Областное государственное бюджетное

профессиональное образовательное учреждение

 «Смоленская академия профессионального образования»

Утверждаю

Зам. директора по НМР

\_\_\_\_\_\_\_\_\_\_\_\_\_Н.В.Судденкова

Комплект

контрольно-измерительных материалов

для проведения дифференцированного зачета

по учебной дисциплине Криптографические методы защиты информации

для студентов 4 курса

специальности 090905 Организация и технология защиты информации

Смоленск 2014

Комплект контрольно-измерительных материалов дисциплины Криптографические методы защиты информации разработан на основе программы учебной дисциплины Криптографические методы защиты информации для специальности 090905 Организация и технология защиты информации.

Организация разработчик: областное государственное бюджетное профессиональное образовательное учреждение «Смоленская академия профессионального образования»

Разработчик:

Малахова В.Г., преподаватель общепрофессиональных дисциплин

Рассмотрено на заседании кафедры

Протокол № 3 от « 11 » ноября 2014 г.

Зав. кафедрой \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_В.Г.Малахова

Рассмотрено научно-методическим советом ОГБПОУ СмолАПО

Протокол № \_\_\_ от «\_\_\_»\_\_\_\_\_20\_\_г.

\_\_\_\_\_\_\_\_\_\_\_\_\_

**Содержание**

**1. Паспорт комплекта контрольно-оценочных материалов 3**

**1.1. Область применения 3**

**1.2. Освоение умений и усвоение знаний: 4**

**1.3. Организация контроля и оценки освоения программы учебной дисциплины 4**

**2. Оценка освоения теоретического курса учебной дисциплины 4**

**3. Структура контрольно-оценочных материалов для зачета 4**

**3.1. Теоретические вопросы: 4**

**3.2. Практические задания: 5**

**4 Условия выполнения заданий 6**

**4.1 Условия выполнения задания 6**

**4.2 Инструкция по выполнению задания 6**

**5 Критерии оценки 7**

**6 Литература 7**

**Приложение 8**

# 1. Паспорт комплекта контрольно-оценочных материалов

## 1.1. Область применения

 Контрольно-оценочные материалы предназначены для проверки результатов освоения учебной дисциплины Криптографические методы защиты информации основной профессиональной образовательной программы (далее ОПОП) по специальности СПО 090905 Организация и технология защиты информации.

|  |  |
| --- | --- |
| **Освоенные умения, усвоенные знания** | **Показатели оценки результата** |
| **1** | **2** |
| В результате освоения дисциплины обучающийся должен уметь:Использовать программно-аппаратные средства для обработки шифрованных данныхРассчитывать параметры типовых шифров замены и перестановки;Использовать частотные характеристики языков в криптоанализе; | -Результативность использования программно-аппаратных средств для поставленной задачи-Правильность расчета параметров типовых шифров-Павильность криптоанализа текста |
| В результате освоения дисциплины обучающийся должен знать:Место и роль криптографических методов в системах защиты государственной, конфиденциальной и коммерческой информацииТребования к шрифтам и основные характеристики шрифтов; Принципы построения современных шифросистем; Основные математические методы, используемые в анализе типовых криптографических алгоритмовКриптографические протоколы; | -Точность изложения места и роли криптографии в системах защиты информации-Точность изложения характеристик шифров и требований к ним.-Точность определения последовательности действий алгоритмов шифрования-Точность изложения методов анализа криптографических алгоритмов-Точность изложения последовательности действий в криптографических протоколах |

* 1. **Система контроля и оценки освоения программы учебной дисциплины**

Предметом оценки учебной дисциплины являются освоенные умения и усвоенные знания обучающихся.

Текущий контроль освоения программы дисциплины проводится в пределах учебного времени, отведенного на её изучение, с использованием таких методов как написание самостоятельных работ, контрольных работ, выполнение тестов, проведение устного опроса.

Итоговый контроль освоения программы дисциплины Криптографические методы защиты информации проводится в форме: дифференциального зачета.

Зачет проводится в пределах учебного времени, отведенного на изучение программы дисциплины.

Оценка освоения программы учебной дисциплины проводится в соответствии с «Положением о текущем контроле успеваемости и промежуточной аттестации студентов в ОГБПОУ СмолАПО и рабочим учебным планом по специальности.

* 1. **Организация контроля и оценки освоения программы учебной дисциплины**

Условием допуска к зачету является положительная текущая аттестация по всем практическим занятиям учебной дисциплины, ключевым теоретическим вопросам дисциплины.

## 2. Оценка освоения теоретического курса учебной дисциплины

1) Контроль теоретического материала

2) Выполнение практических заданий и проведение самоконтроля

**2.1 Вопросы и практические задания к зачету.**

 **1.** Алгоритм Диффи-Хеллмана дает возможность

* безопасно обменяться общим секретом
* **безопасно обменяться общим секретом при условии аутентификации сторон**
* подписать сообщение

2. Аутентификация сторон в алгоритме Диффи-Хеллмана необходима, потому что

* **в противном случае атакующий может перехватить передаваемые открытые ключи и заменить их своим открытым ключом**
* в противном случае атакующий может взломать дискретный логарифм
* в противном случае стороны не смогут вычислить общий секрет

**3.** Теорема Эйлера формулируется следующим образом

* an-1 ≡ 1 mod n, если n - простое
* **aΦ(n) ≡ 1 mod n для всех взаимнопростых a и n, где Φ(n) - число положительных чисел, меньших n и взаимнопростых с n**
* если р – простое, то число положительных чисел, меньших р и взаимнопростых с р, равно р-1

3. Совокупность заранее оговоренных способов преобразования исходного секретного сообщения с целью его защиты называется

* алгоритм
* протокол
* **шифр**
* ключ

4. В протоколе Нидхэма-Шредера KDC выполняет:

* **распределение ключа сессии**
* распределение открытых ключей участников
* **аутентификацию участников**

**5.** Выберите верное утверждение:

* В криптографии с использованием эллиптических кривых все значения вычисляются по модулю числа n, которое является произведением двух простых чисел.
* **В криптографии с использованием эллиптических кривых все значения вычисляются по модулю простого числа р.**
* В криптографии с использованием эллиптических кривых все значения вычисляются по модулю произвольного числа р.

**6.** Выберите правильное высказывание

* подпись с использованием эллиптических кривых является детерминированной
* уравнения на эллиптических кривых нельзя использовать для создания цифровых подписей
* **подпись с использованием эллиптических кривых является рандомизированной**

**7.** В стандарте ГОСТ 3410 используется следующая хэш-функция

* MD5
* SHA-1
* **ГОСТ 3411**
* **SHA-2**

**8.** Подпись, создаваемая RSA, является

* **детерминированной**
* рандомизированной

**9.** Выберите правильное утверждение

* **подпись должна быть битовым образцом, который зависит от подписываемого сообщения**
* подпись должна обеспечивать невозможность просмотра сообщения
* **подпись должна использовать некоторую уникальную информацию отправителя для предотвращения подделки или отказа**

**10.** Сеть Фейстеля широко используется при разработке алгоритмов симметричного шифрования, потому что

* **для обратимости сети Фейстеля не требуется обратимость образующей функции F**
* **сеть Фейстеля достаточно компактна и проста в реализации**
* других способов реализации алгоритмов симметричного шифрования не существует
* **увеличение количества раундов сети Фейстеля приводит к увеличению стойкости алгоритма шифрования**

**11.** При дешифровании DES подключи используются

* в произвольном порядке
* в том же порядке, что и при шифровании
* **в обратном порядке относительно их использования при шифровании**

**12.** Зависимость между ключами шифрования и дешифрования в алгоритмах симметричного шифрования должна быть следующей:

* между ключами шифрования и дешифрования не должно быть никакой зависимости
* **ключи шифрования и дешифрования должны в точности совпадать**
* **ключ дешифрования должен легко получаться из ключа шифрования**

**13.** Подписи, созданные с использованием стандарта ГОСТ Р3410-94, являются рандомизированными, так как …

* для разных сообщений с использованием одного и того же закрытого ключа каждый раз будут создаваться разные подписи
* **для одинаковых сообщений с использованием одного и того же закрытого ключа каждый раз будут создаваться разные подписи**
* для одинаковых сообщений с использованием разных закрытых ключей каждый раз будут создаваться разные подписи
* для разных сообщений с использованием разных закрытых ключей каждый раз будут создаваться разные подписи

14. Выберите вариант ответа, содержащий только простые числа

* 2, 7, 17, 37, 57, 107
* 3, 7, 19, 39, 59, 101
* 2, 6, 18, 39, 58, 117
* **2, 11, 31, 61, 101, 131**

**15.** Дополнительными параметрами хэш-функции ГОСТ 3411 являются

* ключи для алгоритма симметричного шифрования ГОСТ 28147
* начальное значение хэш-кода
* **стартовый вектор хэширования**

**16.** Под replay-атакой понимается:

* невозможность получения сервиса законным пользователем
* **повторное использование переданного ранее сообщения**
* модификация передаваемого сообщения

**17.** Сервис, который обеспечивает невозможность несанкционированного просмотра данных, называется

* аутентификацией
* целостностью
* **конфиденциальностью**

**18.** Конфиденциальность – это

* **невозможность несанкционированного просмотра данных**
* невозможность несанкционированного изменения данных
* невозможность несанкционированного доступа к данным

**19.** Выходом хэш-функции является

* **сообщение фиксированной длины**
* сообщение той же длины, что и входное сообщение
* сообщение меньшей длины

**20.** Требование односторонности хэш-функции состоит в следующем

* **легко создать хэш-код по данному сообщению, но вычислительно невозможно восстановить сообщение по данному хэш-коду**
* вычислительно невозможно найти два сообщения, имеющих одинаковый хэш-код
* хэш-код может быть вычислен для сообщения любой длины

**21.** Первым шагом в хэш-функции MD5 выполняется добавление битов, цель которого

* добавить случайные биты, усложняющие восстановление сообщения
* **сделать сообщение кратным 512 битам**
* скрыть истинную длину сообщения

**22.** Выполните операцию циклического сдвига вправо на 5 разрядов для двоичного числа 01011001. Ответ представьте в двоичной системе счисления

**Ответ: 11001010**

**23.** Пусть каждые три бита входного сообщения заменяются по следующей таблице замен: Выполните разбиение исходного сообщения на блоки по три бита и произведите поблочную замену для сообщения, представленного в цифровом виде: 0В57 . Ответ представьте в двоичной системе счисления.



**Ответ: 1101 1000 0100**

**24.** Найдите числа х и у, удовлетворяющие уравнению 30х +12y = НОД(30,12) В качестве ответа запишите через запятую сначала значение х, а затем без пробела – значение у Например, если при вычислениях получилось, что х=-5, а у=2, то ответ надо записать так: -5,2

**Ответ: 1,-2**

**25.** Определите последовательность из первых четырех чисел, вырабатываемых линейным конгруэнтным генератором псевдослучайных чисел для следующих параметров генератора: а =21, b =19 и c = 32 (k0 принять равным 0)

**Ответ: k1=19, k2=2, k3=29, k4=20**

**26.** Определите первые 8 бит псевдослучайной последовательности, получаемой с помощью генератора ПСЧ на основе линейного сдвигового регистра, изображенного на рисунке, если начальное значение регистра следующее: b4=0, b3=1, b2=0, b1=1



**Ответ: 10100111**

**27.** Абоненты некоторой сети применяют цифровую подпись по стандарту ГОСТ Р3410-94 с общими параметрами p = 47, q = 23, a = 7. Найдите открытый ключ абонента. Петрова и вычислите его цифровую подпись для Х = 8, k = 7, h = 10.

**Ответ: 16, r = 9, s = 4**

**28.** Зашифруйте сообщение m шифром Вернама с ключом k: m = 1111001101, k = 0110001011

**Ответ: 1001000110**

**29.** Расшифруйте сообщение, зашифрованное методом перестановки по таблице 4x4 (символ подчеркивания заменяет пробел) Ключ указывает порядок считывания столбцов при шифровании.

Ответ запишите прописными русскими буквами; в качестве пробела используйте символ подчеркивания Сообщение: ЕТ\_ЧСЕЙЮРЫЛКНК Ключ: 2143

**Ответ: СЕКРЕТНЫЙ\_КЛЮЧ**

**30.** Имеется таблица замены для двух шифров простой замены: шифра №1 и шифра №2



Расшифруйте сообщение ВЖПРЮЛЪЦ, зашифрованное с помощью шифра №1. Ответ запишите прописными русскими буквами. Если ответ состоит из нескольких слов, запишите его с пробелами, например: НОВОЕ ЗАДАНИЕ

**Ответ: АПЕЛЬСИН**

## 4 Условия выполнения заданий

#### 4.1 Условия выполнения задания

Задание выполняется в учебной аудитории.

Используемое оборудование: персональные компьютеры, прикладное программное обеспечение

Соблюдение техники безопасности.

#### 4.2 Инструкция по выполнению задания

Задание выполняется в тестирующей оболочке:

Время выполнения задания – 60 минут

## 5 Критерии оценки

Вопросы 1-21 – по 1 баллу, всего 21 балл.

Вопросы 22-30- по 3 балла, всего 27 баллов.

Итого: 48 баллов.

Оценка «5» ставится в случае, если по результатам тестирования набрано 42-48 баллов.

 Оценка «4» ставится в случае, если по результатам тестирования набрано 36-41 баллов.

 Оценка «3» ставится в случае, если по результатам тестирования набрано 26-35 баллов.

 Оценка «2» ставится в случае, если по результатам тестирования набрано 0-25 баллов..

## 6.Литература

1. Спирина М.С.,Спирин П.А.Дискретная математика:учебник: Рекомендовано ГОУВПО «МГТУ им. Н. Э. Баумана» для студентов СПО. — 2014, — 368 c.
2. ГОСТ Р 34.311-95 Информационная технология. Криптографическая защита информации. Функция хэширования» - российский криптографический стандарт, определяющий алгоритм и процедуру вычисления хеш-функции.
3. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования данных
4. ГОСТ Р34.10-94. Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма
5. ГОСТ Р34.11-94. Информационная технология. Криптографическая защита информации. Функция хэширования
6. ГОСТ Р34.10-2001. Процессы формирования и проверки электронной цифровой подписи
7. ГОСТ Р 34.10-2001. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи»)
8. Гашков С., Применко Э., Черепнев М. Криптографические методы защиты информации. – М.: Академия, 2010
9. Хохлов Г.И.Основы теории информации: учебник. — 320 c., М.: Академия, 2012 г.