Оценочные материалы для промежуточной аттестации 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

Типовые задания для контрольной работы:

Примерные задания для контрольной работы:

Задание 1. Определите ключи шифра Цезаря, если известны следующие пары открытый текст – шифротекст (исходный алфавит:
АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ):
АПЕЛЬСИН - ТВЧЮОДЫА
МАНДАРИН – ТЁУЙЁЦОУ
Задание 2. Расшифруйте следующие сообщения, зашифрованные шифром Цезаря, и определите ключ n, 0<n<33, если известно, что исходные сообщения составлены из алфавита АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ:
ЮВПЛШУХ
СФЫЮБШЯФУ
Задание 3. Зашифровать свою фамилию с помощью алгоритма RSA.
Задание 4. Зашифровать свою фамилию с помощью алгоритма шифрования Эль-Гамаля.
Задание 5. Зашифровать свою фамилию с помощью алгоритма шифрования о открытым ключом.
Задание 6. Зашифровать свою фамилию с помощью алгоритма шифрования о открытым ключом.
Задание 7. Для заданного файла необходимо определить скрытое сообщение и использованный метод его стеганографического сокрытия.
Задание 8. Получить от пользователя ключ, имя входного и выходного файла. Инициализировать генератор случайных чисел с помощью ключа. Открыть указанные файлы.
Задание 9. Прочитать строку из файла. Получить случайное число. Получить ASCII-код очередного символа строки и увеличить его на случайное число, полученное на шаге 4. Проверить правильность (допустимый диапазон) нового ASCII-кода.
Задание 10. В выходную строку записать очередной символ, соответствующий ASCII-коду, полученному на шаге 6. Если не достигли конца входной строки, то перейти к шагу

4. Записать полученную строку в выходной файл. Если не достигнут конец файла, то перейти к шагу 3. Закрыть файлы.

***Типовые вопросы к экзамену*:**

1. Предмет криптографии. Определения. Задачи. Исторические примеры.
2. Виды атак на криптографические алгоритмы. Понятие стойкости.
3. Классификация алгоритмов шифрования. Примеры простейших шифров.
4. Шифры замены. Математическая модель. Примеры.
5. Шифры перестановки. Математическая модель. Примеры.
6. Шифры гаммирования. Математическая модель. Примеры.
7. Принципы построения блочных шифров. Схема Фейстеля.
8. Алгоритм симметричного шифрования DES.
9. Алгоритм симметричного шифрования Rijndael.
10. Алгоритмы симметричного шифрования IDEA и Blowfish.
11. Режимы выполнения алгоритмов симметричного шифрования.
12. Поточные криптосистемы. Принципы построения. Классификация. Проблема синхронизации.
13. Поточные шифры. Отличия от блочных. Стойкость. Методы анализа.
14. Примеры поточных шифров на основе LFSR.
15. Примеры поточных шифров, использующих аддитивные генераторы.
16. Примеры поточных шифров на основе FCSR.
17. Математические методы криптоанализа: метод опробования, методы на основе теории статистических решений.
18. Линейный криптоанализ.
19. Разностный криптоанализ.
20. Основные принципы построения асимметричных криптосистем. Стойкость.
21. Шифросистема RSA. Стойкость.
22. Шифросистема Эль-Гамаля. Стойкость.
23. Шифросистема на основе принципа «рюкзака».
24. Шифросистема Рабина. Стойкость.
25. Алгоритм обмена ключами Диффи-Хеллмана.
26. Хэш-функции. Требования. Типы функций хэширования.
27. Атаки на функции хэширования.
28. Функция хеширования MD5.
29. Функция хеширования SHA-1.
30. Общие положения электронной цифровой подписи. Задачи. Требования.
31. Прямая и арбитражная цифровая подписи. Примеры.
32. Стандарт электронной цифровой подписи DSS.
33. Цифровая подпись на основе алгоритмов с открытыми ключами. Схема Фиата-Шамира.
34. Цифровая подпись Эль-Гамаля. Схема RSA.
35. Стандарт электронной цифровой подписи DSS.
36. Применение эллиптических кривых в криптографии. Алгоритм шифрования на основе эллиптических кривых.
37. Алгоритмы обмена ключами и электронной цифровой подписи на основе эллиптических кривых.
38. Стеганографические методы защиты информации. Основные понятия и определения. Области применения.
39. Общая модель стеганосистемы. Проблема устойчивости. Стегоанализ.
40. Методы сокрытия информации в неподвижных изображениях.
41. Методы сокрытия информации в текстовых данных.

42. Протоколы аутентификации. Двусторонняя аутентификация.
43. Протоколы аутентификации. Односторонняя аутентификация.