Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новосибирский государственный технический университет»
Кафедра вычислительной техники
Кафедра защиты информации

Паспорт
расчетно-графической работы

по дисциплине «Криптографические методы защиты информации», 2 семестр

1. **Методика оценки.**

Задание: Шифр Виженера.

Структура:1. Цель работы. 2. Постановка задачи. 3.Результаты выполнения. 4. Заключение. 5. Список литературы.

Этапы выполнения и защиты: в соответствии со структурой

Оцениваемые позиции: работа в целом.

2. **Критерии оценки.**

- работа считается **не выполненной,** если оценка составляет менее 49 баллов.
- работа считается выполненной **на пороговом** уровне, если оценка составляет 50-72 баллов.
- работа считается выполненной **на базовом** уровне, если оценка составляет 73-88 баллов.
- работа считается выполненной **на продвинутом** уровне, если оценка составляет более 88 баллов.

3. **Шкала оценки.**

В общей оценке по дисциплине баллы за работы учитываются в соответствии с правилами балльно-рейтинговой системы, приведенными в рабочей программе дисциплины.

4. **Примерный перечень тем РГР.**

1. Шифр одиночной перестановка по ключу.
2. Шифр двойной перестановка по ключу.
3. Шифр перестановки с запретом записи.
4. Шифр перестановки на основе «магического» квадрата.
5. Шифр перестановки «по маршрутам».
6. Шифр перестановки с различными размерами блоков.
7. Шифр простой перестановки с изменением направления записи/чтения.
8. Шифры замены. Система Цезаря.
9. Шифры замены. Система Полибия.
10. Шифры замены. Простая замена.
11. Шифр Гронсфельда.
12. Шифр Виженера.
13. Шифр многоалфавитной замены.

14. Шифр монофонической замены.

15. Шифр гаммирования.

5. Перечень вопросов к защите РГР.

Вопросы для защиты РГР по дисциплине
«Криптографические методы защиты информации»

Минимальное количество вопросов – 2, по одному из каждой части.

Часть 1

1.
1. Дайте определение шифра, ключа.
2. Чем шифрование отличается от кодирования.
3. Что такое тайнопись.
4. Для чего применяются шифры.
5. Что такое алфавит.
6. Какое значение имеет буква.
7. Что такое (k. –граммы.
8. Что такое индекс совпадения и как он вычисляется.
   Как в закодированном тексте выделить с помощью биграмм:
9. Символы (О,Е,А,И);
10. Символы (Ь,Ы).
11. Символ (Э);
12. Символы (С,Т);
13. Символ (Л);
14. Символ (Н);
15. Символы (О,В).

2.
1. Какие шифры называются симметричными.
2. Особенность секретной связи при использовании симметричных шифров.
3. Какие шифры называются перестановкой.
4. Определение функциональной эквивалентности шифров.
5. В чем заключается единственность шифра перестановки.
   Приведите схему перестановки:
6. простой;
7. одиночной по ключу;
8. двойной по ключу;
9. с запретом записи;
10. с использованием магических квадратов;
11. по «маршрутам»;
12. со сменой направления записи/чтения;
13. использующей разные размеры блоков;
14. повторной перестановки.
15. Как определить размер блока линейной перестановки для повторных перестановок.
16. В чем заключаются фундаментальные особенности шифров перестановки.
17. Что называется циклом или раундом при шифровании.
18. Что такое характеристическая функция ключа и для чего она может быть использована.
19. Какому шифру перестановки функционально эквивалентны остальные шифры перестановки.

3.
1. Как определяется стойкость шифра.
2. В каких единицах измеряется длина ключа.
3. В каких единицах измеряется стойкость шифра.
4. Что такое расстояние единственности.
5. В каких единицах измеряется переборная стойкость шифра.
6. В чем различие между длиной и размером ключа.
7. Что такое период ключа.
8. В чем заключаются фундаментальные особенности перестановки.
9. Приведите примеры чувствительности перестановки к специально подобранному тексту.
10. В чем заключается зависимости длины ключа перестановки от шифруемого текста.

11. В чем особенность шифрования перестановкой не полностью заполненного блока текста.
12. Какими способами можно повысить эффективность шифра перестановки.
13. Что такое защищенная кодировка и в чем ее смысл.
14. Как и в каких единицах измеряется переборная стойкость шифра.

4.
1. Какие шифры называются шифрами замены.
2. Опишите шифр:
а. Цезаря;
б. Полибия;
в. простой замены;
г. Гронсфельда;
д. Виженера.
3. Чем системы Цезаря, Полибия и простой замены отличаются от других шифров замены.
4. Приведите формулу общей математической модели шифров Цезаря, Гронсфелда, Виженера.
5. Какие шифры называются шифрами Бофора.
6. Какой шифр называется шифром Вернама.
7. Постройте собственный пример шифрования и расшифрования по формулам (4.2., отличающийся от приведенного в пособии.
8. Какой шифр называется шифром гаммирования, с какими известными шифрами и как он связан.
9. Что называется инфляцией алфавита.
10. В чем основная особенность шифра гаммирования.
11. Какой условие должно выполняться для обратимого шифрования композицией замен.
12. Какой алфавит называется входным (исходным) для шифра, а какой – выходным алфавитом.
13. Какие шифры называются одноалфавитными, моноалфавитными, полиалфавитными, многоалфавитными.
14. Как получить ключ шифра замены при шифровании перестановкой.
15. Частным случаем каких шифров является шифр перестановки.
16. Какой шифр называется шифром гаммирования с обратной связью.
17. Что общего у шифров монофонической замены, перестановки и гаммирования с обратной связью.
18. Как объединяются повторные применения шифров:
а. Цезаря;
б. Виженера;
в. простой замены и Виженера.

Часть 2.

5.
1. Размер блока и ключа шифра DES.
2. Размер блока и ключа шифра AES.
3. Размер блока и ключа шифра ГОСТ.
4. Режимы работы шифра DES.
5. Режимы работы шифра ГОСТ.
6. Количество базовых циклов шифрования в шифре DES.
7. Количество базовых циклов шифрования в шифре AES.
8. Количество базовых циклов шифрования в шифре ГОСТ.
9. Что называется имитовставкой в шифре ГОСТ.
10. Как определяется размер имитовставки.
11. Что называется синхропосылкой в шифре ГОСТ.
12. Что называется сетью Фейстейля.
13. Что называется SP-сетью.
14. Где в сообщении должна располагаться имитовставка шифра ГОСТ.
15. Какой шифр называется 3DES.

6.
1. Назначение и ограничения метода полного перебора.
2. Что называется переборным пространством.
3. Теоретическая оценка сокращения переборного пространства при поиске по образцу.
4. Чем отличается направленный случайный поиск от простого случайного поиска.
5. В каком случае при случайном поиске число просмотров будет минимальным.
6. В чем заключается метод проб и ошибок, с каким разделом математической статистики он связан.

7. Что называется «парадоксом дней рождения».
8. Каким требованиям (по Шеннону. должен отвечать «хороший» статистический метод криптоанализа.
9. Определите два основных класса методов криптоанализа.

В ответах на контрольные вопросы 10-16 дайте определение и опишите основные элементы для указанного в вопросе метода.

10. Метод вероятных слов.
11. Тест Казиски.
12. Метод «встречи посередине».
13. Метод линейного криптоанализа.
14. Метод дифференциального криптоанализа
15. Слайдовый метод.
16. Метод криптоанализа на связанных ключах.