Тестовое задание для диагностического тестирования по дисциплине: «Криптографические методы защиты информации» 5 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

№	Задание	Варианты ответов	Тип сложности вопроса
1	Какая из следующих задач НЕ решается с помощью криптографических методов?	a) защита конфиденциальности b) защита целостности c) защита доступности d) аутентификация	**низкий**
2	Какой алгоритм шифрования был разработан с целью заменить устаревший алгоритм DES?	a) Магма b) RSA c) AES d) Blowfish	**низкий**
3	Что такое атака с помощью социальной инженерии?	a) Попытка взлома шифра с использованием социальных сетей b) Попытка взлома шифра путем подкупа или манипулирования людьми, имеющими доступ к защищаемой информации c) Попытка взлома шифра путем обратного инжиниринга программного обеспечения d) Попытка взлома шифра путем перехвата и анализа передаваемой информации	**низкий**
4	Что такое атака грубой силы?	a) Попытка взлома шифра путем систематической проверки всех возможных ключей b) Попытка взлома шифра путем подмешивания вредоносного кода в зашифрованное сообщение c) Попытка взлома шифра путем перехвата и анализа передаваемой информации d) Попытка взлома шифра путем перебора всех возможных комбинаций символов	**низкий**
5	Что такое симметричное шифрование?	a) Шифрование, при котором используется один и тот же ключ для шифрования и дешифрования b) Шифрование, при котором используется симметричный ключ для шифрования c) Шифрование, при котором ключ генерируется с использованием симметричного преобразования d) Абсолютно стойкое шифрование	**низкий**
6	Какое утверждение о криптографических хэш-функциях является верным?	a) Хэш-функции используются только для шифрования сообщений b) Хэш-функции являются однонаправленными c) Хэш-функции позволяют выполнять шифрование с использованием открытого ключа d) Хэш-функции используются только для аутентификации пользователей	**средний**

№	Задание	Варианты ответов	Тип сложности вопроса
7	На чем основана стойкость алгоритма RSA?	a) передача зашифрованного ключа b) факторизация c) дискретное логарифмирование d) аутентификация	**средний**
8	На чем основана стойкость алгоритма Диффи-Хелламана?	a) передача зашифрованного ключа b) факторизация c) дискретное логарифмирование d) аутентификация	**средний**
9	Какое утверждение об абсолютной стойкости шифрования верно?	a) Существует единственный стойкий шифр b) Абсолютная стойкость недостижима c) Алгоритм Эль-Гамаля предоставляет абсолютную стойкость d) Алгоритм DES предоставляет абсолютную стойкость	**средний**
10	Что такое цифровая подпись?	a) Хэш-значение сообщения b) Симметричный ключ для шифрования сообщений c) Инструмент аутентификации d) Публичный ключ получателя	**средний**
11	На основе каких шифров строятся трёхэтапные протоколы?	a) Симметричных b) Асимметричных c) Однонаправленных d) Коммутативных	**средний**
12	Какая атака основана на сопоставлении статистик шифртекста и естественного языка?	a) Атака методом грубой силы b) Линейный криптоанализ c) Дифференциальный криптоанализ d) Частотный криптоанализ	**средний**
13	Какие операции определены в кольце?	а) Сложение и умножение б) Сложение и деление в) Вычитание и умножение г) Вычитание и деление	**средний**
14	Что такое протоколы нулевого разглашения?	а) Протоколы, которые обеспечивают анонимность отправителя сообщения б) Протоколы, которые позволяют сторонам проверить совпадение некоторой информации без раскрытия в) Протоколы, которые гарантируют, что сообщение не было изменено в процессе передачи г) Протоколы, которые обеспечивают защиту от атак типа "человек посередине"	**средний**
15	Для чего предназначен алгоритм Эль-Гамаля в криптографии?	а) Для шифрования сообщений с использованием симметричного ключа б) Для создания цифровых подписей и протоколов аутентификации	**средний**

№	Задание	Варианты ответов	Тип сложности вопроса
		в) Для генерации случайных чисел в криптографических системах г) Для обнаружения и исправления ошибок в передаваемых данных	
16	Какой алгоритм шифрования используется в протоколе HTTPS?	a) DES b) RSA c) AES d) Эль-Гамаля	**высокий**
17	Что такое криптографическая соль?	a) Хэш-значение сообщения b) Случайная строка c) Публичный ключ получателя d) Секретный ключ для шифрования сообщений	**высокий**
18	Как называется группа, все элементы которой коммутируют?	а) Абелева группа б) Кольцо в) Поле г) Моноид	**высокий**
19	При каком условии гаммирование будет абсолютно стойким шифром?	а) длина открытого текста не превышает гаммы б) гамма будет совершенно случайным набором символов в) противник не будет знать ключа г) гаммирование не может быть абсолютно стойким ни при каких обстоятельствах	**высокий**
20	Каково количество раундов преобразований в алгоритме Кузнечик?	a) 10 раундов b) 12 раундов c) 14 раундов d) 16 раундов	**высокий**