Тестовое задание для диагностического тестирования по дисциплине:

Прикладная криптография,
8 семестр

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

№ п-п	Проверяемая компетенция	Задание	Варианты ответов	Тип сложности вопроса
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 ПК-16.1 ПК-16.2 ПК-16.3 ПК-17.1 ПК-17.2 ПК-17.3	Шифрование – это… .	1) необратимое преобразование информации с целью сокрытия от неавторизованных лиц и предоставления доступа к ней авторизованным пользователям 2) обратимое преобразование информации с целью открыть неавторизованным лицам и предоставления им доступа ко всей информации 3) обратимое преобразование информации с целью сокрытия от неавторизованных лиц и предоставления доступа к ней авторизованным пользователям 4) обратимое преобразование информации с целью открыть неавторизованным лицам и предоставления им доступа к части информаци	Низкий
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 ПК-16.1 ПК-16.2 ПК-16.3 ПК-17.1 ПК-17.2 ПК-17.3	Дешифрование – это…	1) на основе ключа шифрованный текст преобразуется в исходный 2) пароли для доступа к сетевым ресурсам 3) сертификаты для доступа к сетевым ресурсам и зашифрованным данным на самом компьютере	Низкий

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 ПК-16.1 ПК-16.2 ПК-16.3 ПК-17.1 ПК-17.2 ПК-17.3	Криптографическая система представляет собой…	1) набор криптографических преобразований или алгоритмов, предназначенных для решения определенной задачи защиты информационного процесса 2) ннабор криптографических преобразований информационного процесса 3) набор алгоритмов, предназначенных для решения определенной задачи защиты информационного процесса 4) преобразования, предназначенные для решения определенной задачи защиты информационного процесса	Низкий
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 ПК-16.1 ПК-16.2 ПК-16.3 ПК-17.1 ПК-17.2 ПК-17.3	Пространство ключей k – это…	1) набор возможных значений ключа 2) длина ключа 3) значение ключа 3) нет правильного ответа	Низкий
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 ПК-16.1 ПК-16.2 ПК-16.3 ПК-17.1 ПК-17.2 ПК-17.3	Что является основой большинства современных блочных симметричных алгоритмов шифрования?	1) Сеть Фейстеля 2) Гаммирование 3) Перемешивание 4) Алфавит	Низкий
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 ПК-16.1 ПК-16.2 ПК-16.3 ПК-17.1	Какие ключи используются в системах с открытым ключом	1) открытый 2) закрытый 3) иожет использоваться любой 4) ключ отсутсвуют	Средний

	ПК-17.2 ПК-17.3			
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 ПК-16.1 ПК-16.2 ПК-16.3 ПК-17.1 ПК-17.2 ПК-17.3	Укажите ассиметричный алгоритм шифрования	1) IDEA 2) DES 3) Blowfish 4) Схема Эль-Гаммаля	Средний
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 ПК-16.1 ПК-16.2 ПК-16.3 ПК-17.1 ПК-17.2 ПК-17.3	Электронной подписью называется…	1) комбинация знаков или паролей, которая служит эквивалентом обычной подписи на бумаге 2) комбинация знаков 3) комбинация паролей 4) текст	Средний
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 ПК-16.1 ПК-16.2 ПК-16.3 ПК-17.1 ПК-17.2 ПК-17.3	Распределение ключей между пользователями вычислительной сети реализуется следующим образом:	1) прямым обменом сеансовыми ключами между пользователями сети; 2) использованием одного центра распределения ключей; 3) использованием нескольких центров распределения ключей; 4) использованием альтернативных каналов связи.	Средний
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 ПК-16.1	Показатели криптостойкости:.	А) количество всех возможных ключей Б) вероятность подбора ключа за заданное время с заданными ресурсами В) количество операций или время (с заданными ресурсами), необходимое для взлома шифра с заданной вероятностью 4) стоимость вычисления ключевой информации или исходного текста	Средний

	ПК-16.2 ПК-16.3 ПК-17.1 ПК-17.2 ПК-17.3			
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 ПК-16.1 ПК-16.2 ПК-16.3 ПК-17.1 ПК-17.2 ПК-17.3	Для современных криптографических систем защиты информации сформулированы следующие общепринятые требования:	1) длина шифрованного текста должна быть равной длине исходного текста 2) зашифрованное сообщение должно поддаваться чтению только при наличии ключа 3) знание алгоритма шифрования не должно влиять на надежность защиты 4) любой ключ из множества возможных должен обеспечивать надежную защиту информации; 5) алгоритм шифрования должен допускать как программную, так и аппаратную реализацию	Средний
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 ПК-16.1 ПК-16.2 ПК-16.3 ПК-17.1 ПК-17.2 ПК-17.3	Методы шифрования, при которых символы исходного текста складываются с символами некой случайной последовательности – это…	1) алгоритм гаммирования 2) алгоритм перестановки 3) алгоритм налитических преобразований 4) нет правильного ответа	Средний
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 ПК-16.1 ПК-16.2 ПК-16.3 ПК-17.1 ПК-17.2 ПК-17.3	Укажите размер блока шифрования в алгоритме "Магма", описанном в ГОСТ 34.12-2018. (ответ в количестве бит)	1) 16 бит 2) 64 бит 3) 8 бит 4) 128 бит	Средний

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 ПК-16.1 ПК-16.2 ПК-16.3 ПК-17.1 ПК-17.2 ПК-17.3	Укажите размер блока шифрования в алгоритме "Кузнечик", описанном в ГОСТ 34.12-2018. (ответ в количестве бит)	1) 16 бит 2) 64 бит 3) 8 бит 4) 128 бит	Средний
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 ПК-16.1 ПК-16.2 ПК-16.3 ПК-17.1 ПК-17.2 ПК-17.3	Криптографические протоколы аутентификации используются для выполнения некоторых действий по обмену информацией в ситуации	А) цели участников могут быть нарушены злоумышленником Б) под угрозой оказывается конфиденциальность сообщений. В) под угрозой оказывается целостность сообщений. Г) под угрозой оказывается подтверждаемость сообщений	Средний
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 ПК-16.1 ПК-16.2 ПК-16.3 ПК-17.1 ПК-17.2 ПК-17.3	«Электронная цифровая подпись» формируется на основе следующих элементов:	1) набор значений только в ивде отрытого ключа 2) ключевая пара из набора значений: «открытый» и «закрытый» ключ. 3) сертификат ключа проверки электронной цифровой подписи 4) средство криптографической защиты информации	Высокий
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 ПК-16.1 ПК-16.2 ПК-16.3 ПК-17.1	Какой метод используется при шифровании с помощью аналитических преобразований	1) алгебры матриц 2) матрица 3) факториал 4) производная	Высокий

	ПК-17.2 ПК-17.3			
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 ПК-16.1 ПК-16.2 ПК-16.3 ПК-17.1 ПК-17.2 ПК-17.3	Какие таблицы Вижинера можно использовать для повышения стойкости шифрования	1) во всех (кроме первой) строках таблицы буквы располагаются в произвольном порядке 2) в качестве ключа используется случайность последовательных чисел 3) качестве ключа используются случайные последовательности чисел, которые задают номера используемых строк матрицы Вижинера для шифрования 4) нет правильного ответа	Высокий
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 ПК-16.1 ПК-16.2 ПК-16.3 ПК-17.1 ПК-17.2 ПК-17.3	Дешифрование	1) используется для чтения зашифрованных данных 2) выполняется с помощью тех же алгоритмов, что и шифрование. 3) выполняется с помощью алгоритмов существенно отличаемых от шифрования 4) в процессе испорльзуется ключ	Высокий
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 ПК-16.1 ПК-16.2 ПК-16.3 ПК-17.1 ПК-17.2 ПК-17.3	В криптографии и криптосистемах число бит в ключе, используемом в криптографических операциях, таких как шифрование и подписывание электронной цифровой подписью – это:	1) размер ключа 2) длина ключа 3) пространство ключей 4) ключ	Высокий