Криптографические методы защиты информации.ти_ФРК

1. Предположительно раньше других появился …
2. Первая механическая шифровальная машина была изобретена в …
3. «Атбаш» предположительно появился в …
4. Установите последовательность, в которой появились перечисленные шифры.
5. Своя дешифровальная служба до Первой мировой войны была у …
6. Датой учреждения первой государственной шифровальной службы в России принято считать …
7. Механическую машину, названную «шифровальным колесом», изобрел …
8. Электромеханическая машина «Бомба» была разработана в …
9. Первые программные вычислительные машины появились …
10. Доклад «Теория связи в секретных системах» представил …
11. AES был принят как государственный стандарт в …
12. В Российской Федерации основным законодательным актом, призванным стандартизировать и классифицировать методы защиты информации является …
13. Соотнесите закон и его назначение.
14. Установите последовательность, в которой происходило развитие криптографии.
15. Установите последовательность, описывающую принцип работы машины «Бомба».
16. Установите последовательность, в которой представлены положения Федерального закона № 63-ФЗ «Об электронной подписи»:

17 Установите соответствие между частью света (или страной) и проводимым конкурсом.

18 Установите соответствие между устройством и страной его происхождения.

19 Установите соответствие между государствами и уровнем развития криптографии в них до начала Первой Мировой Войны.

20 В соответствии с № 152-ФЗ «О персональных данных» персональными данными не является …

21 Шифр A5/1 образует кольцо из … элементов.

22 Если размерность полей Галуа определяется простым числом, то расширенные поля имеют размерность равную …

23 Для факторизации чисел с использованием эллиптических кривых можно прибегнуть к использованию алгоритма …

24 Эллиптические кривые строятся на основе уравнения вида …

25 Для исключения особых кривых должно выполняться условие, заданное уравнением …

26 Если порядок кривой равен n, то умножение точки на число k будет иметь эффект, эквивалентный …

27 Если точка не является точкой бесконечности, то число при тесте Эль-Гамаля …

28 Установите порядок действий при использовании алгоритма ECDSA для создания подписи.

29 Установите порядок действий, который позволяет реализовать тест Эль-Гамаля на простоту.

30 Установите последовательность действий для обмена ключами с использованием протокола Диффи-Хеллмана.

31 Установите последовательность, описывающую принцип получения ключей при использовании алгоритма RSA.

32 Для вычисления НОД не предназначен …

33 Вычислительная сложность алгоритма Евклида составляет …

34 При модуле 5 существует … классов вычетов.

35 Если a и b - элементы кольца классов вычетов Z/nZ, то их сумма a + b и произведение a * b ...

36 Результат вычисления функции Эйлера при p = 7 и q = 17 равен ...

37 Алгоритм RSA является безопасным при условии, что невозможно ...

38 Установите соответствие между выражением и принятым наименованием алгебраического кольца.

39 Установите соответствие между шифром и его описанием.

40 Установите соответствие между алгоритмом и утверждением о нём.

41 Режим, при котором каждый блок шифруется независимо друг от друга, но с использованием одного и того же ключа, называется ...

42 Режим, при котором каждый блок данных шифруется с использованием предыдущего, называется ...

43 Режим, при использовании которого применяется уникальный счетчик, называется ...

44 Сопоставьте операционную систему и используемый по умолчанию алгоритм в EFS.

45 Сопоставьте операцию и возвращаемый ею результат.

46 Сложение в SHA-256 происходит по модулю ...

47 Укажите последовательность действий, выполняемых EFS при расшифровке файла.

48 Ключ шифрования тома, создаваемый BitLocker, называется ...

49 Установите последовательность действий, которую выполняет BitLocker при расшифровке файлов.

50 Установите последовательность действий, которая происходит при работе SSL (последовательность указана частично).

51 Установите последовательность действий, соответствующую принципу работы Kerberos.

52 Установите соответствие между протоколами и утверждениями о них.

53 IPsec может функционировать на одном и том же узле в … режимах.

54 В SSH по умолчанию используется номер порта …

55 Алгоритм … обязательно должен поддерживаться клиентом для использования последней версии протокола S/MIME при шифровании.

56 Для алгоритма DES предполагается … раундов.

57 Алгоритм 3DES стандартно использует ключи длины …

58 Для AES-128 требуется … раундовых ключей.

59 Установите соответствие между операцией и её описанием в алгоритме AES.

60 Операция … в AES не включена в последний раунд.

61 Способ защиты данных, при котором информация шифруется на каждом этапе передачи, называется …

62 К алгоритмам с асимметричным шифрованием не относится …

63 Формула … позволяет вычислить число g, являющееся генератором по модулю p при использовании DSA.

64 Сопоставьте утверждение и хеш-функцию.

65 Установите соответствие между типом электронной подписи и частью её описания.

66 Открытый ключ при использовании схемы Эль-Гамаля состоит из … чисел.

67 Описанию ПЭП не соответствует утверждение, что ПЭП …

68 Установите последовательность действий при генерации ключей с использованием схемы Эль-Гамаля.

69 Установите последовательность действий, описывающую общий принцип сквозного шифрования.

70 Размер хеш-значения, получаемого в результате работы MD5, составляет …

71 Коллизия хеш-функции – это …

72 Битовая длина L числа p при использовании DSA в качестве алгоритма для подписания документа может составлять …

73 При использовании схемы Эль-Гамаля получателям передается … чисел.

74 Любой тип электронной подписи не содержит …

75 Установите соответствие между злоумышленным действием и его описанием.

76 Установите соответствие между видом электронной подписи и способом её получения.

77 Служба каталогов, которая обеспечивает управление централизованной аутентификацией и авторизацией пользователей, учетных записей и компьютеров в сети, называется …

78 Неверно утверждение об асимметричном шифровании …

79 Установите последовательность действий, описывающую общий работы CRC.

80 Установите последовательность действий, описывающую принцип работы HMAC.

81 Установите последовательность действий для процесса квантового распределения ключей.

82 Ключевым свойством квантовой криптографии является …

83 Операции, которые не вносят изменения в квантовое состояние системы при измерении, называются …

84 Понятие «гомоморфное шифрование» впервые было сформировано в …

85 Криптосистема, которая позволяет выполнять неограниченное количество операций сложения и одну операцию умножения, была представлена в …

86 Частично гомоморфные схемы позволяют производить …

87 К алгоритмам речевого шифрования не относится …

88 Для обеспечения безопасности речевого сигнала чаще других может быть использован алгоритм …

89 В случае использования QKD можно предъявлять более низкие требования в плане безопасности к …

90 В … году была обоснована возможность создания полностью гомоморфной криптосистемы шифрования и предложена такая система.

91 Изолированная область памяти внутри процессора для технологии Intel SGX называется …

92 Установите соответствие между компонентами и их функционалом в технологии Intel SGX.

93 Соотнесите направление криптографии и наиболее частый способ его применения.

94 Установите соответствие между технологией шифрования и описанием её свойств.

95 Установите соответствие между изолированной средой и её описанием для технологии ARM Trust Zone.

96 Intel SGX поддерживается с … поколения процессоров.

97 ARM TrustZone … шифрует данные по умолчанию.

98 Установите последовательность действий при работе Intel SGX.

99 Установите последовательность, в которой появлялись направления криптографии.

100 Установите последовательность, в которой происходит обработка транзакции в общем случае.