



Математические методы защиты информации.э

- 1 Шифром называется ...
- 2 При использовании моноалфавитного шифра каждому символу исходного сообщения соответствует ...
- 3 В симметричной системе получатель и отправитель используют для шифрования и расшифрования сообщения ...
- 4 При использовании полиалфавитного шифра замены длина криптограммы по сравнению с исходным сообщением ...
- 5 Ключ шифра – это ...
- 6 Передача симметричного ключа по незащищенным каналам в открытой форме ...
- 7 В асимметричной системе получатель и отправитель используют для шифрования и расшифрования сообщения ...
- 8 Основой для формирования алгоритмов симметричного шифрования является предположение «...»
- 9 Концепция криптографических систем с открытым ключом основана на ...
- 10 Минимальное количество раундов шифрования, предусмотренных ГОСТ 28174-89, составляет ...
- 11 В симметричной системе шифрования для независимой работы N абонентов требуется ...
- 12 Первое из требований, выполнение которых обеспечивает безопасность асимметричной криптосистемы, гласит: «...»
- 13 Третье требования к безопасности асимметричной системы гласит: «...»
- 14 Эффект полного рассеивания входных данных при шифровании в соответствии с ГОСТ 28174-89 наступает после раундов шифрования
- 15 Неверно, что требованием к безопасности асимметричной системы является: «...»
- 16 Результатом хэш-преобразования исходного сообщения является сообщение ...





- 17) Количество итераций, выполняемых при хэшировании по ГОСТ Р 34.11-94 всегда ...
- 18) Отечественный стандарт хэширования ГОСТ Р 34.11-94 ...
- 19) Длина ключа при шифровании в соответствии с ГОСТ 29174-89 составляет ...
- 20) Если шифр соответствует установленным требованиям, знание злоумышленником алгоритма шифрования ...
- 21) Длина ключа при шифровании в соответствии со стандартом DES составляет ...
- 22) Если шифр соответствует установленным требованиям, незначительное изменение ключа ...
- 23) Если шифр соответствует установленным требованиям, длина шифрованного текста ...
- 24) В асимметричной системе шифрования для независимой работы N абонентов требуется ...
- 25) Электронная цифровая подпись – это ...
- 26) При использовании моноалфавитного шифра замены длина криптограммы по сравнению с исходным сообщением ...
- 27) Принцип действия электронной цифровой подписи основан на ...
- 28) Степень надежности криптографической системы определяется ...
- 29) Неверно, что к достоинствам симметричной системы шифрования относится ...
- 30) К недостаткам симметричной системы шифрования относятся особенности ...
- 31) К достоинствам асимметричной системы шифрования относятся особенности ...
- 32) К недостаткам асимметричной системы шифрования относится ...
- 33) При использовании полиалфавитного шифра каждому символу исходного сообщения соответствует ...
- 34) Подмена шифрованного сообщения предусматривает...
- 35) Моделирование процедуры расшифрования предусматривает ...





- 36) Моделирование процедуры дешифрования предусматривает ...
- 37) Под шифром обычно понимается ...
- 38) Неверно, что активная атака, проводимая противником, предусматривает ...
- 39) Пассивная атака, проводимая противником, связана с ...
- 40) Важнейшим компонентом шифра является ...
- 41) В шифре простой замены каждому символу исходного сообщения соответствует ...
- 42) При скремблировании речевого сигнала изменяются ...
- 43) Спектром сигнала называется эквивалентный сигналу...
- 44) Форманта – это области спектра, ...
- 45) Фонема – это ...
- 46) Средняя продолжительность взрывного звука составляет ...
- 47) Средняя продолжительность фрикативного звука составляет ...
- 48) С увеличением полосы пропускания канала возможность голосовой идентификации ...
- 49) Неверно, что при искусственном формировании речевого сигнала используется такая его характеристика, как ...
- 50) В поточных шифрах в один момент времени процедура шифрования производится над ...
- 51) Неверно, что к достоинствам поточных систем относится ...
- 52) Неверно, что к достоинствам блочных систем относятся ...
- 53) Зашифрованное сообщение должно поддаваться чтению ...
- 54) Число операций, необходимых для определения использованного ключа шифрования по фрагменту зашифрованного сообщения и соответствующего ему открытого текста, должно быть ..





- 55) Использование симметричного криптоалгоритма использование различных ключей для шифрования и расшифрования ...
- 56) Знание противником алгоритма шифрования ...
- 57) Длина шифрованного текста должна быть ...
- 58) При проведении словарной атаки ...
- 59) Элемент одноразового блокнота представляет из себя ...
- 60) Осмысленные открытые тексты, полученные в результате дешифрования криптограммы, сформированной с использованием одноразового блокнота ...
- 61) Одноразовый блокнот проверку целостности сообщения ...
- 62) В совершенном (идеальном) шифре апостериорные вероятности открытых текстов (вычисленные после получения криптограммы)...
- 63) При рассмотрении практической стойкости шифров предполагается, что для рассматриваемого шифра, обычно будет существовать ...
- 64) Рабочая характеристика шифра – это Средний объем работы $W(N)$, необходимый для определения ...
- 65) Наиболее надежной считается оценка практической стойкости шифра, если количество символов ключа ...
- 66) Имитовставка предназначена для проверки ...
- 67) Содержание имитовставки должно зависеть ...
- 68) Противник, производя подмену или имитацию сообщения исходит из предположения, что ...
- 69) При моделировании активных действий противника, его обычно ставят ...
- 70) Мерой имитостойкости шифра является вероятность успешного ...
- 71) Код аутентификации сообщения обеспечивает ...
- 72) Идеальная безопасность обеспечивается, когда длина ключа ...





- 73) Одноразовое шифрование наиболее приемлемо для обработки ...
- 74) Максимальное количество раундов шифрования по стандарту ГОСТ 28147-89 составляет ...
- 75) При зашифровании по стандарту шифрования ГОСТ 28147-89 полное рассеивание входных данных происходит после ...
- 76) В симметричной системе получатель и отправитель используют для шифрования и расшифрования сообщения ...
- 77) Основой для формирования алгоритмов симметричного шифрования является предположение, что ...
- 78) В симметричной системе шифрования для независимой работы N абонентов требуется ...
- 79) Неверно, что к достоинствам симметричных систем шифрования относятся ...
- 80) Неверно, что к недостаткам симметричных систем шифрования относятся ...
- 81) В асимметричной системе шифрования для независимой работы N абонентов требуется ...
- 82) Надежность алгоритма RSA основывается ...
- 83) Открытый и закрытый ключи в асимметричной системе ...
- 84) В асимметричной криптосистеме RSA ...
- 85) Достоинством асимметричных систем шифрования (по сравнению с симметричными системами) является ...
- 86) Недостатком асимметричных систем шифрования является ...
- 87) Неверно, что к недостаткам асимметричных криптосистем относится ...
- 88) Неверно, что к недостаткам асимметричных криптосистем относится ...
- 89) Ренегатство – это ...
- 90) Подмена – это ...
- 91) Повтор – это ...





- 92) Электронная цифровая подпись – это ...
- 93) При формировании цифровой подписи используется ...
- 94) При проверке цифровой подписи используется ...
- 95) Алгоритмы формирования и проверки электронной цифровой подписи ...
- 96) Параметр q отечественного стандарта цифровой подписи ГОСТ Р 34.10-94 имеет размерность ...
- 97) Для первоначального распределения ключей ...
- 98) Результатом генерации исходной информации при предварительном распределении ключей является ...
- 99) Протокол Диффи-Хеллмана является протоколом...
- 100) Протокол Диффи-Хеллмана ...
- 101) Метод разделения секрета используется, в первую очередь для снижения рисков ...
- 102) В системе открытого распределения ключей Диффи-Хеллмана используется ...
- 103) Защита информации в системе Диффи-Хеллмана основана на сложности...
- 104) Практическая реализация алгоритма Диффи-Хеллмана ...
- 105) Шифром называется ...
- 106) При использовании моноалфавитного шифра каждому символу исходного сообщения соответствует ...
- 107) В симметричной системе получатель и отправитель используют для шифрования и расшифрования сообщения ...
- 108) При использовании полиалфавитного шифра замены длина криптограммы по сравнению с исходным сообщением ...
- 109) Ключ шифра – это ...
- 110) Передача симметричного ключа по незащищенным каналам в открытой форме ...





- 111 В асимметричной системе получатель и отправитель используют для шифрования и расшифрования сообщения ...
- 112 Основой для формирования алгоритмов симметричного шифрования является предположение «...»
- 113 Концепция криптографических систем с открытым ключом основана на ...
- 114 Минимальное количество раундов шифрования, предусмотренных ГОСТ 28174-89, составляет ...
- 115 В симметричной системе шифрования для независимой работы N абонентов требуется ...
- 116 Первое из требований, выполнение которых обеспечивает безопасность асимметричной криптосистемы, гласит: «...»
- 117 Третье требования к безопасности асимметричной системы гласит: «...»
- 118 Эффект полного рассеивания входных данных при шифровании в соответствии с ГОСТ 28174-89 наступает после раундов шифрования
- 119 Неверно, что требованием к безопасности асимметричной системы является: «...»
- 120 Результатом хэш-преобразования исходного сообщения является сообщение ...
- 121 Количество итераций, выполняемых при хэшировании по ГОСТ Р 34.11-94 всегда ...
- 122 Отечественный стандарт хэширования ГОСТ Р 34.11-94 ...
- 123 Длина ключа при шифровании в соответствии с ГОСТ 29174-89 составляет ...
- 124 Если шифр соответствует установленным требованиям, знание злоумышленником алгоритма шифрования ...
- 125 Длина ключа при шифровании в соответствии со стандартом DES составляет ...
- 126 Если шифр соответствует установленным требованиям, незначительное изменение ключа ...
- 127 Если шифр соответствует установленным требованиям, длина шифрованного текста ...





- 128) В асимметричной системе шифрования для независимой работы N абонентов требуется ...
- 129) Электронная цифровая подпись – это ...
- 130) При использовании моноалфавитного шифра замены длина криптограммы по сравнению с исходным сообщением ...
- 131) Принцип действия электронной цифровой подписи основан на ...
- 132) Степень надежности криптографической системы определяется ...
- 133) Неверно, что к достоинствам симметричной системы шифрования относится ...
- 134) К недостаткам симметричной системы шифрования относятся особенности ...
- 135) К достоинствам асимметричной системы шифрования относятся особенности ...
- 136) К недостаткам асимметричной системы шифрования относится ...
- 137) При использовании полиалфавитного шифра каждому символу исходного сообщения соответствует ...
- 138) Шифром называется ...
- 139) При использовании моноалфавитного шифра каждому символу исходного сообщения соответствует ...
- 140) В симметричной системе получатель и отправитель используют для шифрования и расшифрования сообщения ...
- 141) При использовании полиалфавитного шифра замены длина криптограммы по сравнению с исходным сообщением ...
- 142) Ключ шифра – это ...
- 143) Передача симметричного ключа по незащищенным каналам в открытой форме ...
- 144) В асимметричной системе получатель и отправитель используют для шифрования и расшифрования сообщения ...
- 145) Основой для формирования алгоритмов симметричного шифрования является предположение «...»





- 146) Концепция криптографических систем с открытым ключом основана на ...
- 147) Минимальное количество раундов шифрования, предусмотренных ГОСТ 28174-89, составляет ...
- 148) В симметричной системе шифрования для независимой работы N абонентов требуется ...
- 149) Первое из требований, выполнение которых обеспечивает безопасность асимметричной криптосистемы, гласит: «...»
- 150) Третье требования к безопасности асимметричной системы гласит: «...»
- 151) Эффект полного рассеивания входных данных при шифровании в соответствии с ГОСТ 28174-89 наступает после раундов шифрования
- 152) Неверно, что требованием к безопасности асимметричной системы является: «...»
- 153) Результатом хэш-преобразования исходного сообщения является сообщение ...
- 154) Количество итераций, выполняемых при хэшировании по ГОСТ Р 34.11-94 всегда ...
- 155) Отечественный стандарт хэширования ГОСТ Р 34.11-94 ...
- 156) Длина ключа при шифровании в соответствии с ГОСТ 29174-89 составляет ...
- 157) Если шифр соответствует установленным требованиям, знание злоумышленником алгоритма шифрования ...
- 158) Длина ключа при шифровании в соответствии со стандартом DES составляет ...
- 159) Если шифр соответствует установленным требованиям, незначительное изменение ключа ...
- 160) Если шифр соответствует установленным требованиям, длина шифрованного текста ...
- 161) В асимметричной системе шифрования для независимой работы N абонентов требуется ...
- 162) Электронная цифровая подпись – это ...





- 163) При использовании моноалфавитного шифра замены длина криптограммы по сравнению с исходным сообщением ...
- 164) Принцип действия электронной цифровой подписи основан на ...
- 165) Степень надежности криптографической системы определяется ...
- 166) Неверно, что к достоинствам симметричной системы шифрования относится ...
- 167) К недостаткам симметричной системы шифрования относятся особенности ...
- 168) К достоинствам асимметричной системы шифрования относятся особенности ...
- 169) К недостаткам асимметричной системы шифрования относится ...
- 170) При использовании полиалфавитного шифра каждому символу исходного сообщения соответствует ...
- 171) Подмена шифрованного сообщения предусматривает...
- 172) Моделирование процедуры расшифрования предусматривает ...
- 173) Моделирование процедуры дешифрования предусматривает ...
- 174) Под шифром обычно понимается ...
- 175) Неверно, что активная атака, проводимая противником, предусматривает ...
- 176) Пассивная атака, проводимая противником, связана с ...
- 177) Важнейшим компонентом шифра является ...
- 178) В шифре простой замены каждому символу исходного сообщения соответствует ...
- 179) При скремблировании речевого сигнала изменяются ...
- 180) Спектром сигнала называется эквивалентный сигналу...
- 181) Форманта – это области спектра, ...





- 182 Фонема – это ...
- 183 Средняя продолжительность взрывного звука составляет ...
- 184 Средняя продолжительность фрикативного звука составляет ...
- 185 С увеличением полосы пропускания канала возможность голосовой идентификации ...
- 186 Неверно, что при искусственном формировании речевого сигнала используется такая его характеристика, как ...
- 187 В поточных шифрах в один момент времени процедура шифрования производится над ...
- 188 Неверно, что к достоинствам поточных систем относится ...
- 189 Неверно, что к достоинствам блочных систем относятся ...
- 190 Зашифрованное сообщение должно поддаваться чтению ...
- 191 Число операций, необходимых для определения использованного ключа шифрования по фрагменту зашифрованного сообщения и соответствующего ему открытого текста, должно быть ..
- 192 Использование симметричного криптоалгоритма использование различных ключей для шифрования и расшифрования ...
- 193 Знание противником алгоритма шифрования ...
- 194 Длина зашифрованного текста должна быть ...
- 195 При проведении словарной атаки ...
- 196 Элемент одноразового блокнота представляет из себя ...
- 197 Осмысленные открытые тексты, полученные в результате дешифрования криптограммы, сформированной с использованием одноразового блокнота ...
- 198 Одноразовый блокнот проверку целостности сообщения ...
- 199 В совершенном (идеальном) шифре апостериорные вероятности открытых текстов (вычисленные после получения криптограммы)...





- 200) При рассмотрении практической стойкости шифров предполагается, что для рассматриваемого шифра, обычно будет существовать ...
- 201) Рабочая характеристика шифра – это Средний объем работы $W(N)$, необходимый для определения ...
- 202) Наиболее надежной считается оценка практической стойкости шифра, если количество символов ключа ...
- 203) Имитовставка предназначена для проверки ...
- 204) Содержание имитовставки должно зависеть ...
- 205) Противник, производя подмену или имитацию сообщения исходит из предположения, что ...
- 206) При моделировании активных действий противника, его обычно ставят ...
- 207) Мерой имитостойкости шифра является вероятность успешного ...
- 208) Код аутентификации сообщения обеспечивает ...
- 209) Идеальная безопасность обеспечивается, когда длина ключа ...
- 210) Одноразовое шифрование наиболее приемлемо для обработки ...
- 211) Максимальное количество раундов шифрования по стандарту ГОСТ 28147-89 составляет ...
- 212) При зашифровании по стандарту шифрования ГОСТ 28147-89 полное рассеивание входных данных происходит после ...
- 213) В симметричной системе получатель и отправитель используют для шифрования и расшифрования сообщения ...
- 214) Передача симметричного ключа по незащищенным каналам в открытой форме ...
- 215) Основой для формирования алгоритмов симметричного шифрования является предположение, что ...
- 216) В симметричной системе шифрования для независимой работы N абонентов требуется ...
- 217) Неверно, что к достоинствам симметричных систем шифрования относятся ...





- 218 Неверно, что к недостаткам симметричных систем шифрования относятся ...
- 219 В асимметричной системе шифрования для независимой работы N абонентов требуется ...
- 220 Надежность алгоритма RSA основывается ...
- 221 Открытый и закрытый ключи в асимметричной системе ...
- 222 В асимметричной криптосистеме RSA ...
- 223 Достоинством асимметричных систем шифрования (по сравнению с симметричными системами) является ...
- 224 Недостатком асимметричных систем шифрования является ...
- 225 Неверно, что к недостаткам асимметричных криптосистем относится ...
- 226 Неверно, что к недостаткам асимметричных криптосистем относится ...
- 227 Ренегатство – это ...
- 228 Подмена – это ...
- 229 Повтор – это ...
- 230 Электронная цифровая подпись – это ...
- 231 При формировании цифровой подписи используется ...
- 232 При проверке цифровой подписи используется ...
- 233 Алгоритмы формирования и проверки электронной цифровой подписи ...
- 234 Параметр q отечественного стандарта цифровой подписи ГОСТ Р 34.10-94 имеет размерность ...
- 235 Для первоначального распределения ключей ...
- 236 Результатом генерации исходной информации при предварительном распределении ключей является ...





- 237) Протокол Диффи-Хеллмана является протоколом...
- 238) Протокол Диффи-Хеллмана ...
- 239) Метод разделения секрета используется, в первую очередь для снижения рисков ...
- 240) В системе открытого распределения ключей Диффи-Хеллмана используется ...
- 241) Защита информации в системе Диффи-Хеллмана основана на сложности...
- 242) Практическая реализация алгоритма Диффи-Хеллмана ...

