Министерство науки и высшего образования РФ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Национальный исследовательский университет «МЭИ»

Направление подготовки/специальность: 01.04.02 Прикладная математика и информатика

Наименование образовательной программы: Математическое и компьютерное моделирование

Уровень образования: высшее образование - магистратура

Форма обучения: Очная

Оценочные материалы
по дисциплине
Криптографические методы защиты информации

Москва
2022

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ РАЗРАБОТАЛ:

Преподаватель	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Фролов А.Б. Идентификатор: Ref8507cb-FrolovAB-a54b01e2	А.Б. Фролов
(должность)	(подпись)	(расшифровка подписи)

СОГЛАСОВАНО:

Руководитель образовательной программы	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Черепова М.Ф. Идентификатор: R9267877e-CherepovaMF-dbb9bf1	М.Ф. Черепова
(должность, ученая степень, ученое звание)	(подпись)	(расшифровка подписи)
Заведующий выпускающей кафедры	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Зубков П.В. Идентификатор: R4920bc6f-ZubkovPV-8172426c	П.В. Зубков
(должность, ученая степень, ученое звание)	(подпись)	(расшифровка подписи)

ОБЩАЯ ЧАСТЬ

Оценочные материалы по дисциплине предназначены для оценки: достижения обучающимися запланированных результатов обучения по дисциплине, этапа формирования запланированных компетенций и уровня освоения дисциплины.

Оценочные материалы по дисциплине включают оценочные средства для проведения мероприятий текущего контроля успеваемости и промежуточной аттестации.

Формируемые у обучающегося компетенции:

1. ПК-1 Способен разрабатывать и исследовать математические модели естествознания и технологий, а также осуществлять их компьютерную реализацию

ИД-3 Демонстрирует знание терминологии, основных понятий и методов решения и компьютерного моделирования прикладных задач

ИД-6 Разрабатывает и исследует алгоритмы компьютерного моделирования прикладных задач

ИД-7 Проводит компьютерное моделирование прикладных задач и анализирует его результаты

и включает:

для текущего контроля успеваемости:

Форма реализации: Билеты (письменный опрос)

1. Асимметричное шифрование и электронная подпись (Тестирование)
2. Блочные шифры и функции хеширования (Тестирование)
3. Протоколы с нулевым разглашением. Аутентификация с нулевым разглашением секрета. Скрытая передача (Тестирование)

Форма реализации: Письменная работа

1. Формальные модели шифров. Свойства криптографических преобразований (Решение задач)

БРС дисциплины

2 семестр

Раздел дисциплины	Веса контрольных мероприятий, %				
	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
	Срок КМ:	4	8	12	15
Криптография и ее задачи. Формальные модели шифров					
Криптография и ее задачи. Формальные модели шифров		+			
Свойства криптографических преобразований и их компьютерный анализ					
Свойства криптографических преобразований и их компьютерный анализ		+			
Блочные системы шифрования					
Блочные системы шифрования			+		

Функции и алгоритмы хеширования				
Хеш-функции и их применение		+		
Асимметричные криптосистемы				
Асимметричные криптосистемы			+	
Электронная цифровая подпись				
Электронная цифровая подпись			+	
Аутентификация с нулевым разглашением секрета. Скрытая передача				
Аутентификация с нулевым разглашением секрета. Скрытая передача				+
Управление ключами. Ключевые системы беспроводных сенсорных сетей				
Управление ключами. Ключевые системы беспроводных сенсорных сетей				+
Вес КМ:	25	25	25	25

$Общая часть/Для промежуточной аттестации$

СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ТЕКУЩЕГО КОНТРОЛЯ

I. Оценочные средства для оценки запланированных результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Индекс компетенции	Индикатор	Запланированные результаты обучения по дисциплине	Контрольная точка
ПК-1	ИД-З$_{ПК-1}$ Демонстрирует знание терминологии, основных понятий и методов решения и компьютерного моделирования прикладных задач	Знать: основные задачи криптографии, формальные модели шифров; основные свойства криптографических преобразований; перемешивающие свойства отображений Уметь: строить формальные модели шифров, преобразования Фурье и Уолша-Адамара булевых функций, статистическую структуру булевой функции, вычислять расстояние между булевыми функциями	Формальные модели шифров. Свойства криптографических преобразований (Решение задач)
ПК-1	ИД-6$_{ПК-1}$ Разрабатывает и исследует алгоритмы компьютерного моделирования прикладных задач	Знать: формальное определение, структуру и режимы использования блочного шифра и методы	Блочные шифры и функции хеширования (Тестирование)

		построения функций хеширования; отечественные и зарубежные стандарты блочных шифров и функций хеширования Уметь: строить структурные элементы блочного шифра и криптографических функций хеширования	
ПК-1	ИД-7$_{ПК-1}$ Проводит компьютерное моделирование прикладных задач и анализирует его результаты	Знать: основные методы асимметричного шифрования; гибридную схему шифрования; схемы электронной подписи типа Эль-Гамаля и Шнорра; отечественные и зарубежные стандарты электронной подписи протоколы аргументации и доказательства с нулевым разглашением; способы распределения ключевой информации в компьютерной сети Уметь: моделировать схемы шифрования RSA, Рабина и Эль-Гамаля, электронной подписи типа Эль-Гамаля и Шнорра и анализировать	Асимметричное шифрование и электронная подпись (Тестирование) Протоколы с нулевым разглашением. Аутентификация с нулевым разглашением секрета. Скрытая передача (Тестирование)

		их стойкость моделировать протоколы аргументации с нулевым разглашением, протоколы доказательства с нулевым разглашением и протоколы распределения ключевой информации в компьютерной сети	

II. Содержание оценочных средств. Шкала и критерии оценивания

КМ-1. Формальные модели шифров. Свойства криптографических преобразований

Формы реализации: Письменная работа
Тип контрольного мероприятия: Решение задач
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Письменная работа проводится по вариантам. Работа содержит 4 задания на 20 минут

Краткое содержание задания:
Решением задач проверяется знание основных задач криптографии, формальных моделей шифров; основных свойств криптографических преобразований; перемешивающих свойств отображений и умения строить формальные модели шифров, преобразования Фурье и Уолша-Адамара булевых функций, статистическую структуру булевой функции, вычислять расстояние между булевыми функциями.

Контрольные вопросы/задания:

Знать: основные задачи криптографии, формальные модели шифров; основные свойства криптографических преобразований; перемешивающие свойства отображений	1.Конфиденциальность — это защита информации, при которой • - скрывается факт ее передачи, - она передается по открытому каналу связи, - она не может трансформироваться при передаче, - она не может быть переадресована. 2.Целостность информации обеспечивается сопровождением ее кодом аутентификации, который позволяет выявить - искажение переданного сообщения, подмену переданного сообщения, - содержание сообщения. 3.Аутентификация — это проверка целостности сообщения с использованием идентификатора пользователя, в роли которого может быть • - ключ проверки цифровой подписи, • - адрес электронной почты, • - номер мобильного телефона. 4.Алгебраическая модель шифра задается • - тремя множествами и двумя отображениями. - пятью множествами. - пятью отображениями. 5.Вероятностная модель шифра задается - тремя множествами, двумя отображениями и двумя вероятностными распределениями, - семью множествами, - пятью множествами и двумя вероятностными распределениями. 6.Разложение булевой функции, по которому

	определяется ее спектр это - разложение в ряд Фурье, - преобразование Уолша-Адамара, - статистическая структура булевой функции. 7.Привести примеры бент-функций - от 6-и переменных, - от 8 переменных. 8.Нелинейность булевой функции определяется - наибольшей степенью монома ее полинома Жегалкина, - числом нелинейных членов полинома Жегалкина, • - расстоянием до множества аффинных функций 9.Группой инерции функции в группе G называется • - множество подстановок на ее области определения, сохраняющих значение функции, • - множество двоичных наборов, на которых функция имеет значение 1, • - множество двоичных наборов, на которых функция имеет значение 0.
Уметь: строить формальные модели шифров, преобразования Фурье и Уолша-Адамара булевых функций, статистическую структуру булевой функции, вычислять расстояние между булевыми функциями	1.Построить статистическая структуру булевой функции 4-х переменных, 2.Построить преобразование Уолша-Адамара булевой функции от 4-хпеременных. 3.Построить формальную модель блочного шифра. 4.Построить исполнимую модель шифра простой замены - в кольце Z_{143} (шифр RSA), - в кольце Z_{143}(шифр Рабина), - в кольце Z_{143}(шифр Цезаря), 5.Построить шифр перестановки - на множестве Z32 (DES P); - на множестве Z56(DES в алгоритме развертки ключа); - на множестве - Z32 (Магма, функция *f*). 6.Построить шифр перестановки - блока S_1 в схеме Фейстеля шифратора «Магма», - блока S_2 в схеме Фейстеля шифратора «Магма», - блока S_8 в схеме Фейстеля шифратора «Магма». 7.Построить модель поточного шифра - для криптосистемы Блюма-Гольдвассер, - гаммирования в кольце Z_8. 8.Построить композицию -шифров RSA и Рабина в кольце Z143. -шифров Цезаря и Рабина в кольце Z143. -шифра перестановки на множестве Z56 (DES в алгоритме развертки ключа) и его же. 9.Для заданной булевой функции от 6-и переменных построить - преобразование Фурье, - преобразование Адамара,

	- статистическую структуру. 10.Вычислить для заданной функции от 6-и переменных • - расстояние до класса аффинных функций, - расстояние до класса линейных функций. 11.Применить схему Грина вычисления коэффициентов преобразования Уолша-Адамара - булевой функции от 4-х переменных, - булевой функции от 5-и переменных.

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 75
Описание характеристики выполнения знания: Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно

Оценка: 4
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Оценка "хорошо" выставляется если большинство вопросов раскрыто. Выбрано верное направление для решения задач.

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено.

КМ-2. Блочные шифры и функции хеширования

Формы реализации: Билеты (письменный опрос)
Тип контрольного мероприятия: Тестирование
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Проводится на практическом занятии, продолжительность выполнения работы 20 минут. Студентам выдаётся один вариант заданий.

Краткое содержание задания:
Тестированием проверяется знание формального определения, структуры и режимов использования блочного шифра и методов построения функций хеширования; отечественных и зарубежных стандартов блочных шифров и функций хеширования и умение строить структурные элементы блочного шифра и криптографических функций хеширования

Контрольные вопросы/задания:

Знать: формальное определение, структуру и режимы использования блочного шифра и методы построения функций хеширования; отечественные и зарубежные стандарты блочных шифров и функций хеширования	1.Формальное определение блочного шифра это пара отображений, - множества *n* разрядных векторов открытого текста в множество *n* разрядных векторов шифр текста и множества *n* разрядных векторов шифр текста в множество *n* разрядных векторов открытого текста, - декартова произведения множества *m*-разрядных ключей и множества *n*-разрядных векторов открытого текста в множество и множества *n* разрядных векторов шифр текста и декартова

	произведения множества *m*-разрядных ключей и множества n-разрядных векторов шифртекста в множество n разрядных векторов открытого текста. - декартова произведения множества *m*-разрядных ключей и множества n-разрядных векторов открытого текста в множество и множества *n* разрядных векторов шифр текста и декартова произведения множества m-разрядных ключей и множества n-разрядных векторов шифртекста в множество n разрядных векторов открытого текста с трудно решаемыми задачами определения открытого текста по шифртексту при знании определенного множества пар таких текстов, а также ключа признании определенного множества таких пар. 2.Структурой блочного шифра не предусматриваются - раундовые преобразования сетью Фейстеля, - последовательные применения некоторого числа подстановок и перестановок (SP-сеть), - сложные одно раундовые преобразования. 3.Российским стандартом не предусматривается режим использования блочного шифра - простой замены, • - простой замены с зацеплением, - обратной связи по шифртексту, - обратной связи по выходу, • m-битной обратной связи по шифртексту. 4.Американским стандартом DES определен размер ключа -64 бит, -56 бит, -128 бит. 5.В стандарт ГОСТ Р 34.12-2015 включен алгоритм ГОСТ 28147-89 под названием -«Кузнечик», -«Магма», -«Стрибог». 6.Результат бесключевой функции хеширования это • - код целостности сообщения, • - код аутентичности сообщения, - имитовставка. 7.Результат ключевой функции хеширования это • - код целостности сообщения, • - код аутентичности сообщения, - дайджест сообщения. 8.Бесключевая функция хеширования это -отображение двоичной последовательности произвольной длины в множество бинарных наборов фиксированной длины *n*.

	- однонаправленное отображение двоичной последовательности произвольной длины в множество бинарных наборов фиксированной длины *n*. - однонаправленное отображение двоичной последовательности произвольной длины в множество бинарных наборов фиксированной длины *n* с труднорешаемой проблемой создания коллизии, - однонаправленное отображение двоичной последовательности произвольной длины в множество бинарных наборов фиксированной длины *n* с труднорешаемыми проблемами создания коллизии и построения второго прообраза. 9.Алгоритм функции хеширования по ГОСТ Р 34.11-94 реализован на основе подхода - Матиаса-Мейера-Осеаса, - Микаэля-Рабина, • - Дэвиса-Майера, • - Миягучи-Принеля. 10.Ключевая функция хеширования HMAC вычисляет код аутентичности сообщения за время, превышающее время вычисления кода целостности бесключевой функцией хеширования - в два раза, • - в три раза, - в четыре раза.
Уметь: строить структурные элементы блочного шифра и криптографических функций хеширования	1.Написать программы для ЭВМ, реализующую перестановки S_1, $S_{\neg 2}$… или S_8 сети Фейстеля шифратора «Магма» по заданному номеру перестановки. 2.Построить последовательность элементов $\omega_0,\ \omega_1$, по алгоритму режима блочного шифра с гарантированным периодом гаммы при малом размере блока (4 вместо 32) и убедитесь, что эта последовательность имеет период $2^4 * (2^4 - 1) = 240$. 3.Построить генератор последовательности элементов $\omega_0,\ \omega_1$ по алгоритму режима блочного шифра с гарантированным периодом гаммы при реальном размере блока. 4.Написать программу развертки ключа алгоритма Магма. 5.Написать программу линейного преобразования L алгоритма «Кузнечик»

Описание шкалы оценивания:

Оценка: 5

Нижний порог выполнения задания в процентах: 70

Описание характеристики выполнения знания: Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно

Оценка: 4
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

КМ-3. Асимметричное шифрование и электронная подпись

Формы реализации: Билеты (письменный опрос)
Тип контрольного мероприятия: Тестирование
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Письменный опрос проводится на практическом занятии, продолжительность выполнения работы 20 минут. Студентам выдаётся один вариант заданий.

Краткое содержание задания:
Тестированием проверяется знание основных методов асимметричного шифрования; гибридной схемы шифрования; схемы электронной подписи типа Эль-Гамаля и Шнорра; отечественных и зарубежных стандартов электронной подписи и умение моделировать схемы шифрования RSA, Рабина и Эль-Гамаля, электронной подписи типа Эль-Гамаля и Шнорра и анализировать их стойкость.

Контрольные вопросы/задания:

Знать: основные методы асимметричного шифрования; гибридную схему шифрования; схемы электронной подписи типа Эль-Гамаля и Шнорра; отечественные и зарубежные стандарты электронной подписи	1.Теоретически стойкими являются криптосистемы - Эль-Гамаля и RSA, - Рабина и RSA, - Рабина и Эль-Гамаля. 2.Теоретически стойкими считаются асимметричные криптосистемы, криптографические системы, стойкость которых определяется трудностью проблемы -целочисленной факторизации, -дискретного логарифмирования, Диффи-Хеллмана. 3.Мультипликативное свойство криптосистемы RSA не допускает - успешную атаку по выбираемому шифртексту, - вскрытие секретного ключа, - создание нового подписанного сообщения по цифровым подписям. 4.Первым элементом шифртекста гибридной системы шифрования является - инкапсулированная разовый ключ U, - разовый ключ K, - разовый ключ аутентификации K_a.
Уметь: моделировать схемы шифрования RSA, Рабина и Эль-	1.Построить исполнимую спецификацию криптосистемы RSA.

Гамаля, электронной подписи типа Эль-Гамаля и Шнорра и анализировать их стойкость	2.Построить исполнимую спецификацию криптосистемы Эль Гамаля. 3.Построить исполнимую спецификацию цифровой подписи Эль Гамаля..

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно

Оценка: 4
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

КМ-4. Протоколы с нулевым разглашением. Аутентификация с нулевым разглашением секрета. Скрытая передача

Формы реализации: Билеты (письменный опрос)
Тип контрольного мероприятия: Тестирование
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Письменный опрос проводится на практическом занятии, продолжительность выполнения работы 20 минут. Студентам выдаётся один вариант заданий.

Краткое содержание задания:
Тестированием проверяется знание протоколов аргументации и доказательства с нулевым разглашением; способов распределения ключевой информации в компьютерной сети и умение моделировать протоколы аргументации с нулевым разглашением, протоколы доказательства с нулевым разглашением и протоколы распределения ключевой информации в компьютерной сети

Контрольные вопросы/задания:

Знать: протоколы аргументации и доказательства с нулевым разглашением; способы распределения ключевой информации в компьютерной сети	1.Протоколом доказательства с нулевым разглашение является - протокол Шнорра, - протокол Фиата-Шамира, - протокол доказательства квадратичного вычета. 2.Протоколом аргументации с нулевым разглашение является - протокол Шнорра, - протокол доказательства квадратичного невычета, - протокол доказательства квадратичного вычета. 3.Протоколом доказательства или аргументации с нулевым разглашением и двусторонней ошибкой является - протокол доказательства квадратичного невычета,

	- протокол доказательства квадратичного вычета, - протокол доказательства, что составное число имеет только два множителя. 4.Устойчивость δ протокола с нулевым разглашением зависит - от числа раундов запрос-ответ, - порядка алгебраической структуры, - открытого ключа. 5.Протоколы с нулевым разглашением секрета используются для - идентификации участников, - шифрования данных, - обеспечения целостности сообщения.
Уметь: моделировать протоколы аргументации с нулевым разглашением, протоколы доказательства с нулевым разглашением и протоколы распределения ключевой информации в компьютерной сети	1.Построить исполнимую спецификацию протокола аргументации о знании дискретного логарифма. 2.Построить исполнимую спецификацию протокола аргументации о знании квадратного корня по модулю составного числа. 3.Построить исполнимую спецификацию протокола доказательства знания квадратичного вычета. 4.Построить исполнимую спецификацию протокола забывающей передачи.

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно

Оценка: 4
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

2 семестр

Форма промежуточной аттестации: Экзамен

Пример билета

Вопрос 1. Разложения булевых функций, статистическая структура и статистические аналоги булевых функций.
Вопрос 2. Российский стандарт хеш-функции ГОСТ Р 34.11-94. Функция «Стрибог» ГОСТ Р 34.11-2-2012.
Вопрос. 3. Возможны ли следующие две различные подписи Эль Гамаля под разными сообщениями (105,1111111111111111), (105,11111110111111111)?
а. возможны,
б. не возможны.

Процедура проведения

Экзамен проводится в письменно-устной форме. На подготовку ответа дается 60 минут. Кроме ответа на вопросы билета, студент должен ответить на дополнительные вопросы.

I. Перечень компетенций/индикаторов и контрольных вопросов проверки результатов освоения дисциплины

1. Компетенция/Индикатор: ИД-З$_{ПК-1}$ Демонстрирует знание терминологии, основных понятий и методов решения и компьютерного моделирования прикладных задач

Вопросы, задания

1.Алгебраическая и вероятностная модели шифра.
2. Шифры простой замены и перестановки.
3.Разложения булевых функций, статистическая структура и статистические аналоги булевых функций, расстояние между булевыми функциями.
4.Строгий лавинный критерий. Критерий распространения.
5.Сильная равновероятость булевых функций.
6.Перемешивающие свойства отображений.
7.Криптоанализ блочных систем шифрования: метод компромисса «время-объем памяти», дифференциальный криптоанализ.
8.Понятие криптографической хеш-функции. Бесключевые и ключевые хеш-функции и их свойства.
9.Понятие, назначение и необходимые свойства цифровой подписи.
10.Общая характеристика протоколов с нулевым разглашением секрета. Полнота и устойчивость.
11.Ключевые системы беспроводных сенсорных сетей.
12.Построить статистическая структуру булевой функции 4-х переменных,
13.Построить преобразование Уолша-Адамара булевой функции от 4-хпеременных.
14.Построить формальную модель блочного шифра.
15.Построить исполнимую модель шифра простой замены
- в кольце Z143 (шифр RSA),
- в кольце Z143(шифр Рабина),
- в кольце Z143(шифр Цезаря),
16.Построить шифр перестановки
- на множестве Z32 (DES P);

- на множестве Z56(DES в алгоритме развертки ключа);
- на множестве - Z32 (Магма, функция *f*).

17.Построить шифр перестановки
- блока S1 в схеме Фейстеля шифратора «Магма»,
- блока S2 в схеме Фейстеля шифратора «Магма»,
- блока S8 в схеме Фейстеля шифратора «Магма».

Материалы для проверки остаточных знаний

1.Конфиденциальность — это защита информации, при которой

Ответы:

- скрывается факт ее передачи, - она передается по открытому каналу связи, - она не может трансформироваться при передаче, - она не может быть переадресована.

Верный ответ: - она передается по открытому каналу связи

2.Целостность информации обеспечивается сопровождением ее кодом аутентификации, который позволяет выявить

Ответы:

- искажение переданного сообщения, - подмену переданного сообщения, - содержание сообщения.

Верный ответ: - искажение переданного сообщения

3.Разложение булевой функции, по которому определяется ее спектр это

Ответы:

- разложение в ряд Фурье, - преобразование Уолша-Адамара, - статистическая структура булевой функции.

Верный ответ: - разложение в ряд Фурье

4.Статистическая структура булевой функции дает информацию

Ответы:

- о линейных статистических аналогах функции, - о расстоянии между функциями, - о спектре булевой функции.

Верный ответ: - о линейных статистических аналогах функции

5.Результат бесключевой функции хеширования это

Ответы:

- код целостности сообщения, - код аутентичности сообщения, - имитовставка.

Верный ответ: - код целостности сообщения

6.Аутентификация — это проверка целостности сообщения с использованием идентификатора пользователя, в роли которого может быть

Ответы:

- ключ проверки цифровой подписи, - адрес электронной почты, - номер мобильного телефона.

Верный ответ: - ключ проверки цифровой подписи,

7.Булева функция сильно равновероятна тогда и только тогда, когда

Ответы:

- она сбалансирована, - отсутствуют запреты, - она m-равновероятна.

Верный ответ: - отсутствуют запреты,

8.Нелинейность булевой функции определяется

Ответы:

- наибольшей степенью монома ее полинома Жегалкина, - числом нелинейных членов полинома Жегалкина, - расстоянием до множества аффинных функций.

Верный ответ: - расстоянием до множества аффинных функций.

9.Группой инерции функции в группе G называется

Ответы:

- множество подстановок на ее области определения, сохраняющих значение функции, - множество двоичных наборов, на которых функция имеет значение 1, - множество двоичных наборов, на которых функция имеет значение 0.

Верный ответ: - множество подстановок на ее области определения, сохраняющих значение функции,

10.При определении перемешивающего свойства отображения используются

Ответы:

- его координатные функции, - статистические спектры координатных функций, - статистические структуры координатных функций.

Верный ответ: - его координатные функции,

11.Мультипликативное свойство криптосистемы RSA не допускает

Ответы:

- успешную атаку по выбираемому шифртексту, - вскрытие секретного ключа, - создание нового подписанного сообщения по цифровым подписям.

Верный ответ: - вскрытие секретного ключа,

2. Компетенция/Индикатор: ИД-6$_{ПК-1}$ Разрабатывает и исследует алгоритмы компьютерного моделирования прикладных задач

Вопросы, задания

1.Принципы построения блочных систем шифрования. Схема Фейстеля.

2.Примеры блочных систем шифрования: стандарты шифрования DES, «Магма» ГОСТ 28147-89, AES, «Кузнечик» ГОСТ Р34.12-2015.

3.Режимы использования блочных шифров. Код аутентификации сообщения.

4.Российский стандарт хеш-функции ГОСТ Р 34.11-94. Функция «Стрибог» ГОСТ Р 34.11-2-2012.

5.KDP-схема предварительного распределения ключей.

6.Протоколы распределения ключей с использованием симметричной криптосистемы. Протокол Нидмэн-Шроедера.

7.Схема Блома распределения ключей. Условия безопасности использования при компрометации части ключевого материала.

8.Написать программы для ЭВМ, реализующую перестановки S1, S2… или S8 сети Фейстеля шифратора «Магма» по заданному номеру перестановки.

9.Построить последовательность элементов ω0, ω1, по алгоритму режима блочного шифра с гарантированным периодом гаммы при малом размере блока (4 вместо 32) и убедитесь, что эта последовательность имеет период 24*(24-1)=240.

10.Построить генератор последовательности элементов ω0, ω1 по алгоритму режима блочного шифра с гарантированным периодом гаммы при реальном размере блока.

11.Написать программу развертки ключа алгоритма Магма.

12.Написать программу линейного преобразования L алгоритма «Кузнечик»

Материалы для проверки остаточных знаний

1.Структурой блочного шифра не предусматриваются

Ответы:

- раундовые преобразования сетью Фейстеля, - последовательные применения некоторого числа подстановок и перестановок (SP-сеть), - сложные одно раундовые преобразования.

Верный ответ: - сложные одно раундовые преобразования

2.Стойкость схемы проверяемого секрета

Ответы:

- безусловна, - определяется трудностью проблемы целочисленной факторизации, - трудностью проблемы дискретного логарифмирования.

Верный ответ: трудностью проблемы дискретного логарифмирования

3.Российским стандартом не предусматривается режим использования блочного шифра

Ответы:

- простой замены, - простой замены с зацеплением, - обратной связи по шифртексту, - обратной связи по выходу, - m-битной обратной связи по шифртексту.

Верный ответ: - m-битной обратной связи по шифртексту.

4.Американским стандартом DES определен размер ключа

Ответы:

- 64 бит, - 56 бит, - 128 бит.

Верный ответ: - 56 бит,

5.В стандарт ГОСТ Р 34.12-2015 включен алгоритм ГОСТ 28147-89 под названием

Ответы:

- «Кузнечик», - «Магма», - «Стрибог».

Верный ответ: - «Магма»,

6.Результат ключевой функции хеширования это

Ответы:

- код целостности сообщения, - код аутентичности сообщения, - дайджест сообщения.

Верный ответ: - код аутентичности сообщения,

7.Алгоритм функции хеширования по ГОСТ Р 34.11-94 реализован на основе подхода

Ответы:

- Матиаса-Мейера-Осеаса, - Микаэля-Рабина, - Дэвиса-Майера, - Миягучи-Принеля.

Верный ответ: - Матиаса-Мейера-Осеаса,

8.Ключевая функция хеширования HMAC вычисляет код аутентичности сообщения за время, превышающее время вычисления кода целостности бесключевой функцией хеширования

Ответы:

- в два раза, - в три раза, - в четыре таза.

Верный ответ: - в два раза,

3. Компетенция/Индикатор: ИД-7$_{ПК-1}$ Проводит компьютерное моделирование прикладных задач и анализирует его результаты

Вопросы, задания

1.Криптосистема RSA, особенности выбора параметров, использование в компьютерной сети. Цифровая подпись RSA. Атака по выбираемому шифртексту.

2.Криптосистема Рабина, ее теоретическая стойкость и условия однозначности расшифрования.

3.Криптосистема Эль Гамаля, условия безопасности использования. Реализация в мультипликативной группе конечного поля и в группе точек эллиптической кривой.

4.Цифровая подпись Эль Гамаля. Условия безопасного использования. Реализация в мультипликативной и аддитивной группах.

5.Особенности Российского ГОСТ Р 34.11-2-2012 и американского ECDSA стандартов цифровой подписи.

6.Цифровая подпись Эль Гамаля. Криптографическая стойкость. Особенности использования рандомизатора и хеш-функции.

7.Цифровая подпись с личностным ключом проверки.

8.Цифровая подпись с возвратом сообщения. Электронная подпись ГОСТ Р. 34.10-2012.

9.Протоколы аутентификации при ограниченных вычислительных возможностях доказывающего: доказательство знания дискретного логарифма, протокол Фиата-Шамира, протокол Шнорра.

10.Протоколы аутентификации при неограниченных возможностях доказывающего: доказательство знания квадратичного вычета или квадратичного невычета.

11.Протоколы распределения ключей по открытым каналам: протокол Диффи-Хеллмана, протокол Месси-Омуры, MQV-протокол.
12.Построить исполнимую спецификацию криптосистемы RSA.
13.Построить исполнимую спецификацию криптосистемы Эль Гамаля.
14.Построить исполнимую спецификацию цифровой подписи Эль Гамаля..
15.Построить исполнимую спецификацию протокола аргументации о знании дискретного логарифма.
16.Построить исполнимую спецификацию протокола аргументации о знании квадратного корня по модулю составного числа.
17.Построить исполнимую спецификацию протокола доказательства знания квадратичного вычета.
18.Построить исполнимую спецификацию протокола забывающей передачи.

Материалы для проверки остаточных знаний

1.Теоретически стойкими являются криптосистемы
Ответы:
- Эль-Гамаля и RSA, - Рабина и RSA, - Рабина и Эль-Гамаля.
Верный ответ: - Рабина и RSA

2.Электронная подпись RSA не удовлетворяет требованию невозможности
Ответы:
- подделки подписи, - создания подписанного сообщения - подмены сообщения.
Верный ответ: - создания подписанного сообщения

3.Протоколом доказательства с нулевым разглашением является
Ответы:
- протокол Шнорра, - протокол Фиата-Шамира, - протокол доказательства квадратичного вычета.
Верный ответ: протокол доказательства квадратичного вычета

4.Теоретически стойкими считаются асимметричные криптосистемы, криптографические системы, стойкость которых определяется трудностью проблемы
Ответы:
- целочисленной факторизации, - дискретного логарифмирования, - Диффи-Хеллмана.
Верный ответ: - целочисленной факторизации,

5.Криптографическая стойкости цифровой подписи Эль-Гамаля эквивалента стойкости проблемы
Ответы:
- дискретного логарифмирования, - целочисленной факторизации, - квадратичного вычета.
Верный ответ: - дискретного логарифмирования,

II. Описание шкалы оценивания

Оценка: 5
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Оценка «ОТЛИЧНО» выставляется студенту, правильно выполнившему практическое задание, который показал при ответе на вопросы экзаменационного билета, и на дополнительные вопросы, что владеет материалом изученной дисциплины, свободно применяет свои знания для объяснения различных явлений и решения задач.

Оценка: 4
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Оценка «ХОРОШО» выставляется студенту, правильно выполнившему практическое задание и в основном правильно ответившему на

вопросы экзаменационного билета и на дополнительные вопросы, но допустившему при этом непринципиальные ошибки.

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка «УДОВЛЕТВОРИТЕЛЬНО» выставляется студенту, который в ответах на вопросы экзаменационного билета допустил существенные и даже грубые ошибки, но затем исправил их сам, а также не выполнил практическое задание из экзаменационного билета, но либо наметил правильный путь его выполнения, либо по указанию экзаменатора решил другую задачу из того же раздела дисциплины.

III. Правила выставления итоговой оценки по курсу

Оценка определяется в соответствии с Положением о балльно-рейтинговой системе для студентов НИУ «МЭИ» на основании семестровой и экзаменационной составляющих.