Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Косенок Сергей Михайлович
Должность: ректор
Дата подписания: 19.06.2024 07:40:58
Уникальный программный ключ:
e3a68f3eaa1e62674b54f4998099d3d6bfdcf836

Тестовое задание для диагностического тестирования по дисциплине:

Прикладная криптография,
8 семестр

Код, направление подготовки	09.03.02 Информационные системы и технологии
Направленность (профиль)	Информационные системы и технологии
Форма обучения	Очная
Кафедра разработчик	Информатики и вычислительной техники
Выпускающая кафедра	Информатики и вычислительной техники

№	Проверяемая компетенция	Задание	Варианты ответов	Тип сложности вопроса	Кол-во баллов за правильный ответ
1	ПК-4.1 ПК-4.2 ПК-4.3 ПК-2.1 ПК- 2.2 ПК-2.3 ПК-5.1 ПК- 5.2 ПК-5.3	Шифрование – это…	А) преобразовательный процесс исходного текста в зашифрованный Б) упорядоченный набор из элементов алфавита В) нет правильного ответа	Низкий	2

2	ПК-4.1 ПК-4.2 ПК-4.3 ПК-2.1 ПК- 2.2 ПК-2.3 ПК-5.1 ПК- 5.2 ПК-5.3	Дешифрование – это…	А) на основе ключа шифрованный текст преобразуется в исходный Б) пароли для доступа к сетевым ресурсам В) сертификаты для доступа к сетевым ресурсам и зашифрованным данным на самом компьютере	Низкий	2
3	ПК-4.1 ПК-4.2 ПК-4.3 ПК-2.1 ПК- 2.2 ПК-2.3 ПК-5.1 ПК- 5.2 ПК-5.3	Криптографическая система представляет собой…	А) семейство T преобразований открытого текста, члены его семейства индексируются символом k Б) программу В) систему	Низкий	2
4	ПК-4.1 ПК-4.2 ПК-4.3 ПК-2.1 ПК- 2.2 ПК-2.3 ПК-5.1 ПК- 5.2 ПК-5.3	Пространство ключей k – это…	А) набор возможных значений ключа Б) длина ключа В) нет правильного ответа	Низкий	2

5	ПК-4.1 ПК-4.2 ПК-4.3 ПК-2.1 ПК- 2.2 ПК-2.3 ПК-5.1 ПК- 5.2 ПК-5.3	Что является основой большинства современных блочных симметричных алгоритмов шифрования?	А) Сеть Фейстеля Б) Гаммирование В) Перемешивание Г) Алфавит	Низкий	2
6	ПК-4.1 ПК-4.2 ПК-4.3 ПК-2.1 ПК- 2.2 ПК-2.3 ПК-5.1 ПК- 5.2 ПК-5.3	Какие ключи используются в системах с открытым ключом	А) открытый Б) закрытый В) нет правильного ответа	Средний	5
7	ПК-4.1 ПК-4.2 ПК-4.3 ПК-2.1 ПК- 2.2 ПК-2.3 ПК-5.1 ПК- 5.2 ПК-5.3	Укажите ассиметричный алгоритм шифрования.	А) Эль-Гаммаля Б) IDEA В) DES Г) Blowfish	Средний	5

8	ПК-4.1 ПК-4.2 ПК-4.3 ПК-2.1 ПК- 2.2 ПК-2.3 ПК-5.1 ПК- 5.2 ПК-5.3	Электронной подписью называется…	А) присоединяемое к тексту его криптографическое преобразование Б) текст В) зашифрованный текст	Средний	5

9	ПК-4.1 ПК-4.2 ПК-4.3 ПК-2.1 ПК- 2.2 ПК-2.3 ПК-5.1 ПК- 5.2 ПК-5.3	Распределение ключей между пользователями вычислительной сети реализуется следующим образом:	А) прямым обменом сеансовыми ключами между пользователями сети; Б) использованием одного центра распределения ключей; В) использованием нескольких центров распределения ключей; Г) использованием альтернативных каналов связи.	Средний	5

10	ПК-4.1 ПК-4.2 ПК-4.3 ПК-2.1 ПК- 2.2 ПК-2.3 ПК-5.1 ПК- 5.2 ПК-5.3	Показатели криптостойкости:	А) количество всех возможных ключей Б) среднее время, необходимое для криптоанализа В) количество символов в ключе	Средний	5
11	ПК-4.1 ПК-4.2 ПК-4.3 ПК-2.1 ПК- 2.2 ПК-2.3 ПК-5.1 ПК- 5.2 ПК-5.3	Для современных криптографических систем защиты информации сформулированы следующие общепринятые требования:	А) длина шифрованного текста должна быть равной лине исходного текста Б) зашифрованное сообщение должно поддаваться чтению только при наличии ключа В) нет правильного ответа	Средний	5

12	ПК-4.1 ПК-4.2 ПК-4.3 ПК-2.1 ПК- 2.2 ПК-2.3 ПК-5.1 ПК- 5.2 ПК-5.3	Символы исходного текста складываются с символами некой случайной последовательности – это…	А) алгоритм гаммирования Б) алгоритм перестановки В) алгоритм аналитических преобразований	Средний	5
13	ПК-4.1 ПК-4.2 ПК-4.3 ПК-2.1 ПК- 2.2 ПК-2.3 ПК-5.1 ПК- 5.2 ПК-5.3	Самой простой разновидность подстановки является	А) простая замена Б) перестановка В) простая перестановка Г) алгоритм гаммирования	Средний	5
14	ПК-4.1 ПК-4.2 ПК-4.3 ПК-2.1 ПК- 2.2 ПК-2.3 ПК-5.1 ПК- 5.2 ПК-5.3	Из скольки последовательностей состоит расшифровка текста по таблице Вижинера	А) 3 Б) 4 В) 5 Г) 7	Средний	5

15	ПК-4.1 ПК-4.2 ПК-4.3 ПК-2.1 ПК- 2.2 ПК-2.3 ПК-5.1 ПК- 5.2 ПК-5.3	Укажите размер блока шифрования в алгоритме "Магма", описанном в ГОСТ 34.12-2018. (ответ в количестве бит)	А) 64 бит Б) 16 бит В) 8 бит Г) 128 бит	Средний	5

16	ПК-4.1 ПК-4.2 ПК-4.3 ПК-2.1 ПК- 2.2 ПК-2.3 ПК-5.1 ПК- 5.2 ПК-5.3	Алгоритм применения цифровой подписи на основе алгоритма шифрования RSA:	А) Получатель подтверждает подлинность подписи Б) Получатель вычисляет хэш-функцию m' = SKo mod N В) Значения (M,S) отправляются получателю. Г) Сравнение m'=m, по которому получатель признает подпись подлинной. Д) Получатель вычисляет хэш-функцию m = H(M) Е) Вычисление пары ключей: секретный и открытый, используя алгоритм шифрования RSA. Ж) Отправитель вычисляет m=H(M), где m – целое число. З) Отправитель вычисляет цифрову подпись S = mKs mod N	Высокий	8

17	ПК-4.1 ПК-4.2 ПК-4.3 ПК-2.1 ПК- 2.2 ПК-2.3 ПК-5.1 ПК- 5.2 ПК-5.3	Криптографические протоколы аутентификации используются, если	А) участвуют только два участника; Б) требуется подтверждение подлинности участников сеанса связи. В) пользователь протокола уверен в достоверности информации, получаемой от другого пользователя; Г) участники протокола не доверяют друг другу	Высокий	8
18	ПК-4.1 ПК-4.2 ПК-4.3 ПК-2.1 ПК- 2.2 ПК-2.3 ПК-5.1 ПК- 5.2 ПК-5.3	«Цифровая подпись» формируется на основе следующих элементов:	А) сообщения отправителя Б) секретного ключа отправителя В секретного ключа получателя Г) открытого ключа отправителя	Высокий	8

19	ПК-4.1 ПК-4.2 ПК-4.3 ПК-2.1 ПК- 2.2 ПК-2.3 ПК-5.1 ПК- 5.2 ПК-5.3	Какой метод используется при шифровании с помощью аналитических преобразований	А) алгебры матриц Б) матрица В) факториал Г) производная	Высокий	8
20	ПК-4.1 ПК-4.2 ПК-4.3 ПК-2.1 ПК- 2.2 ПК-2.3 ПК-5.1 ПК- 5.2 ПК-5.3	Какие таблицы Вижинера можно использовать для повышения стойкости шифрования	А) во всех (кроме первой) строках таблицы буквы располагаются в произвольном порядке Б) в качестве ключа используется случайность последовательных чисел В) нет правильного ответа	Высокий	8