МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное учреждение
высшего профессионального образования
"Казанский (Приволжский) федеральный университет"
Высшая школа информационных технологий и информационных систем

УТВЕРЖДАЮ
Проректор
по образовательной деятельности КФУ
Проф. Минзарипов Р.Г.
_____
"___"_____20___ г.

Программа дисциплины

Криптография с открытым ключом Б3.ДВ.6

Направление подготовки: 230700.62 - Прикладная информатика
Профиль подготовки: Прикладная информатика в экономике
Квалификация выпускника: бакалавр
Форма обучения: очное
Язык обучения: русский
Автор(ы):
Лернер Э.Ю.
Рецензент(ы):
Кугураков В.С.

СОГЛАСОВАНО:
Заведующий(ая) кафедрой: Миссаров М. Д.
Протокол заседания кафедры No ___ от "____" _____ 201__г
Учебно-методическая комиссия Высшей школы информационных технологий и информационных систем:
Протокол заседания УМК No ____ от "____" _____ 201__г

Регистрационный No

Казань
2015

Содержание

Программу дисциплины разработал(а)(и) доцент, к.н. (доцент) Лернер Э.Ю. кафедра анализа данных и исследования операций отделение фундаментальной информатики и информационных технологий , Eduard.Lerner@gmail.com

1. Цели освоения дисциплины

Курс "Криптография систем с открытым ключом" предназначен для студентов 4 курса направления "Прикладная информатика". Он направлен на проверенное собственной программной реализацией знание теоретических основ и практических аспектов систем с открытым ключом, являющихся фундаментом современной электронной коммерции. Знания, полученные в рамках курса, существенно повысят ценность специалиста.

2. Место дисциплины в структуре основной образовательной программы высшего профессионального образования

Данная учебная дисциплина включена в раздел " Б3.ДВ.6 Профессиональный" основной образовательной программы 230700.62 Прикладная информатика и относится к дисциплинам по выбору. Осваивается на 4 курсе, 8 семестр.

Данная дисциплина опирается на дисциплины "Информатика и программирование", "Математика 1", "Теория вероятностей и математическая статистика", полезным является знакомство с основами курса по выбору "Моделирование с пакетом Mathematica".

3. Компетенции обучающегося, формируемые в результате освоения дисциплины /модуля

В результате освоения дисциплины формируются следующие компетенции:

Шифр компетенции	Расшифровка приобретаемой компетенции
ОК-5 (общекультурные компетенции)	способен самостоятельно приобретать и использовать в практической деятельности новые знания и умения, стремиться к саморазвитию
ОК-6 (общекультурные компетенции)	способен осознавать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности
ОК-7 (общекультурные компетенции)	способен понимать сущность и проблемы развития современного информационного общества
ПК-4 (профессиональные компетенции)	способен ставить и решать прикладные задачи с использованием современных информационно-коммуникационных технологий
ПК-8 (профессиональные компетенции)	способен проводить обследование организаций, выявлять информационные потребности пользователей, формировать требования к информационной системе, участвовать в реинжиниринге прикладных и информационных процессов
ПК-16 (профессиональные компетенции)	способен оценивать и выбирать современные операционные среды и информационно-коммуникационные технологии для информатизации и автоматизации решения прикладных задач и создания ИС

В результате освоения дисциплины студент:

1. должен знать:

- теоретические основы систем с открытым ключом, в том числе различные фундаментальные теоретико-числовые алгоритмы.

- основные криптографические протоколы и уметь реализовывать их в тех же средах.

2. должен уметь:

- реализовывать базовые алгоритмы систем с открытым ключом в средах программирования со встроенной длинной арифметикой.

3. должен владеть:

навыками выбирать современные операционные среды и информационно-коммуникационные технологии для информатизации и автоматизации решения прикладных задач и создания ИС

4. должен демонстрировать способность и готовность:

Студенты, завершившие изучение данной дисциплины должны:

- Знать теоретические основы систем с открытым ключом, в том числе различные фундаментальные теоретико-числовые алгоритмы.
- Уметь реализовывать базовые алгоритмы систем с открытым ключом в средах программирования со встроенной длинной арифметикой.
- Знать основные криптографические протоколы и уметь реализовывать их в тех же средах.

4. Структура и содержание дисциплины/ модуля

Общая трудоемкость дисциплины составляет 4 зачетных(ые) единиц(ы) 144 часа(ов).

Форма промежуточного контроля дисциплины экзамен в 8 семестре.

Суммарно по дисциплине можно получить 100 баллов, из них текущая работа оценивается в 50 баллов, итоговая форма контроля - в 50 баллов. Минимальное количество для допуска к зачету 28 баллов.

86 баллов и более - "отлично" (отл.);

71-85 баллов - "хорошо" (хор.);

55-70 баллов - "удовлетворительно" (удов.);

54 балла и менее - "неудовлетворительно" (неуд.).

4.1 Структура и содержание аудиторной работы по дисциплине/ модулю

Тематический план дисциплины/модуля

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практические занятия	Лабораторные работы	
1.	Тема 1. Некоторые алгоритмические вопросы элементарной теории чисел. 1. Временные оценки сложности арифметических операций. Свойства функций оценки сложности (иерархия функций, символы O, □, □; операции с O). Сложность арифметических операций с целыми числами. Сложность наивных алгоритмов факторизации и проверки простоты числа. 2. Делимость. Алгоритм Евклида. Основная теорема арифметики. Сложность алгоритма Евклида. Расширенный алгоритм Евклида для решения линейных диофантовых уравнений. Доказательство основной теоремы арифметики с помощью расширенного алгоритма Евклида. 3. Модулярная арифметика. Теорема Ферма. Функция Эйлера. Теорема Эйлера. Быстрые алгоритмы возведения в степень и нахождения обратного элемента в модулярной арифметике. Китайская теорема об остатках. Реализация алгоритмов из пу	8	1-2	0	0	10	

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практические занятия	Лабораторные работы	
2.	Тема 2. 3. Рандомизированные алгоритмы проверки простоты. Связь символа Лежандра и степеней элемента. Тест Соловея-Штрассена. Вероятность ошибки. Тест Рабина проверки на простоту. Понятие о расширенной гипотезе Римана и полиномиальность детерминированного алгоритма Миллера при ее справедливости. 4. Взаимосвязь свидетелей простоты в алгоритме Миллера-Рабина, в алгоритме Ферма и в алгоритме Соловея-Штрассена. 5. Основные понятия полиномиального теста распознования простоты Агравала-Каяла-Саксены. Полиномиальная арифметика по модулю. Следствия результата Фоуври. Оценка работы алгоритма и возможности его улучшения. Реализация алгоритмов из пунктов 1, 2, 3 в системах со встроенной длинной арифметикой.	8	5-6	0	0	10	

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практические занятия	Лабораторные работы	
2.	Тема 2. Как отличить составное число от простого? 1. Математические основы. Распределение простых чисел, неравенства для (x). Понятия о более точных оценках (x), постулат Бертрана. Структура мультипликативной группы по модулю. Случай простого модуля. Разложение мультипликативной группы для любого натурального модуля на взаимно-простые составляющие: понятие о циклической группе; свойства; формулировка основной теоремы (без доказательства). Квадратичные вычеты: понятия символа Лежандра и символа Якоби; квадратичный закон взаимности; значение символа Лежандра для малых положительных и отрицательных значений; полиномиальный алгоритм нахождения символа Якоби. 2. Простейшие алгоритмы проверки на простоту. Критерий Вильсона. Тесты, основанные на малой теореме Ферма. Свойства чисел Кармайкла. Написание п	8	3-4	0	0	10	

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практические занятия	Лабораторные работы	
3.	Тема 3. Криптосистемы с открытым ключом. 1. Математические основы. Обобщение теоремы Эйлера. Дискретное логарифмирование, сравнение трудоемкости дискретного логарифмирования и возведения в степень. 2. Теория и практика криптоситем с открытым ключом. Суть криптографии с открытым ключом: односторонние функции, функции с секретом, понятия открытого и закрытого ключа. Криптосистема RSA. Практические ограничения, накладываемы на параметры системы RSA. ?Подводные камни? криптосистемы RSA. Примеры работы системы. Криптосистема Эль-Гамаля. Криптоситема Мэсси-Омуры для передачи сообщений. 3. Генерация случайных чисел. Мультипликативные и конгруэнтные датчики случайных чисел. Их всевозможные обобщения ? датчики Фибоначчи, датчики вычитания с заимствованием и сложения с переносом. Быстрота работы и криптографическая неуст	8	7-10	0	0	10	

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практические занятия	Лабораторные работы	
4.	Тема 4. 4. Протоколы разделения секрета между несколькими участниками. Протокол, основанный на сложение по модулю два. Протокол, основанный на китайской теореме об остатках. 5. Протоколы доказательств с нулевым разглашением. Основы доказательств с нулевым разглашением. Протоколы доказательств для задач изоморфизма графов и гамильтонова цикла и раскраски в 3 цвета. Протоколы доказательств для задачи дискретного логарифма и вскрытия RSA. Реализация всех рассматриваемых протоколов.	8	15-18	0	0	10	

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практические занятия	Лабораторные работы	
4.	Тема 4. Основные криптографические протоколы. 1. Протокол Диффи-Хеллмана выработки общего секрета. Атака посредника. ?Подводные камни? реализации. Надежные простые числа. Использование подгрупп меньшего размера. Размер p. Практические правила. Что может пойти не так. Алгоритм Диффи-Хелмана с тремя и более участниками. Обобщение алгоритма на коммутативные кольца. 2. Протоколы аутентификации и цифровой подписи. Схема подписи в системе RSA. Подписи, основанные на односторонних функциях. Схема аутентификации Шнорра и ее ?подводные камни?. Схема цифровой подписи Шнорра. 3. Протокол подбрасывания монеты по телефону.	8	11-14	0	0	10	
5.	Тема 5. Подготовка к экзамену	8		0	0	0	
.	Тема . Итоговая форма контроля	8		0	0	0	экзамен
	Итого			0	0	60	

4.2 Содержание дисциплины

Тема 1. Некоторые алгоритмические вопросы элементарной теории чисел. 1. Временные оценки сложности арифметических операций. Свойства функций оценки сложности (иерархия функций, символы O, □ , □ ; операции с O). Сложность арифметических операций с целыми числами. Сложность наивных алгоритмов факторизации и проверки простоты числа. 2. Делимость. Алгоритм Евклида. Основная теорема арифметики. Сложность алгоритма Евклида. Расширенный алгоритм Евклида для решения линейных диофантовых уравнений. Доказательство основной теоремы арифметики с помощью расширенного алгоритма Евклида. 3. Модулярная арифметика. Теорема Ферма. Функция Эйлера. Теорема Эйлера. Быстрые алгоритмы возведения в степень и нахождения обратного элемента в модулярной арифметике. Китайская теорема об остатках. Реализация алгоритмов из пунктов 2, 3 в системах со встроенной длинной арифметикой.

лабораторная работа (10 часа(ов)):

1. Временные оценки сложности арифметических операций. Свойства функций оценки сложности (иерархия функций, символы O, □, □; операции с O). Сложность арифметических операций с целыми числами. Сложность наивных алгоритмов факторизации и проверки простоты числа. 2. Делимость. Алгоритм Евклида. Основная теорема арифметики. Сложность алгоритма Евклида. Расширенный алгоритм Евклида для решения линейных диофантовых уравнений. Доказательство основной теоремы арифметики с помощью расширенного алгоритма Евклида. 3. Модулярная арифметика. Теорема Ферма. Функция Эйлера. Теорема Эйлера. Быстрые алгоритмы возведения в степень и нахождения обратного элемента в модулярной арифметике. Китайская теорема об остатках. Реализация алгоритмов из пунктов 2, 3 в системах со встроенной длинной арифметикой.

Тема 2. 3. Рандомизированные алгоритмы проверки простоты. Связь символа Лежандра и степеней элемента. Тест Соловея-Штрассена. Вероятность ошибки. Тест Рабина проверки на простоту. Понятие о расширенной гипотезе Римана и полиномиальность детерминированного алгоритма Миллера при ее справедливости. 4. Взаимосвязь свидетелей простоты в алгоритме Миллера-Рабина, в алгоритме Ферма и в алгоритме Соловея-Штрассена. 5. Основные понятия полиномиального теста распознования простоты Агравала-Каяла-Саксены. Полиномиальная арифметика по модулю. Следствия результата Фоуври. Оценка работы алгоритма и возможности его улучшения. Реализация алгоритмов из пунктов 1, 2, 3 в системах со встроенной длинной арифметикой.

лабораторная работа (10 часа(ов)):

3. Рандомизированные алгоритмы проверки простоты. Связь символа Лежандра и степеней элемента. Тест Соловея-Штрассена. Вероятность ошибки. Тест Рабина проверки на простоту. Понятие о расширенной гипотезе Римана и полиномиальность детерминированного алгоритма Миллера при ее справедливости. 4. Взаимосвязь свидетелей простоты в алгоритме Миллера-Рабина, в алгоритме Ферма и в алгоритме Соловея-Штрассена. 5. Основные понятия полиномиального теста распознования простоты Агравала-Каяла-Саксены. Полиномиальная арифметика по модулю. Следствия результата Фоуври. Оценка работы алгоритма и возможности его улучшения. Реализация алгоритмов из пунктов 1, 2, 3 в системах со встроенной длинной арифметикой.

Тема 2. Как отличить составное число от простого? 1. Математические основы. Распределение простых чисел, неравенства для □ (x). Понятия о более точных оценках □ (x), постулат Бертрана. Структура мультипликативной группы по модулю. Случай простого модуля. Разложение мультипликативной группы для любого натурального модуля на взаимно-простые составляющие: понятие о циклической группе; свойства; формулировка основной теоремы (без доказательства). Квадратичные вычеты: понятия символа Лежандра и символа Якоби; квадратичный закон взаимности; значение символа Лежандра для малых положительных и отрицательных значений; полиномиальный алгоритм нахождения символа Якоби. 2. Простейшие алгоритмы проверки на простоту. Критерий Вильсона. Тесты, основанные на малой теореме Ферма. Свойства чисел Кармайкла. Написание программы генерирующие числа Кармайкла, меньшие миллиона.

лабораторная работа (10 часа(ов)):

1. Математические основы. Распределение простых чисел, неравенства для (x). Понятия о более точных оценках (x), постулат Бертрана. Структура мультипликативной группы по модулю. Случай простого модуля. Разложение мультипликативной группы для любого натурального модуля на взаимно-простые составляющие: понятие о циклической группе; свойства; формулировка основной теоремы (без доказательства). Квадратичные вычеты: понятия символа Лежандра и символа Якоби; квадратичный закон взаимности; значение символа Лежандра для малых положительных и отрицательных значений; полиномиальный алгоритм нахождения символа Якоби. 2. Простейшие алгоритмы проверки на простоту. Критерий Вильсона. Тесты, основанные на малой теореме Ферма. Свойства чисел Кармайкла. Написание программы генерирующие числа Кармайкла, меньшие миллиона.

Тема 3. Криптосистемы с открытым ключом. 1. Математические основы. Обобщение теоремы Эйлера. Дискретное логарифмирование, сравнение трудоемкости дискретного логарифмирования и возведения в степень. 2. Теория и практика криптоситем с открытым ключом. Суть криптографии с открытым ключом: односторонние функции, функции с секретом, понятия открытого и закрытого ключа. Криптосистема RSA. Практические ограничения, накладываемы на параметры системы RSA. ?Подводные камни? криптосистемы RSA. Примеры работы системы. Криптосистема Эль-Гамаля. Криптоситема Мэсси-Омуры для передачи сообщений. 3. Генерация случайных чисел. Мультипликативные и конгруэнтные датчики случайных чисел. Их всевозможные обобщения ? датчики Фибоначчи, датчики вычитания с заимствованием и сложения с переносом. Быстрота работы и криптографическая неустойчивость всех таких датчиков. Числа Блюма и датчики Блюма. Степень их криптографической устойчивости. Реализация всех криптосистем из пункта 2.

лабораторная работа (10 часа(ов)):

1. Математические основы. Обобщение теоремы Эйлера. Дискретное логарифмирование, сравнение трудоемкости дискретного логарифмирования и возведения в степень. 2. Теория и практика криптоситем с открытым ключом. Суть криптографии с открытым ключом: односторонние функции, функции с секретом, понятия открытого и закрытого ключа. Криптосистема RSA. Практические ограничения, накладываемы на параметры системы RSA. ?Подводные камни? криптосистемы RSA. Примеры работы системы. Криптосистема Эль-Гамаля. Криптоситема Мэсси-Омуры для передачи сообщений. 3. Генерация случайных чисел. Мультипликативные и конгруэнтные датчики случайных чисел. Их всевозможные обобщения ? датчики Фибоначчи, датчики вычитания с заимствованием и сложения с переносом. Быстрота работы и криптографическая неустойчивость всех таких датчиков. Числа Блюма и датчики Блюма. Степень их криптографической устойчивости. Реализация всех криптосистем из пункта 2.

Тема 4. 4. Протоколы разделения секрета между несколькими участниками. Протокол, основанный на сложение по модулю два. Протокол, основанный на китайской теореме об остатках. 5. Протоколы доказательств с нулевым разглашением. Основы доказательств с нулевым разглашением. Протоколы доказательств для задач изоморфизма графов и гамильтонова цикла и раскраски в 3 цвета. Протоколы доказательств для задачи дискретного логарифма и вскрытия RSA. Реализация всех рассматриваемых протоколов.

лабораторная работа (10 часа(ов)):

4. Протоколы разделения секрета между несколькими участниками. Протокол, основанный на сложение по модулю два. Протокол, основанный на китайской теореме об остатках. 5. Протоколы доказательств с нулевым разглашением. Основы доказательств с нулевым разглашением. Протоколы доказательств для задач изоморфизма графов и гамильтонова цикла и раскраски в 3 цвета. Протоколы доказательств для задачи дискретного логарифма и вскрытия RSA. Реализация всех рассматриваемых протоколов.

Тема 4. Основные криптографические протоколы. 1. Протокол Диффи-Хеллмана выработки общего секрета. Атака посредника. ?Подводные камни? реализации. Надежные простые числа. Использование подгрупп меньшего размера. Размер p. Практические правила. Что может пойти не так. Алгоритм Диффи-Хелмана с тремя и более участниками. Обобщение алгоритма на коммутативные кольца. 2. Протоколы аутентификации и цифровой подписи. Схема подписи в системе RSA. Подписи, основанные на односторонних функциях. Схема аутентификации Шнорра и ее ?подводные камни?. Схема цифровой подписи Шнорра. 3. Протокол подбрасывания монеты по телефону.

лабораторная работа (10 часа(ов)):

1. Протокол Диффи-Хеллмана выработки общего секрета. Атака посредника. ?Подводные камни? реализации. Надежные простые числа. Использование подгрупп меньшего размера. Размер p. Практические правила. Что может пойти не так. Алгоритм Диффи-Хелмана с тремя и более участниками. Обобщение алгоритма на коммутативные кольца. 2. Протоколы аутентификации и цифровой подписи. Схема подписи в системе RSA. Подписи, основанные на односторонних функциях. Схема аутентификации Шнорра и ее ?подводные камни?. Схема цифровой подписи Шнорра. 3. Протокол подбрасывания монеты по телефону.

Тема 5. Подготовка к экзамену

4.3 Структура и содержание самостоятельной работы дисциплины (модуля)

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
1.	Тема 1. Некоторые алгоритмические вопросы элементарной теории чисел. 1. Временные оценки сложности арифметических операций. Свойства функций оценки сложности (иерархия функций, символы O, □, □; операции с O). Сложность арифметических операций с целыми числами. Сложность наивных алгоритмов факторизации и проверки простоты числа. 2. Делимость. Алгоритм Евклида. Основная теорема арифметики. Сложность алгоритма Евклида. Расширенный алгоритм Евклида для решения линейных диофантовых уравнений. Доказательство основной теоремы арифметики с помощью расширенного алгоритма Евклида. 3. Модулярная арифметика. Теорема Ферма. Функция Эйлера. Теорема Эйлера. Быстрые алгоритмы возведения в степень и нахождения обратного элемента в модулярной арифметике. Китайская теорема об остатках. Реализация алгоритмов из пунктов 2, 3 в системах со встроенной длинной арифметикой.	8	1-2	домашняя работа	8	устно

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
2.	Тема 2. Как отличить составное число от простого? 1. Математические основы. Распределение простых чисел, неравенства для (x). Понятия о более точных оценках (x), постулат Бертрана. Структура мультипликативной группы по модулю. Случай простого модуля. Разложение мультипликативной группы для любого натурального модуля на взаимно-простые составляющие: понятие о циклической группе; свойства; формулировка основной теоремы (без доказательства). Квадратичные вычеты: понятия символа Лежандра и символа Якоби; квадратичный закон взаимности; значение символа Лежандра для малых положительных и отрицательных значений; полиномиальный алгоритм нахождения символа Якоби. 2. Простейшие алгоритмы проверки на простоту. Критерий Вильсона. Тесты, основанные на малой теореме Ферма. Свойства чисел Кармайкла. Написание программы генерирующие числа Кармайкла, меньшие миллиона.	8	3-4	домашняя работа	8	устно

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
2.	Тема 2. 3. Рандомизированные алгоритмы проверки простоты. Связь символа Лежандра и степеней элемента. Тест Соловея-Штрассена. Вероятность ошибки. Тест Рабина проверки на простоту. Понятие о расширенной гипотезе Римана и полиномиальность детерминированного алгоритма Миллера при ее справедливости. 4. Взаимосвязь свидетелей простоты в алгоритме Миллера-Рабина, в алгоритме Ферма и в алгоритме Соловея-Штрассена. 5. Основные понятия полиномиального теста распознования простоты Агравала-Каяла-Саксены. Полиномиальная арифметика по модулю. Следствия результата Фоуври. Оценка работы алгоритма и возможности его улучшения. Реализация алгоритмов из пунктов 1, 2, 3 в системах со встроенной длинной арифметикой.	8	5-6	домашняя работа	8	устно

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
3.	Тема 3. Криптосистемы с открытым ключом. 1. Математические основы. Обобщение теоремы Эйлера. Дискретное логарифмирование, сравнение трудоемкости дискретного логарифмирования и возведения в степень. 2. Теория и практика криптоситем с открытым ключом. Суть криптографии с открытым ключом: односторонние функции, функции с секретом, понятия открытого и закрытого ключа. Криптосистема RSA. Практические ограничения, накладываемы на параметры системы RSA. ?Подводные камни? криптосистемы RSA. Примеры работы системы. Криптосистема Эль-Гамаля. Криптоситема Мэсси-Омуры для передачи сообщений. 3. Генерация случайных чисел. Мультипликативные и конгруэнтные датчики случайных чисел. Их всевозможные обобщения ? датчики Фибоначчи, датчики вычитания с заимствованием и сложения с переносом. Быстрота работы и криптографическая неустойчивость всех таких датчиков. Числа Блюма и датчики Блюма.	8	7-10	домашняя работа	8	устно

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
4.	Тема 4. 4. Протоколы разделения секрета между несколькими участниками. Протокол, основанный на сложение по модулю два. Протокол, основанный на китайской теореме об остатках. 5. Протоколы доказательств с нулевым разглашением. Основы доказательств с нулевым разглашением. Протоколы доказательств для задач изоморфизма графов и гамильтонова цикла и раскраски в 3 цвета. Протоколы доказательств для задачи дискретного логарифма и вскрытия RSA. Реализация всех рассматриваемых протоколов.	8	15-18	домашняя работа	8	устно

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
4.	Тема 4. Основные криптографические протоколы. 1. Протокол Диффи-Хеллмана выработки общего секрета. Атака посредника. ?Подводные камни? реализации. Надежные простые числа. Использование подгрупп меньшего размера. Размер p. Практические правила. Что может пойти не так. Алгоритм Диффи-Хелмана с тремя и более участниками. Обобщение алгоритма на коммутативные кольца. 2. Протоколы аутентификации и цифровой подписи. Схема подписи в системе RSA. Подписи, основанные на односторонних функциях. Схема аутентификации Шнорра и ее ?подводные камни?. Схема цифровой подписи Шнорра. 3. Протокол подбрасывания монеты по телефону.	8	11-14	домашняя работа	8	устно
	Итого				48	

5. Образовательные технологии, включая интерактивные формы обучения

Аудиторные занятия со студентами по данной дисциплине проводятся в форме лабораторных занятий. Кроме того, предусмотрена самостоятельная работа студентов.

6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов

Тема 1. Некоторые алгоритмические вопросы элементарной теории чисел. 1. Временные оценки сложности арифметических операций. Свойства функций оценки сложности (иерархия функций, символы O, □ , □ ; операции с O). Сложность арифметических операций с целыми числами. Сложность наивных алгоритмов факторизации и проверки простоты числа. 2. Делимость. Алгоритм Евклида. Основная теорема арифметики. Сложность алгоритма Евклида. Расширенный алгоритм Евклида для решения линейных диофантовых уравнений. Доказательство основной теоремы арифметики с помощью расширенного алгоритма Евклида. 3. Модулярная арифметика. Теорема Ферма. Функция Эйлера. Теорема Эйлера. Быстрые алгоритмы возведения в степень и нахождения обратного элемента в модулярной арифметике. Китайская теорема об остатках. Реализация алгоритмов из пунктов 2, 3 в системах со встроенной длинной арифметикой.

устно, примерные вопросы:

реферат по теме раздела

Тема 2. 3. Рандомизированные алгоритмы проверки простоты. Связь символа Лежандра и степеней элемента. Тест Соловея-Штрассена. Вероятность ошибки. Тест Рабина проверки на простоту. Понятие о расширенной гипотезе Римана и полиномиальность детерминированного алгоритма Миллера при ее справедливости. 4. Взаимосвязь свидетелей простоты в алгоритме Миллера-Рабина, в алгоритме Ферма и в алгоритме Соловея-Штрассена. 5. Основные понятия полиномиального теста распознования простоты Агравала-Каяла-Саксены. Полиномиальная арифметика по модулю. Следствия результата Фоуври. Оценка работы алгоритма и возможности его улучшения. Реализация алгоритмов из пунктов 1, 2, 3 в системах со встроенной длинной арифметикой.

устно , примерные вопросы:

реферат по теме раздела

Тема 2. Как отличить составное число от простого? 1. Математические основы. Распределение простых чисел, неравенства для □ (x). Понятия о более точных оценках □ (x), постулат Бертрана. Структура мультипликативной группы по модулю. Случай простого модуля. Разложение мультипликативной группы для любого натурального модуля на взаимно-простые составляющие: понятие о циклической группе; свойства; формулировка основной теоремы (без доказательства). Квадратичные вычеты: понятия символа Лежандра и символа Якоби; квадратичный закон взаимности; значение символа Лежандра для малых положительных и отрицательных значений; полиномиальный алгоритм нахождения символа Якоби. 2. Простейшие алгоритмы проверки на простоту. Критерий Вильсона. Тесты, основанные на малой теореме Ферма. Свойства чисел Кармайкла. Написание программы генерирующие числа Кармайкла, меньшие миллиона.

устно , примерные вопросы:

реферат по теме раздела

Тема 3. Криптосистемы с открытым ключом. 1. Математические основы. Обобщение теоремы Эйлера. Дискретное логарифмирование, сравнение трудоемкости дискретного логарифмирования и возведения в степень. 2. Теория и практика криптоситем с открытым ключом. Суть криптографии с открытым ключом: односторонние функции, функции с секретом, понятия открытого и закрытого ключа. Криптосистема RSA. Практические ограничения, накладываемы на параметры системы RSA. ?Подводные камни? криптосистемы RSA. Примеры работы системы. Криптосистема Эль-Гамаля. Криптоситема Мэсси-Омуры для передачи сообщений. 3. Генерация случайных чисел. Мультипликативные и конгруэнтные датчики случайных чисел. Их всевозможные обобщения ? датчики Фибоначчи, датчики вычитания с заимствованием и сложения с переносом. Быстрота работы и криптографическая неустойчивость всех таких датчиков. Числа Блюма и датчики Блюма. Степень их криптографической устойчивости. Реализация всех криптосистем из пункта 2.

устно , примерные вопросы:

реферат по теме раздела

Тема 4. 4. Протоколы разделения секрета между несколькими участниками. Протокол, основанный на сложение по модулю два. Протокол, основанный на китайской теореме об остатках. 5. Протоколы доказательств с нулевым разглашением. Основы доказательств с нулевым разглашением. Протоколы доказательств для задач изоморфизма графов и гамильтонова цикла и раскраски в 3 цвета. Протоколы доказательств для задачи дискретного логарифма и вскрытия RSA. Реализация всех рассматриваемых протоколов.

устно , примерные вопросы:

реферат по теме раздела

Тема 4. Основные криптографические протоколы. 1. Протокол Диффи-Хеллмана выработки общего секрета. Атака посредника. ?Подводные камни? реализации. Надежные простые числа. Использование подгрупп меньшего размера. Размер p. Практические правила. Что может пойти не так. Алгоритм Диффи-Хелмана с тремя и более участниками. Обобщение алгоритма на коммутативные кольца. 2. Протоколы аутентификации и цифровой подписи. Схема подписи в системе RSA. Подписи, основанные на односторонних функциях. Схема аутентификации Шнорра и ее ?подводные камни?. Схема цифровой подписи Шнорра. 3. Протокол подбрасывания монеты по телефону.

устно , примерные вопросы:

реферат по теме раздела

Тема 5. Подготовка к экзамену

Тема . Итоговая форма контроля

Примерные вопросы к экзамену:

По данной дисциплине предусмотрено проведение экзамена. Вопросы экзамена повторяют вопросы программы, к каждому вопросу также прилагается задача.

Примерный список задач.

Теоретические основы RSA

1. Почему доказательство малой теоремы Ферма проходит только для сравнения по простому модулю. В каком месте используется простота?

2. Используя формулу бинома Ньютона, докажите, что

(a+b)^p=a^p+b^p (mod p),

а также

(a+b+?+z)^p=a^p+b^p+z^p (mod p).

3. Используя результат предыдущего упражнения дайте другое доказательство малой теоремы Ферма.

4. Напишите таблицы для групповых операций в группе сложения по модулю 4 и в группе умножения (ненулевых элементов) по модулю 5. Докажите, что эти группы изоморфны.

5. Найдите все x, для которых x=4 (mod 5) и x=5 (mod 11).

6. Найдите все целые числа x, дающие при делении на 2,3,4,5,6 остатки 1,2,3,4,5 соответственно. (Игровая формулировка задачи ? деление x слитков золота между 6 разбойниками. 5 раз подряд не хватает одного слитка одному разбойнику, и его убивают оставшиеся. В конце остается один разбойник. Сколько было слитков золота?)

7. Пусть известны все простые делители натурального числа n. Используя вероятностные соображения найдите долю чисел меньших n и взаимно простых с ним (n).

Алгоритмы теоретико-числовой арифметики.

8. Используя алгоритм Евклида докажите что

НОД(2^n-1,2^m-1)=2^НОД(m,n)-1/

9. Докажите, что в последовательности 2+1,2^2+1,2^4+1,?,2^(2^n)+1,? любые два числа взаимно просты.

10. Проследите за выполнением расширенного алгоритма Евклида для входа (899,493) и найдите тройки (d,x,y).

11. Перепишите процедуру, реализующую алгоритм Евклида, заменив рекурсию циклом и ограничившись фиксированном объемом памяти.

12. Какой ответ дает расширенный алгоритм Евклида для входа, представляющего собой пару последовательных чисел Фибоначчи.

13. Укажите эффективный алгоритм нахождения наименьшего общего кратного нескольких чисел.

14. Предложите алгоритм вычисления a^b mod n, который обрабатывает биты двоичной записи двоичной записи b справа налево (от старших к младшим).

15. Объясните, как вычислить a^(-1) mod n при помощи процедуры возведения в степень, если известно (n) (см. упражнение 7).

Алгоритмы проверки на простоту

16. Докажите, что если нечетное целое число n не является простым и не является степенью простого числа, то в кольце вычетов по модулю n существует нетривиальный корень из единицы.

17. Докажите, что всякое число Кармайкла не делится на квадрат никакого простого числа и имеет по крайней мере 3 простых делителя. (Это одна из причин, почему числа Кармайкла редки.)

RSA

18. Вычислите открытый и секретный RSA ключи при p=11, q=29, n=319 и e=3. Чему равно d в секретном ключе? Зашифруйте сообщение M=100.

19. Пусть значение e для открытого ключа равно 3. Докажите, что враг, узнавший значение d, сможет разложить n на множители за время, полиномиальное относительно длины двоичной записи n.

20. Докажите, что система RSA мультипликативна, то есть по модулю n произведение двух зашифрованных сообщений совпадает с шифровкой числа, представляющего собой произведение исходных сообщений. Предположим, что враг умеет расшифровывать 1% всех сообщений (рассматриваемых как числа по модулю n). Используя мультипликативность системы RSA, объясните, как тогда он может с высокой вероятностью достаточно быстро расшифровать любое сообщение.

21. Придумайте и реализуйте эффективный алгоритм (квадратично зависящий от количества бит входной информации) поиска одного из делителей числа Кармайкла. Почему такой алгоритм не годится для произвольного натурального числа?

7.1. Основная литература:

1. Введение в криптографию, под редакцией Ященко И.В. - М.: МЦНМО, 2000.

2. Кнут Д. Искусство программирования. Том 2. Получисленные алгоритмы. - М.: Вильямс, 2003.

3. Коблиц Н. Курс теории чисел и криптографии - М.: ТВП, 2001.

4. Кормен Т., Лейзерсон Ч., Ривест Р. Алгоритмы: построение и анализ. - М.:МЦНМО, 1999.

5. Лернер Э.Ю., Кашина О.А. Пакет Mathematica: практические сюжеты // Казань: Изд-во КГУ, 2006.

6. Черемушкин А.В. Лекции по арифметическим алгоритмам в криптографии. - М.: МЦНМО, 2002.

7. Шнайер Б. Прикладная криптография. - М.: Триумф, 2002.

8. Шнайер Б. Секреты и ложь. Безопасность данных в цифровом мире. ? СПб.: Питер, 2003.

9. Фергюсон Н., Шнайер Б. Практическая криптография. ? М.: Вильямс, 2005.

7.2. Дополнительная литература:

10. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии. - М.:МЦНМО, 2003.

11. Гэри М., Джонсон Д. Вычислительные машины и труднорешаемые задачи. М.: Мир, 1982.

12. Лернер Э.Ю. Свидетели простоты в алгоритме Шора и в алгоритме Миллера-Рабина // "Известия высших учебных заведений. Математика", № 12, 2008, с. 43-48.

13. Соловьев Ю.П., Садовничий В.А., Шавгулидзе Е.Т., Белокуров В.В. Эллиптические кривые и современные алгоритмы теории чисел. - Москва-Ижевск: Институт компьютерных исследований, 2003.

14. Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone. Handbook of applied cryptography. CRC Press, 2001.

7.3. Интернет-ресурсы:

Сайт - http://ru.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D1%81%D0%B8%D

Сайт - http://pv.bstu.ru/crypto/OpenKeyCrypt.pdf

Сайт - https://sites.google.com/site/anisimovkhv/learning/kripto/lecture/tema8

Сайт - http://www.studzona.com/referats/view/17386

Сайт - http://mind-control.wikia.com/wiki/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D1%81%D0%

8. Материально-техническое обеспечение дисциплины(модуля)

Освоение дисциплины "Криптография с открытым ключом" предполагает использование следующего материально-технического обеспечения:

Компьютерные классы (9 классов) лаборатории малой вычислительной техники Института ВМ и ИТ, оснащенные мультимедийным оборудованием.

Программа составлена в соответствии с требованиями ФГОС ВПО и учебным планом по направлению 230700.62 "Прикладная информатика" и профилю подготовки Прикладная информатика в экономике .

Автор(ы):
Лернер Э.Ю. _____
"__" _____ 201 __ г.

Рецензент(ы):
Кугураков В.С. _____
"__" _____ 201 __ г.