По какой причине удостоверяющий центр отзывает сертификат?

Если закрытый ключ пользователя скомпрометирован

Метод шифрования, в котором коды символов открытого текста складываются с элементами случайной или псевдослучайной последовательности называется

Гаммированием

Какая криптосистема применяется для открытого распределения ключей симметричного шифрования?

DH (Диффи-Хеллмана)

Что из перечисленного ниже лучше всего описывает удостоверяющий центр?

Организация, которая выпускает сертификаты открытых ключей

Функции, для которых легко найти функцию прямого отображения и вычислительно сложно найти обратное называются:

Односторонние функции

Установление санкционированным получателем (приемником) того факта, что полученное сообщение послано санкционированным отправителем называется

Аутентификацией

Как проверить, что самоподписанный сертификат был модифицирован?

Проверить цифровую подпись сертификата с помощью открытого ключа из этого сертификата

В чем преимущество RSA над DSA?

Он может обеспечить функциональность цифровой подписи и шифрования

Системы, где с помощью открытого ключа шифруют ключ симметричного криптоалгоритма, а само сообщение шифруют с помощью этого секретного ключа, называют

Гибридные криптосистемы

Какой из перечисленных ниже алгоритмов основан на сложности задачи дискретного логарифмирования?

DH (Диффи-Хеллмана)

Чему равна разрядность ключа алгоритма …Магма ГОСТ …?

256 бит
1

Что используется для создания 111¹1¹цифровой подписи?1

Закрытый ключ отправителя

(а для проверки - открытый ключ отправителя)
1

Какова эффективная длина ключа 3DES в схеме EDE2?

112 бит
1

При использовании классических криптографических алгоритмов ключ шифрования и ключ расшифрования совпадают и такие криптосистемы 1

Симметричными криптосистемами

Что необходимо иметь получателю для проверки электронной подписи на документе отправителя?

Сертификат открытого ключа отправителя

Какой из перечисленных ниже алгоритмов основан на сложности разложения больших чисел на два исходных простых сомножителя?

RSA

Чему равна допустимая разрядность ключа алгоритма шифрования Кузнечик?

256 бит

Какой из перечисленных ниже алгоритмов использует симметричный ключ и алгоритм хэширования?

HMAC

Какой ключ используется для зашифрования информации в асимметричной криптосистеме?

Открытый ключ получателя

Для чего используется протокол Цербер?

Для симметричной аутентификации (нам вроде такое не давали)

Какая цель атаки “предсказания дополнения” на блочный симметричный шифр?

Расшифровка блоков сообщения

Совокупность действий, выполняемых в заданной последовательности двумя или более субъектами с целью достижения определенного результата называется:

Протоколом

Какова цель атаки на гибридную криптосистему?

Подбор симметричного ключа

Что из перечисленного ниже лучше всего описывает цифровую подпись?

Это метод, позволяющий получателю сообщения проверить его источник и убедиться в целостности сообщения.

Какой атаке подвержены классические асимметричные криптосистемы?

Атака посредника

Какая из ниже приведенных систем с открытым ключом имеет наибольшую производительность?

ECC

Какая из ниже приведенных систем с открытым ключом

используется только для генерации цифровой подписи?

DSS

К какому типу криптоалгоритма относится алгоритм RSA?

Доказуемо стойкий

Что лежит в основе стойкости метода El-Gamal?

Вычисление логарифма в конечном поле

Что лежит в основе стойкости метода Диффи-Хеллмана?

Вычисление логарифма в конечном поле

Какой компонент ИОК отвечает за формирование списка отозванных сертификатов?

Центр сертификации или Удостоверяющий центр

Какой протокол был разработан для обеспечения системы электронных банковских расчетов с использованием пластиковых карт?

SET

Какая процедура распределения ключей не требует использования защищенного канала для передачи ключа адресату?

Метод Диффи-Хеллмана

Какая процедура задачи управления ключами наиболее важна с точки зрения уменьшения вероятности раскрытием ключа путем криптоанализа?

Генерация ключей

Какая атака на криптосистему RSA является наиболее эффективной?

Атака с подставкой (Man-in-the-middle attack)

Какая специфическая ошибка характерна при реализации таких криптоалгоритмов, как DES?

Отсутствие проверки на слабые ключи

Что такое криптографический протокол?

Совокупность алгоритмов криптографических преобразований…

К какому классу преобразований относится система шифрования Вижинера?

Подстановка

Сколько в среднем попыток требуется для взлома идеально стойкого криптоалгоритма с ключом длины N?

2^N

Какой из приведенных алгоритмов не является симметричным?

El-Gamal

Какую длину имеет секретный ключ в криптосистеме DES?

56 бит

В каком режиме должен работать блочный шифр, чтобы представлять собой синхронный поточный шифр?

OFB

В каком режиме должен работать блочный шифр, чтобы представлять собой самосинхронизирующийся поточный шифр?

CFB

Какова длина дайджеста, порождаемого хэш-функцией ГОСТ Р34.11-94?

256 бит

Какой алгоритм вычисления значения хэш-функции лежит в основе стандарта цифровой подписи DSS?

SHA

Сколько этапов составляют главный цикл алгоритма вычисления цифровой сигнатуры в MD5?

4

Какая из приведенных хэш-функций является самой медленной?

MD2