должно поддаваться чтению**
16. **Защита информации в системе Диффи - Хеллмана основана на сложности…**
17. **Знание противником алгоритма шифрования**
18. **Идеальная безопасность обеспечивается, когда длина ключа**
19. **Имитовставка предназначена для проверки**
20. **Использование симметричного криптоалгоритма использование различных ключей для шифрования и расшифрования**
21. **Код аутентификации сообщения обеспечивает..**
22. **Максимальное количество раундов шифрования по стандарту ГОСТ 28147-89 составляет..**
23. **Мерой имитостойкости шифра является вероятность успешного**
24. **Метод разделения секрета используется, в первую очередь для снижения рисков - целостности информации**
25. **Моделирование процедуры дешифрования предусматривает**
26. **Моделирование процедуры расшифрования предусматривает**
27. **Надежность алгоритма RSA основывается**
28. **Наиболее надежной считается оценка практической стойкости шифра, если количество символов ключа**
29. **Неверно, что активная атака, проводимая противником, предусматривает**
30. **Неверно, что к достоинствам поточных систем относится**
31. **Неверно, что к достоинствам симметричных систем шифрования относятся - автоматическая аутентификация отправителя**

32. **Неверно, что к недостаткам асимметричных криптосистем относится - скорость работы - длина ключа**
33. **Неверно, что к недостаткам симметричных систем шифрования относится ...**
34. **Неверно, что при искусственном формировании речевого сигнала используется такая его характеристика, как**
35. **Неверно., что к достоинствам блочных систем относятся**
36. **Неверно.. что к достоинствам поточных систем относится .**
37. **Недостатком асимметричных систем шифрования является количество ключей, требуемых для работы в сети**
38. **Одноразовое шифрование наиболее приемлемо для обработки**
39. **Одноразовый блокнот проверку целостности сообщения**
40. **Осмысленные открытые тексты, полученные в результате дешифрования криптограммы, сформированной с использованием одноразового блокнота ...**
41. **Основой для формирования алгоритмов симметричного шифрования является предположение, что …**
42. **Открытый и закрытый ключи в асимметричной системе**
43. **Параметр q отечественного стандарта цифровой подписи ГОСТ Р 34.10-94 имеет размерность**
44. **Пассивная атака, проводимая противником, связана с**
45. **Передача симметричного ключа по незащищенным каналам в открытой форме - допускается, в зависимости от обстоятельств**
46. **Повтор - ЭТО**
47. **Под шифром обычно понимается**
48. **Подмена - это**
49. **Подмена шифрованного сообщения предусматривает...**
50. **Практическая реализация алгоритма Диффи-Хеллмана**
51. **При зашифровании по стандарту шифрования ГОСТ 28147-89 полное рассеивание входных данных происходит после**
52. **При моделировании активных действий противника, его обычно ставят**
53. **При проведении словарной атаки**
54. **При проверке цифровой подписи используется**
55. **При рассмотрении практической стойкости шпоров предполагается, что для рассматриваемого шифра, обычно будет существовать...**
56. **При скремблировании речевого сигнала изменяются**
57. **При формировании цифровой подписи используется**
58. **Противник, производя подмену или имитацию сообщения исходит из предположения, что**
59. **Протокол Диффи-Хеллмана**
60. **Протокол Диффи-Хеллмана является протоколом**
61. **Рабочая характеристика шифра**
62. **Результатом генерации исходной информации при предварительном распределении ключей является**
63. **Ренегатство – это**
64. **С увеличением полосы пропускания канала возможность голосовой идентификации**
65. **Содержание имитовставки должно зависеть**
66. **Спектром сигнала называется эквивалентный сигналу.**
67. **Средняя продолжительность взрывного звука составляет**
68. **Средняя продолжительность фрикативного звука составляет**
69. **Фонема – это**
70. **Форманта - это области спектра.**

71. **Число операций, необходимых для определения использованного ключа шифрования по фрагменту шифрованного сообщения и соответствующего ему открытого текста, должно быть..**
72. **Электронная цифровая подпись – это**
73. **Элемент одноразового блокнота представляет из себя**