МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное учреждение
высшего профессионального образования
"Казанский (Приволжский) федеральный университет"
Институт вычислительной математики и информационных технологий

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

Программа дисциплины

Математические основы защиты информации и информационной безопасности М1.Б.3

Направление подготовки: 010300.68 - Фундаментальная информатика и информационные технологии
Профиль подготовки: Математические основы и программное обеспечение информационной безопасности и защиты информации
Квалификация выпускника: магистр
Форма обучения: очное
Язык обучения: русский

Автор(ы):
Ишмухаметов Ш.Т.
Рецензент(ы):
Латыпов Р.Х.

СОГЛАСОВАНО:
Заведующий(ая) кафедрой: Латыпов Р. Х.
Протокол заседания кафедры No ___ от "____" _____ 201__г
Учебно-методическая комиссия Института вычислительной математики и информационных технологий:
Протокол заседания УМК No ____ от "____" _____ 201__г

Регистрационный No

Казань

2013

Содержание

Программу дисциплины разработал(а)(и) профессор, д.н. (доцент) Ишмухаметов Ш.Т. кафедра системного анализа и информационных технологий отделение фундаментальной информатики и информационных технологий , Shamil.Ishmukhametov@kpfu.ru

1. Цели освоения дисциплины

Данный курс входит в систему специализации по направлению информационной безопасности и является продолжением курсов "Основы информационной безопасности" и "Информационная безопасность в сетях". В ходе этого курса студенты должны получить основные знания о математических основах построения криптографических алгоритмов, понятия о вычислительной сложности односторонних функций, используемых в криптографии, методах построения надежных систем защиты и о возможных атаках.

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

Данная учебная дисциплина включена в раздел " М1.Б.3 Общенаучный" основной образовательной программы 010300.68 Фундаментальная информатика и информационные технологии и относится к базовой (общепрофессиональной) части. Осваивается на 1 курсе, 1 семестр.

"Математические основы защиты информации и информационной безопасности" входит в состав общенаучных дисциплин, раздел М1.Б.3. Читается на 1 курсе, в 1 семестре.

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

В результате освоения дисциплины формируются следующие компетенции:

Шифр компетенции	Расшифровка приобретаемой компетенции
ОК-1 (общекультурные компетенции)	способность понимать и анализировать мировоззренческие, социально и личностно значимые философские проблемы
ОК-2 (общекультурные компетенции)	способность совершенствовать и развивать свой интеллектуальный и общекультурный уровень, добиваться нравственного и физического совершенствования своей личности
ОК-3 (общекультурные компетенции)	способность к самостоятельному обучению новым методам исследования, к изменению научного и научно-производственного профиля своей профессиональной деятельности
ОК-4 (общекультурные компетенции)	способность свободно пользоваться русским и иностранным языками как средством делового общения

В результате освоения дисциплины студент:

1. должен знать:

основные концепции информационной безопасности;

2. должен уметь:

ориентироваться в вопросах разработки надежных систем защит и видах угроз информационной безопасности.

3. должен владеть:

теоретическими знаниями о математических основах построения криптографических алгоритмов;

навыков оценки безопасности информационных систем.

4. Структура и содержание дисциплины/ модуля

Общая трудоемкость дисциплины составляет зачетных(ые) единиц(ы) 72 часа(ов).

Форма промежуточного контроля дисциплины экзамен в 1 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. Сервисы информационной безопасности: аутентификация, авторизация, аудит, их краткая характеристика.	1		1	0	0	домашнее задание
2.	Тема 2. Расширенный алгоритм Евклида для решения для заданных чисел A и B уравнения Ax+By=d, где d ? наибольший общий делитель чисел a и b. Оценка его сложности. Алгоритм быстрого возведения в степень по модулю заданного числа.	1		0	2	0	домашнее задание
3.	Тема 3. Методы шифрования с открытым ключом. RSA, его основные алгоритмы. Пример шифрования в RSA.	1		0	2	0	домашнее задание

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. Взлом RSA. Методы факторизации натуральных чисел. Алгоритм Ферма. Оценка его сложности.	1		0	2	0	домашнее задание
5.	Тема 5. Метод Полларда факторизации натуральных чисел. Оценка его сложности	1		0	2	0	домашнее задание
6.	Тема 6. Проверка простоты натуральных чисел. Метод пробного деления. Алгоритм Ферма проверки простоты. Оценка их сложности.	1		0	2	0	домашнее задание
7.	Тема 7. Методы факторизации натуральных чисел. (p-1) и ρ-методы Полларда. Оценка их сложности. ρ-метод Полларда вычисления дискретного логарифма.	1		2	0	0	домашнее задание
8.	Тема 8. Конечные поля. Вычисления в конечных полях (сложение, вычитание, умножение, деление, возведение в степень). Вычисление обратного элемента. Символы Лежандра и Якоби, алгоритм их вычисления.	1		2	0	0	домашнее задание
9.	Тема 9. Шифрование и построение ЭЦП на основе метода Эль-Гамаля.	1		0	2	0	домашнее задание
10.	Тема 10. Методы аутентификации в сети. Сетевая аутентификация на основе метода ?вызов-ответ?.	1		1	0	0	домашнее задание

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практические занятия	Лабораторные работы	
11.	Тема 11. Выработка общего секретного ключа на основе метода Диффи-Хелмана.	1		2	0	0	домашнее задание
12.	Тема 12. Электронная цифровая подпись. Свойства ЭЦП и ее формирование. Построение ЭЦП на основе двухключевых методов шифрования	1		2	0	0	домашнее задание
13.	Тема 13. Удостоверяющие центры, их основные функции. Состав сертификата ЭЦП	1		2	0	0	домашнее задание
14.	Тема 14. Эллиптические кривые. Арифметические операции на эллиптической кривой.	1		2	0	0	домашнее задание
15.	Тема 15. Алгоритм вычисления кратного точки эллиптической кривой. Методы ускорения вычисления кратного. Проективные координаты. Метод Монтгомери вычисления кратного точки эллиптической криво	1		0	2	0	домашнее задание
16.	Тема 16. Шифрование на эллиптических кривых. Построение электронной подписи на эллиптических кривых.	1		0	2	0	домашнее задание
17.	Тема 17. Метод факторизации Х.Ленстры с использованием эллиптических кривых. Выбор границы первой и второй стадий алгоритма. Оценка сложности алгоритма Ленстры.	1		0	2	0	домашнее задание

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практические занятия	Лабораторные работы	
18.	Тема 18. Суперсингулярные эллиптические кривые. Билинейные преобразования. Преобразование Вейля. Алгоритм Миллера вычисления функции Вейля. MOV-атака на эллиптические кривые. Преобразование Тейта. Алгоритм его вычисления.	1		2	0	0	домашнее задание
19.	Тема 19. Использование преобразований Вейля и Тейта в криптографии. Трехсторонний протокол Диффи-Хелмана, построение ЭЦП на основе идентификационных данных пользователя, построение ?слепой подписи	1		1	0	0	домашнее задание
20.	Тема 20. Метод квадратичного решета факторизации натуральных чисел. Основные параметры метода и их выбор.	1		1	0	0	домашнее задание
.	Тема . Итоговая форма контроля	1		0	0	0	экзамен
	Итого			18	18	0	

4.2 Содержание дисциплины

Тема 1. Сервисы информационной безопасности: аутентификация, авторизация, аудит, их краткая характеристика.

лекционное занятие (1 часа(ов)):

Сервисы информационной безопасности: аутентификация, авторизация, аудит, их краткая характеристика.

Тема 2. Расширенный алгоритм Евклида для решения для заданных чисел A и B уравнения Ax+By=d, где d ? наибольший общий делитель чисел a и b. Оценка его сложности. Алгоритм быстрого возведения в степень по модулю заданного числа.

практическое занятие (2 часа(ов)):

Расширенный алгоритм Евклида для решения для заданных чисел A и B уравнения Ax+By=d, где d ? наибольший общий делитель чисел a и b. Оценка его сложности. Алгоритм быстрого возведения в степень по модулю заданного числа.

Тема 3. Методы шифрования с открытым ключом. RSA, его основные алгоритмы. Пример шифрования в RSA.

практическое занятие (2 часа(ов)):

Методы шифрования с открытым ключом. RSA, его основные алгоритмы. Пример шифрования в RSA.

Тема 4. Взлом RSA. Методы факторизации натуральных чисел. Алгоритм Ферма. Оценка его сложности.

практическое занятие (2 часа(ов)):

Взлом RSA. Методы факторизации натуральных чисел. Алгоритм Ферма. Оценка его сложности.

Тема 5. Метод Полларда факторизации натуральных чисел. Оценка его сложности

практическое занятие (2 часа(ов)):

Метод Полларда факторизации натуральных чисел. Оценка его сложности

Тема 6. Проверка простоты натуральных чисел. Метод пробного деления. Алгоритм Ферма проверки простоты. Оценка их сложности.

практическое занятие (2 часа(ов)):

Проверка простоты натуральных чисел. Метод пробного деления. Алгоритм Ферма проверки простоты. Оценка их сложности.

Тема 7. Методы факторизации натуральных чисел. (p-1) и ρ-методы Полларда. Оценка их сложности. ρ-метод Полларда вычисления дискретного логарифма.

лекционное занятие (2 часа(ов)):

Методы факторизации натуральных чисел. (p-1) и ρ-методы Полларда. Оценка их сложности. ρ-метод Полларда вычисления дискретного логарифма.

Тема 8. Конечные поля. Вычисления в конечных полях (сложение, вычитание, умножение, деление, возведение в степень). Вычисление обратного элемента. Символы Лежандра и Якоби, алгоритм их вычисления.

лекционное занятие (2 часа(ов)):

Конечные поля. Вычисления в конечных полях (сложение, вычитание, умножение, деление, возведение в степень). Вычисление обратного элемента. Символы Лежандра и Якоби, алгоритм их вычисления.

Тема 9. Шифрование и построение ЭЦП на основе метода Эль-Гамаля.

практическое занятие (2 часа(ов)):

Шифрование и построение ЭЦП на основе метода Эль-Гамаля.

Тема 10. Методы аутентификации в сети. Сетевая аутентификация на основе метода ?вызов-ответ?.

лекционное занятие (1 часа(ов)):

Методы аутентификации в сети. Сетевая аутентификация на основе метода ?вызов-ответ?.

Тема 11. Выработка общего секретного ключа на основе метода Диффи-Хелмана.

лекционное занятие (2 часа(ов)):

Выработка общего секретного ключа на основе метода Диффи-Хелмана.

Тема 12. Электронная цифровая подпись. Свойства ЭЦП и ее формирование. Построение ЭЦП на основе двухключевых методов шифрования

лекционное занятие (2 часа(ов)):

Электронная цифровая подпись. Свойства ЭЦП и ее формирование. Построение ЭЦП на основе двухключевых методов шифрования

Тема 13. Удостоверяющие центры, их основные функции. Состав сертификата ЭЦП

лекционное занятие (2 часа(ов)):

Удостоверяющие центры, их основные функции. Состав сертификата ЭЦП

Тема 14. Эллиптические кривые. Арифметические операции на эллиптической кривой.

лекционное занятие (2 часа(ов)):

Эллиптические кривые. Арифметические операции на эллиптической кривой.

Тема 15. Алгоритм вычисления кратного точки эллиптической кривой. Методы ускорения вычисления кратного. Проективные координаты. Метод Монтгомери вычисления кратного точки эллиптической криво

практическое занятие (2 часа(ов)):

Алгоритм вычисления кратного точки эллиптической кривой. Методы ускорения вычисления кратного. Проективные координаты. Метод Монтгомери вычисления кратного точки эллиптической кривой

Тема 16. Шифрование на эллиптических кривых. Построение электронной подписи на эллиптических кривых.

практическое занятие (2 часа(ов)):

Шифрование на эллиптических кривых. Построение электронной подписи на эллиптических кривых.

Тема 17. Метод факторизации Х.Ленстры с использованием эллиптических кривых. Выбор границы первой и второй стадий алгоритма. Оценка сложности алгоритма Ленстры.

практическое занятие (2 часа(ов)):

Метод факторизации Х.Ленстры с использованием эллиптических кривых. Выбор границы первой и второй стадий алгоритма. Оценка сложности алгоритма Ленстры.

Тема 18. Суперсингулярные эллиптические кривые. Билинейные преобразования. Преобразование Вейля. Алгоритм Миллера вычисления функции Вейля. MOV-атака на эллиптические кривые. Преобразование Тейта. Алгоритм его вычисления.

лекционное занятие (2 часа(ов)):

Суперсингулярные эллиптические кривые. Билинейные преобразования. Преобразование Вейля. Алгоритм Миллера вычисления функции Вейля. MOV-атака на эллиптические кривые. Преобразование Тейта. Алгоритм его вычисления.

Тема 19. Использование преобразований Вейля и Тейта в криптографии. Трехсторонний протокол Диффи-Хелмана, построение ЭЦП на основе идентификационных данных пользователя, построение ?слепой подписи

лекционное занятие (1 часа(ов)):

Использование преобразований Вейля и Тейта в криптографии. Трехсторонний протокол Диффи-Хелмана, построение ЭЦП на основе идентификационных данных пользователя, построение ?слепой подписи

Тема 20. Метод квадратичного решета факторизации натуральных чисел. Основные параметры метода и их выбор.

лекционное занятие (1 часа(ов)):

Метод квадратичного решета факторизации натуральных чисел. Основные параметры метода и их выбор.

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. Сервисы информационной безопасности: аутентификация, авторизация, аудит, их					

краткая характеристика.

	1		подготовка домашнего задания	1	домашнее задание

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
2.	Тема 2. Расширенный алгоритм Евклида для решения для заданных чисел A и B уравнения Ax+By=d, где d ? наибольший общий делитель чисел a и b. Оценка его сложности. Алгоритм быстрого возведения в степень по модулю заданного числа.	1		подготовка домашнего задания	2	домашнее задание
3.	Тема 3. Методы шифрования с открытым ключом. RSA, его основные алгоритмы. Пример шифрования в RSA.	1		подготовка домашнего задания	2	домашнее задание
4.	Тема 4. Взлом RSA. Методы факторизации натуральных чисел. Алгоритм Ферма. Оценка его сложности.	1		подготовка домашнего задания	2	домашнее задание
5.	Тема 5. Метод Полларда факторизации натуральных чисел. Оценка его сложности	1		подготовка домашнего задания	2	домашнее задание
6.	Тема 6. Проверка простоты натуральных чисел. Метод пробного деления. Алгоритм Ферма проверки простоты. Оценка их сложности.	1		подготовка домашнего задания	2	домашнее задание
7.	Тема 7. Методы факторизации натуральных чисел. (p-1) и ρ-методы Полларда. Оценка их сложности. ρ-метод Полларда вычисления дискретного логарифма.	1		подготовка домашнего задания	2	домашнее задание

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
8.	Тема 8. Конечные поля. Вычисления в конечных полях (сложение, вычитание, умножение, деление, возведение в степень). Вычисление обратного элемента. Символы Лежандра и Якоби, алгоритм их вычисления.	1		подготовка домашнего задания	2	домашнее задание
9.	Тема 9. Шифрование и построение ЭЦП на основе метода Эль-Гамаля.	1		подготовка домашнего задания	2	домашнее задание
10.	Тема 10. Методы аутентификации в сети. Сетевая аутентификация на основе метода ?вызов-ответ?.	1		подготовка домашнего задания	1	домашнее задание
11.	Тема 11. Выработка общего секретного ключа на основе метода Диффи-Хелмана.	1		подготовка домашнего задания	2	домашнее задание
12.	Тема 12. Электронная цифровая подпись. Свойства ЭЦП и ее формирование. Построение ЭЦП на основе двухключевых методов шифрования	1		подготовка домашнего задания	2	домашнее задание
13.	Тема 13. Удостоверяющие центры, их основные функции. Состав сертификата ЭЦП	1		подготовка домашнего задания	2	домашнее задание
14.	Тема 14. Эллиптические кривые. Арифметические операции на эллиптической кривой.	1		подготовка домашнего задания	2	домашнее задание

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
15.	Тема 15. Алгоритм вычисления кратного точки эллиптической кривой. Методы ускорения вычисления кратного. Проективные координаты. Метод Монтгомери вычисления кратного точки эллиптической криво	1		подготовка домашнего задания	2	домашнее задание
16.	Тема 16. Шифрование на эллиптических кривых. Построение электронной подписи на эллиптических кривых.	1		подготовка домашнего задания	2	домашнее задание
17.	Тема 17. Метод факторизации Х.Ленстры с использованием эллиптических кривых. Выбор границы первой и второй стадий алгоритма. Оценка сложности алгоритма Ленстры.	1		подготовка домашнего задания	2	домашнее задание
18.	Тема 18. Суперсингулярные эллиптические кривые. Билинейные преобразования. Преобразование Вейля. Алгоритм Миллера вычисления функции Вейля. MOV-атака на эллиптические кривые. Преобразование Тейта. Алгоритм его вычисления.	1		подготовка домашнего задания	2	домашнее задание

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
19.	Тема 19. Использование преобразований Вейля и Тейта в криптографии. Трехсторонний протокол Диффи-Хелмана, построение ЭЦП на основе идентификационных данных пользователя, построение ?слепой подписи	1		подготовка домашнего задания	1	домашнее задание
20.	Тема 20. Метод квадратичного решета факторизации натуральных чисел. Основные параметры метода и их выбор.	1		подготовка домашнего задания	1	домашнее задание
	Итого				36	

5. Образовательные технологии, включая интерактивные формы обучения

Обучение происходит в форме лекционных и лабораторных занятий, а также самостоятельной работы студентов.

Теоретический материал излагается на лекциях. Причем конспект лекций, который остается у студента в результате прослушивания лекции не может заменить учебник. Его цель-формулировка основных утверждений и определений. Прослушав лекцию, полезно ознакомиться с более подробным изложением материала в учебнике. Список литературы разделен на две категории: необходимый для сдачи экзамена минимум и дополнительная литература.

Изучение курса подразумевает не только овладение теоретическим материалом, но и получение практических навыков для более глубокого понимания разделов на основе решения задач и упражнений, иллюстрирующих доказываемые теоретические положения, а также развитие абстрактного мышления и способности самостоятельно доказывать утверждения.

Самостоятельная работа предполагает выполнение домашних работ. Практические задания, выполненные в аудитории, предназначены для указания общих методов решения задач определенного типа. Закрепить навыки можно лишь в результате самостоятельной работы.

Кроме того, самостоятельная работа включает подготовку к экзамену. При подготовке к сдаче экзамена весь объем работы рекомендуется распределять равномерно по дням, отведенным для подготовки к экзамену, контролировать каждый день выполнения работы. Лучше, если можно перевыполнить план. Тогда будет резерв времени.

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

Тема 1. Сервисы информационной безопасности: аутентификация, авторизация, аудит, их краткая характеристика.

домашнее задание , примерные вопросы:

Углубленное изучение литературы по изучаемой теме. Обсуждение. Решение типовых задач.

Тема 2. Расширенный алгоритм Евклида для решения для заданных чисел A и B уравнения Ax+By=d, где d ? наибольший общий делитель чисел a и b. Оценка его сложности. Алгоритм быстрого возведения в степень по модулю заданного числа.

домашнее задание , примерные вопросы:

Углубленное изучение литературы по изучаемой теме. Обсуждение. Решение типовых задач.

Тема 3. Методы шифрования с открытым ключом. RSA, его основные алгоритмы. Пример шифрования в RSA.

домашнее задание , примерные вопросы:

Углубленное изучение литературы по изучаемой теме. Обсуждение. Решение типовых задач.

Тема 4. Взлом RSA. Методы факторизации натуральных чисел. Алгоритм Ферма. Оценка его сложности.

домашнее задание , примерные вопросы:

Углубленное изучение литературы по изучаемой теме. Обсуждение. Решение типовых задач.

Тема 5. Метод Полларда факторизации натуральных чисел. Оценка его сложности

домашнее задание , примерные вопросы:

Углубленное изучение литературы по изучаемой теме. Обсуждение. Решение типовых задач.

Тема 6. Проверка простоты натуральных чисел. Метод пробного деления. Алгоритм Ферма проверки простоты. Оценка их сложности.

домашнее задание , примерные вопросы:

Углубленное изучение литературы по изучаемой теме. Обсуждение. Решение типовых задач.

Тема 7. Методы факторизации натуральных чисел. (p-1) и ρ-методы Полларда. Оценка их сложности. ρ-метод Полларда вычисления дискретного логарифма.

домашнее задание , примерные вопросы:

Углубленное изучение литературы по изучаемой теме. Обсуждение. Решение типовых задач.

Тема 8. Конечные поля. Вычисления в конечных полях (сложение, вычитание, умножение, деление, возведение в степень). Вычисление обратного элемента. Символы Лежандра и Якоби, алгоритм их вычисления.

домашнее задание , примерные вопросы:

Углубленное изучение литературы по изучаемой теме. Обсуждение. Решение типовых задач.

Тема 9. Шифрование и построение ЭЦП на основе метода Эль-Гамаля.

домашнее задание , примерные вопросы:

Углубленное изучение литературы по изучаемой теме. Обсуждение. Решение типовых задач.

Тема 10. Методы аутентификации в сети. Сетевая аутентификация на основе метода ?вызов-ответ?.

домашнее задание , примерные вопросы:

Углубленное изучение литературы по изучаемой теме. Обсуждение. Решение типовых задач.

Тема 11. Выработка общего секретного ключа на основе метода Диффи-Хелмана.

домашнее задание , примерные вопросы:

Углубленное изучение литературы по изучаемой теме. Обсуждение. Решение типовых задач.

Тема 12. Электронная цифровая подпись. Свойства ЭЦП и ее формирование. Построение ЭЦП на основе двухключевых методов шифрования

домашнее задание , примерные вопросы:

Углубленное изучение литературы по изучаемой теме. Обсуждение. Решение типовых задач.

Тема 13. Удостоверяющие центры, их основные функции. Состав сертификата ЭЦП

домашнее задание , примерные вопросы:

Углубленное изучение литературы по изучаемой теме. Обсуждение. Решение типовых задач.

Тема 14. Эллиптические кривые. Арифметические операции на эллиптической кривой.

домашнее задание , примерные вопросы:

Углубленное изучение литературы по изучаемой теме. Обсуждение. Решение типовых задач.

Тема 15. Алгоритм вычисления кратного точки эллиптической кривой. Методы ускорения вычисления кратного. Проективные координаты. Метод Монтгомери вычисления кратного точки эллиптической криво

домашнее задание , примерные вопросы:

Углубленное изучение литературы по изучаемой теме. Обсуждение. Решение типовых задач.

Тема 16. Шифрование на эллиптических кривых. Построение электронной подписи на эллиптических кривых.

домашнее задание , примерные вопросы:

Углубленное изучение литературы по изучаемой теме. Обсуждение. Решение типовых задач.

Тема 17. Метод факторизации Х.Ленстры с использованием эллиптических кривых. Выбор границы первой и второй стадий алгоритма. Оценка сложности алгоритма Ленстры.

домашнее задание , примерные вопросы:

Углубленное изучение литературы по изучаемой теме. Обсуждение. Решение типовых задач.

Тема 18. Суперсингулярные эллиптические кривые. Билинейные преобразования. Преобразование Вейля. Алгоритм Миллера вычисления функции Вейля. MOV-атака на эллиптические кривые. Преобразование Тейта. Алгоритм его вычисления.

домашнее задание , примерные вопросы:

Углубленное изучение литературы по изучаемой теме. Обсуждение. Решение типовых задач.

Тема 19. Использование преобразований Вейля и Тейта в криптографии. Трехсторонний протокол Диффи-Хелмана, построение ЭЦП на основе идентификационных данных пользователя, построение ?слепой подписи

домашнее задание , примерные вопросы:

Углубленное изучение литературы по изучаемой теме. Обсуждение. Решение типовых задач.

Тема 20. Метод квадратичного решета факторизации натуральных чисел. Основные параметры метода и их выбор.

домашнее задание , примерные вопросы:

Углубленное изучение литературы по изучаемой теме. Обсуждение. Решение типовых задач.

Тема . Итоговая форма контроля

Примерные вопросы к экзамену:

По данной дисциплине предусмотрено проведение экзамена. Примерные вопросы для экзамена - Приложение1.

7.1. Основная литература:

1. Ш.Т.Ишмухаметов. Методы факторизации натуральных чисел: учебное пособие, Казань, КФУ, 2011, 190 с.

7.2. Дополнительная литература:

1. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии/ О.Н. Василен-ко. - МЦНМО, 2003, 326 с.

2. Лидл Р. Конечные поля / Р. Лидл, Г. Нидеррайтер.- т. 1, 2. М.: Мир, 1988, 428 с.

3. Молдовян Н.А. Криптография. От примитивов к синтезу алгоритмов / Н.А. Молдовян, А.А. Молдовян, М.А. Еремеев. - БХВ-Петербург, 2004, 446 с.

4. Черемушкин А.В. Лекции по арифметическим функциям в криптографии/ А.В.~Черемушкин.-- М.: МЦНМО, 2002, 103 с.

7.3. Интернет-ресурсы:

Интернет-портал образовательных ресурсов по ИТ - http://www.intuit.ru

Интернет-портал ресурсов по математике - http://www.math.ru

Электронная библиотека ресурсов по техническим наукам - http://techlibrary.ru

электронное пособие - http://www.ksu.ru/f9/bin_files/metod_tzis!113.doc

электронное пособие - http://www.ksu.ru/f9/bibl/Monograph_ishm.pdf

8. Материально-техническое обеспечение дисциплины/модуля согласно утвержденному учебному плану

Освоение дисциплины "Математические основы защиты информации и информационной безопасности" предполагает использование следующего материально-технического обеспечения:

Программа составлена в соответствии с требованиями ФГОС ВПО и учебным планом по направлению 010300.68 "Фундаментальная информатика и информационные технологии" и магистерской программе Математические основы и программное обеспечение информационной безопасности и защиты информации .

Автор(ы):
Ишмухаметов Ш.Т. _____
"__" _____ 201 __ г.

Рецензент(ы):
Латыпов Р.Х. _____
"__" _____ 201 __ г.

Лист согласования

N	ФИО	Согласование
1	Латыпов Р. Х.	
2	Латыпов Р. Х.	
3	Латыпов Р. Х.	
4	Чижанова Е. А.	
5	Соколова Е. А.	
6	Тимофеева О. А.	