МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«Дальневосточный федеральный университет»
(ДВФУ)

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

Согласовано

Школа естественных наук)
Руководитель ОП
_____ Степанова А.А.,
(подпись) (Ф.И.О. рук. ОП)
«11» июля 2019 г.

«УТВЕРЖДАЮ»

Заведующий кафедрой адгебры, геометрии и анализа
_____ Шепелева Р.П.
(подпись) (Ф.И.О. зав. каф.)
«11» июля 2019 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ (РПУД)
Криптографические методы защиты информации

Направление подготовки: 01.04.01 Математика
Форма подготовки: очная

Школа естественных наук
Кафедра алгебры, геометрии и анализа
курс 2 семестр 3
лекции не предусмотрены
лабораторные занятия 36 час.
самостоятельная работа студентов 36 час.
контрольные работы 36 час.
всего часов аудиторной нагрузки 36 час.
зачет не предусмотрен
экзамен 3 семестр

Рабочая программа составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования, утвержденного приказом Министерства образования и науки РФ от 10 января 2018 г. № 12
Рабочая программа обсуждена на заседании кафедры Алгебры, геометрии и анализа «8» июля 2019 г.

Заведующий кафедрой к.ф.-м.н., профессор Р.П.Шепелева
Составитель: к.ф.-м.н, доцент С.Г. Чеканов

Владивосток
2019

Оборотная сторона титульного листа РПУД

I. Рабочая программа пересмотрена на заседании кафедры:

Протокол от «_____» _____ 200 г. № _____

Заведующий кафедрой _____ _____

(подпись) (И.О. Фамилия)

II. Рабочая программа пересмотрена на заседании кафедры:

Протокол от «_____» _____ 200 г. № _____

Заведующий кафедрой _____ _____

(подпись) (И.О. Фамилия)

Аннотация рабочей программы учебной дисциплины
«Криптографические методы защиты информации»

Рабочая программа учебной дисциплины «Криптографические методы защиты информации» разработана для студентов 1 и 2 курса направления магистратуры 01.04.01 «Математика», магистерской программы «Алгебра», в соответствии с требованиями федерального государственного стандарта высшего образования и образовательного стандарта, самостоятельно устанавливаемого ДВФУ.

Общая трудоемкость освоения дисциплины составляет 4 ЗЕ (144 час.). Учебным планом предусмотрены лабораторные работы (36 час.), курсовая работа (36 час.), самостоятельная работа студента (36 час.), всего часов аудиторной нагрузки (36 час). Дисциплина «Криптографические методы защиты информации» входит в часть, формируемую участниками образовательных отношений, реализуется на 2 курсе в 3 семестре.

Цель преподавания дисциплины «Криптографические методы защиты информации» является развитие логического и алгоритмического мышления.

Задачи преподавания дисциплины:

1. привить навыки математического исследования социальных, технических, экономических и других проблем науки и производства
2. умение мыслить научными категориями в области науки, техники, экономики и социальной сферы
3. умение математически корректно ставить естественнонаучные задачи

Задачи изучения дисциплины раскрываются через изложение требуемых результатов изучения дисциплины, характеризующие знания, умения и формируемые компетенции (в соответствие с ФГОС).

Полученные навыки по курсу «Криптографические методы защиты информации» в дальнейшем будут использоваться при изучении таких

дисциплин как Криптографические протоколы и Информационная безопасность.

Для успешного изучения дисциплины «Криптографические методы защиты информации» у обучающихся должны быть сформированы следующие предварительные компетенции

- способность видеть методологические аспекты построения математических теорий;
- применять системный подход в формализации математических задач;
- способностью к абстрактному мышлению, анализу, синтезу.

Планируемые результаты обучения по данной дисциплине (знания, умения, владения), соотнесенные с планируемыми результатами освоения образовательной программы, характеризуют этапы формирования следующих профессиональных компетенций:

Задача профессиональной деятельности	Объект или область знания	Код и наименование профессиональной компетенции	Код и наименование индикатора достижения профессиональной компетенции
Тип задач профессиональной деятельности: Проектно-технологический			

планирование и реализация научно-исследовательской деятельности в области математики и ее приложений	Универсальная алгебра и алгебраические методы криптографии. Методы и концепции математической логики. Алгоритмы и конструкции алгебраической геометрии.	ПК-6 способен разрабатывать концептуальные и теоретические модели решаемых задач проектной и производственно-технологической деятельности	ПК-6.1. Умеет: проводить анализ и обосновывать необходимость работы над данным проектом и оценивать его эффективность; обосновывать и защищать предлагаемый проект, доказывать его эффективность и востребованность на выбранном рынке ПК-6.2. Знает: особенности рынка данного региона ПК-6.3. Владеет: навыками работы над проектами по выбранной тематике; методами построения, анализа и применения математических моделей для оценки состояния, и прогноза развития экономических процессов и явлений; владеть опытом выражения своих мыслей и мнения
Тип задач профессиональной деятельности: организационно-управленческий			
проектирование, планирование и реализация образовательного процесса по математике в	Универсальная алгебра и алгебраические методы криптографии. Методы и	ПК-7 способен к применению методов математического и алгоритмического моделирования для	ПК7.1. – умеет: проводить анализ необходимых для реализации проекта ресурсов; оценить временные затраты на реализацию проекта; собрать и обработать информацию для

образовательном учреждении высшего и общего образования в соответствии с требованиями ФГОС основного общего образования и ФГОС среднего общего образования	концепции математической логики. Алгоритмы и конструкции алгебраической геометрии.	организации управленческой деятельности	принятия управленческих решений ПК-7.2. – знает: математические методы анализа данных о проекте; методы построения математической модели, необходимые для реализации проекта ПК-7.3. – владеет: алгоритмами математического анализа данных в профессиональной сфере; технологиями организации и распределения обязанностей в команде, реализующей проект

I. СТРУКТУРА И СОДЕРЖАНИЕ ТЕОРЕТИЧЕСКОЙ ЧАСТИ КУРСА

Лекции не предусмотрены учебным планом

II. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКОЙ ЧАСТИ КУРСА

Лабораторные работы (36 час.)

Лабораторная работа 1. Введение (4 часа).

Рассматриваются примеры шифров на основе группы подстановок конечного множества. Проводятся атаки на основе шифртекстов.

Лабораторная работа 2. Шифры простой замены (4 часа).

Изучаются шифры, построенные на основе конечных колец и групп. Шифруются открытые тексты и проводятся атаки на построенные шифры.

Лабораторная работа 3. Многоалфавитные шифры простой замены (4 часа).

Вычисляются статистические характеристики шифртекстов, полученных с помощью шифра Виженера. Выполняется анализ шифра по индивидуальному заданию.

Лабораторная работа 4. Совершенные шифры (4 часа).

Изучаются шифры совершенные по Шеннону. Строятся примеры шифров , которые проверяются на соответствие быть совершенными.

Лабораторная работа 5. Поточные шифры (4 часа).

Изучаются генераторы ключевых последовательностей для поточных шифров. Создаются собственные генераторы ключевых последовательностей для поточных шифров.

Лабораторная работа 6. Блочные шифры (4 часа).

Строятся блочные шифры. Изучаются стандарты шифрования DES, AES.

Лабораторная работа 7. Шифры с открытым ключом (4 часа).

Задача факторизации целых чисел. Логарифмирование в конечных абелевых группах. Схема шифрования RSA и Эль Гамаля. Изучаются возможные атаки на указанные шифры.

Лабораторная работа 8. Эллиптические кривые над конечными полями (4 часа).

Вычисляются группы точек эллиптических кривых для фиксированных конечных полей. Строятся алгоритмы кодировки текстов точками эллиптических кривых.

Лабораторная работа 9. Хеш функции (4 часа).

Строятся примеры хеш функций и оценивается их стойкость. Изучаются возможность построения криптографических протоколов на основе, построенных хеш функций.

III. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине «Криптографические методы защиты информации» представлено в Приложении 1 и включает в себя:

план-график выполнения самостоятельной работы по дисциплине, в том числе примерные нормы времени на выполнение по каждому заданию;

характеристика заданий для самостоятельной работы обучающихся и методические рекомендации по их выполнению;

требования к представлению и оформлению результатов самостоятельной работы;

критерии оценки выполнения самостоятельной работы.

IV. КОНТРОЛЬ ДОСТИЖЕНИЯ ЦЕЛЕЙ КУРСА

№ п/п	Контролируемые разделы / темы дисциплины	Коды и этапы формирования компетенций	Оценочные средства	
			текущий контроль	промежуточная аттестация
1	Введение	способен разрабатывать концептуальные и теоретические модели решаемых задач проектной и производственно-технологической деятельности (ПК-6), применению методов математического и алгоритмического моделирования для организации управленческой деятельности (ПК-7)	ПР-2	УО-2
2	Шифры простой замены	способен разрабатывать концептуальные и теоретические модели решаемых задач проектной и производственно-технологической деятельности (ПК-6),	УО-4	ПР-4
3	Многоалфавитные шифры замены	применению методов математического и алгоритмического моделирования для организации управленческой деятельности (ПК-7)	ПР-2	ПР-4
4	Совершенные шифры	способен разрабатывать концептуальные и теоретические модели решаемых задач проектной и производственно-технологической деятельности (ПК-6),	ПР-2	УО-2

5	Поточные шифры	применению методов математического и алгоритмического моделирования для организации управленческой деятельности (ПК-7)	УО-4	ПР-4
6	Блочные шифры	способен разрабатывать концептуальные и теоретические модели решаемых задач проектной и производственно-технологической деятельности (ПК-6),	УО-4	ПР-4
7	Шифры с открытым ключом	применению методов математического и алгоритмического моделирования для организации управленческой деятельности (ПК-7)	ПР-2	УО-2
8	Эллиптические кривые над конечными полями	способен разрабатывать концептуальные и теоретические модели решаемых задач проектной и производственно-технологической деятельности (ПК-6),	ПР-2	УО-2
9	Хеш функции	применению методов математического и алгоритмического моделирования для организации управленческой деятельности (ПК-7)	УО-4	ПР-4

Типовые контрольные задания и вопросы к зачету представлены в Приложении 2.

V. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

1. а) основная литература:

1. Алферов Н.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии, М. Гелиос АРВ, 2012 г.

http://lib.dvfu.ru:8080/lib/item?id=chamo:1640&theme=FEFU
2. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии, М.: МЦНМО, 2003 г. http://lib.dvfu.ru:8080/lib/item?id=chamo:5790&theme=FEFU

3. Коблиц Н. Курс теории чисел и криптографии, М.: ТВМ, 2001 г.

http://lib.dvfu.ru:8080/lib/item?id=chamo:16477&theme=FEFU

4. Д. К. Фаддеев, И. С. Соминский. Задачи по высшей алгебре. – Санкт-Петербург, «Лань», 1998, - 288 с. http://lib.dvfu.ru:8080/lib/item?id=Lan:Lan-399&theme=FEFU

5. Виноградов И.М. Основы теории чисел. – СПб.: Лань, 2009. – 176 с. http://lib.dvfu.ru:8080/lib/item?id=Lan:Lan-46&theme=FEFU
6. Кострикин А.И. и др. Сборник задач по алгебре. – СПб.: Лань, 2011. – 450 с. http://lib.dvfu.ru:8080/lib/item?id=chamo:103102&theme=FEFU
7. Учебники и другие книги по математике (EqWorld). [Электронный ресурс]: URL: http://eqworld.ipmnet.ru/ru/library/mathematics.htm (Дата обращения 12.05.2014).

б) дополнительная литература:

1. Кострикин А.И. Введение в алгебру – М.: Наука, 2009. – 416 с.
2. А. Г. Курош, Курс высшей алгебры – М.: Наука, 2005.

3. Д. В. Беклемишев. Курс аналитической геометрии и линейной алгебры. – М.: Наука, 2005.

4. Д. К. Фаддеев, И. С. Соминский. Задачи по высшей алгебре. – Санкт-Петербург, «Лань», 1998, - 288 с.

5. Виноградов И.М. Основы теории чисел. – СПб.: Лань, 2009. – 176 с.
6. Кострикин А.И. и др. Сборник задач по алгебре. – СПб.: Лань, 2011. – 450 с.
7. Виноградов И.М. Основы теории чисел. – М.: Наука, 1972 – 176 с.. Электронный ресурс]: URL: http://eqworld.ipmnet.ru/ru/library/books/Vinogradov1972ru.djvu (Дата обращения 12.05.2014).

Интернет-ресурсы

1. http://e.lanbook.com/books/element.php?pl1_id=9303 Василенко О.Н. Теоретико-числовые алгоритмы в криптографии: Изд-во МЦНМО.-2006

2. http://e.lanbook.com/books/element.php?pl1_id=62755 Серёдкин А.Н., Роганов В.Р., Филиппенко В.О. Основы защиты информации и информационные технологии: Учебное пособие в 3 частях. – Кн. 2: Криптография, криптоанализ и методы защиты информации в ИС и ИТ: Изд-во ПензГТУ.-2013

VI. МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

На изучение дисциплины отводится 36 часа аудиторных занятий. На практических и лабораторных занятиях преподаватель разбирает примеры по пройденной теме. Во второй части занятия студентам предлагается работать самостоятельно, выполняя задания по теме. Преподаватель контролирует работу студентов, отвечает на возникающие вопросы, подсказывает ход и метод решения. Если знаний полученных в аудитории оказалось недостаточно, студент может самостоятельно повторно прочитать теорию. После выполнения задания, студент отправляет его на проверку преподавателю. Работа должна быть отослана в формате PDF одним документом. По данному курсу разработаны методические указания.

По данному курсу разработаны методические указания:

1. Чеканов С.Г., Степанова А.А. Строение конечных полей. Учебно-методическое пособие. Изд. ДВФУ. Владивосток, 2013, 30 с.
2. Чеканов С.Г., Степанова А.А. Основы теории конечных групп. Учебно-методическое пособие. Изд. ДВФУ. Владивосток, 2014, 33 с.

VII МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Учебные аудитории кампуса ДВФУ.

Программа составлена в соответствии с требованиями ФГОС ВПО с учётом рекомендаций и ПрООП ВПО по Направление подготовки:01.04.01 Математика

Автор (ы) __С.Г. Чеканов

Рецензент (ы) _____

Программа одобрена на заседании_____

(Наименование уполномоченного органа вуза (УМК, НМС, Ученый совет)

от _____ года, протокол № _____.

Приложение 1

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«Дальневосточный федеральный университет»
(ДВФУ)

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

по дисциплине «Криптографические методы защиты информации»
Направление подготовки: 01.04.01 «Математика»
Форма подготовки очная

Владивосток
2019

План-график выполнения самостоятельной работы по дисциплине

№ п/п	Дата/сроки выполнения	Вид самостоятельной работы	Примерные нормы времени на выполнение
1. Введение	20.09 - 27.09	индивидуальное домашнее задание	1 неделя
2. Шифры простой замены	28.09 - 5.10	индивидуальное домашнее задание	1 неделя
3. Многоалфавитные шифры простой замены	6.10 - 13.10	индивидуальное домашнее задание	1 неделя
4. Совершенные шифры	14.10 - 21.10	индивидуальное домашнее задание	1 неделя
5. Поточные шифры	22.10 - 29.10	индивидуальное домашнее задание	1 неделя
6. Блочные шифры	30.10 - 8.11	индивидуальное домашнее задание	1 неделя
7. Шифры с открытым ключем	8.11 -28.11	индивидуальное домашнее задание	1 неделя
8. Хеш функции	28.11 - 18.12	индивидуальное домашнее задание	1 неделя

Материалы для самостоятельной работы студентов подготовлены в виде индивидуальных домашних заданий по каждой теме (образцы типовых ИДЗ представлены в разделе «Материалы для самостоятельной работы студентов»). Работа должна быть отправлена преподавателю на проверку. Оформление в формате PDF. Критерии оценки: студент получает максимальный балл, если работа выполнена без ошибок и оформлена в соответствии с требованиями преподавателя.

По данной дисциплине разработаны методические рекомендации:

1. Чеканов С.Г., Степанова А.А. Строение конечных полей. Учебно-методическое пособие. Изд. ДВФУ. Владивосток, 2013, 30 с.

2. Чеканов С.Г., Степанова А.А. Основы теории конечных групп. Учебно-методическое пособие. Изд. ДВФУ. Владивосток, 2014, 33 с.

Приложение 2

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«Дальневосточный федеральный университет»
(ДВФУ)

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине «Криптографические методы защиты информации»
Направление подготовки: 01.04.01 «Математика»
Форма подготовки очная

Владивосток
2019

Паспорт фонда оценочных средств

по дисциплине «Криптографические методы защиты информации»

Задача профессиональной деятельности	Объект или область знания	Код и наименование профессиональной компетенции	Код и наименование индикатора достижения профессиональной компетенции
Тип задач профессиональной деятельности: Проектно-технологический			
планирование и реализация научно-исследовательской деятельности в области математики и ее приложений	Универсальная алгебра и алгебраические методы криптографии. Методы и концепции математической логики. Алгоритмы и конструкции алгебраической геометрии.	ПК-6 способен разрабатывать концептуальные и теоретические модели решаемых задач проектной и производственно-технологической деятельности	ПК-6.1. Умеет: проводить анализ и обосновывать необходимость работы над данным проектом и оценивать его эффективность; обосновывать и защищать предлагаемый проект, доказывать его эффективность и востребованность на выбранном рынке ПК-6.2. Знает: особенности рынка данного региона ПК-6.3. Владеет: навыками работы над проектами по выбранной тематике; методами построения, анализа и применения математических моделей для оценки состояния, и прогноза развития экономических процессов и явлений; владеть опытом выражения своих мыслей и мнения
Тип задач профессиональной деятельности: организационно-управленческий			
проектирование, планирование и реализация образовательного процесса по математике в образовательном	Универсальная алгебра и алгебраические методы криптографии. Методы и концепции	ПК-7 способен к применению методов математического и алгоритмического моделирования для организации	ПК7.1. – умеет: проводить анализ необходимых для реализации проекта ресурсов; оценить временные затраты на реализацию проекта; собрать и обработать информацию для принятия управленческих

учреждении высшего и общего образования в соответствии с требованиями ФГОС основного общего образования и ФГОС среднего общего образования	математической логики. Алгоритмы и конструкции алгебраической геометрии.	управленческой деятельности	решений ПК-7.2. – знает: математические методы анализа данных о проекте; методы построения математической модели, необходимые для реализации проекта ПК-7.3. – владеет: алгоритмами математического анализа данных в профессиональной сфере; технологиями организации и распределения обязанностей в команде, реализующей проект

№ п/п	Контролируемые разделы / темы дисциплины	Коды и этапы формирования компетенций	Оценочные средства	
			текущий контроль	промежуточная аттестация
1	Введение	способен разрабатывать концептуальные и теоретические модели решаемых задач проектной и производственно-технологической деятельности (ПК-6), применению методов математического и алгоритмического моделирования для организации управленческой деятельности (ПК-7)	ПР-2	УО-2
2	Шифры простой замены	способен разрабатывать концептуальные и теоретические модели решаемых задач проектной и производственно-технологической деятельности (ПК-6),	УО-4	ПР-4
3	Многоалфавитные шифры замены	применению методов математического и алгоритмического моделирования для организации	ПР-2	ПР-4

		управленческой деятельности (ПК-7)		
4	Совершенные шифры	способен разрабатывать концептуальные и теоретические модели решаемых задач проектной и производственно-технологической деятельности (ПК-6),	ПР-2	УО-2
5	Поточные шифры	применению методов математического и алгоритмического моделирования для организации управленческой деятельности (ПК-7)	УО-4	ПР-4
6	Блочные шифры	способен разрабатывать концептуальные и теоретические модели решаемых задач проектной и производственно-технологической деятельности (ПК-6),	УО-4	ПР-4
7	Шифры с открытым ключом	применению методов математического и алгоритмического моделирования для организации управленческой деятельности (ПК-7)	ПР-2	УО-2
8	Эллиптические кривые над конечными полями	способен разрабатывать концептуальные и теоретические модели решаемых задач проектной и производственно-технологической деятельности (ПК-6),	ПР-2	УО-2
9	Хеш функции	применению методов математического и алгоритмического моделирования для организации управленческой деятельности (ПК-7)	УО-4	ПР-4

II. Шкала оценивания уровня сформированности компетенций по дисциплине «Кольца и модули»

Код и формулировка компетенции	**Этапы формирования компетенции**		**критерии**	**показатели**
ПК-6 способен разрабатывать концептуальные и теоретические модели решаемых задач проектной и производственно-технологической деятельности	знает (пороговый уровень)	особенности рынка данного региона	знание основных понятий и методов научных исследований в выбранной области математики	-способность наличие знаний основных понятий и методов научных исследований в выбранной области математики
	умеет (продвинутый)	проводить анализ и обосновывать необходимость работы над данным проектом и оценивать его эффективность; обосновывать и защищать предлагаемый проект, доказывать его эффективность и востребованность на выбранном рынке	умение применять математические методы при исследовании в выбранной области математики	наличие в диссертации результатов эффективного применения методов системного анализа
	владеет (высокий)	навыками работы над проектами по выбранной тематике; методами построения, анализа и применения математических моделей для оценки	владение основными математическим и методами научных исследований	демонстрация использования основных математических методов научных исследований

		состояния, и прогноза развития экономических процессов и явлений; владеть опытом выражения своих мыслей и мнения		
ПК-7 применению методов математического и алгоритмического моделирования для организации управленческой деятельности	знает (пороговый уровень)	математические методы анализа данных о проекте; методы построения математической модели, необходимые для реализации проекта	знание наиболее применяемых пакетов прикладных программ	наличие знаний наиболее применяемых пакетов прикладных программ
	умеет (продвинутый)	проводить анализ необходимых для реализации проекта ресурсов; оценить временные затраты на реализацию проекта; собрать и обработать информацию для принятия управленческих решений	реализация математически сложных алгоритмов в современных программных комплексах	демонстрация современных методов и технологий программирования с использованием сетей при реализации курсовых работ, ИДК и ВКР
	владеет (высокий)	алгоритмами математического анализа данных в профессиональной сфере; технологиями	использование методов и технологий программирования методами компьютерного и математического	навыками построения непротиворечивых математических теорий

		организации и распределения обязанностей в команде, реализующей проект	моделирования	

Вопросы к экзамену в третьем семестре

1. Шифр простой замены. Примеры.
2. Статистический метод криптоанализа шифра простой замены.
3. Омофоны и усиление шифров простой замены.
4. Многоалфавитные шифры простой замены.
5. Энтропия языка и способы ее вычисления.
6. Условная энтропия и теоретическая стойкость шифра.
7. Шифр Виженера и его криптоанализ.
8. Шифры не распространяющие ошибок.
9. Шифры гаммирования. Характеристики гаммы.
10. Шифр Вернама.
11. Линейные рекуррентные последовательности над конечными полями.
12. Генераторы слчайных последовательностей.
13. Генератор A5.
14. Блочные шифры.
15. Стандарт DES.
16. Асимметричные шифры.
17. Алгоритм RSA.
18. Шифр Эль Гамаля.
19. Сравнительный анализ симметричных и асимметричных шифров.
20. Хеш функции и их криптографические приложения.
21. Шифрсистемы на основе эллиптических кривых.

Примеры индивидуальных заданий

1. Введение

1.1. В чем разница между протоколом и алгоритмом?

1.2. Пусть функция f отображает пространство 200-битовых целых чисел в пространство 100-битовых целых чисел по следующему правилу.

$f(x)$ =(старшие 100 бит числа x) $\oplus$ (младшие 100 бит числа x)

Обладает ли функция $f(x)$ свойствами функции хеширования?

1.3. Можно ли утверждать, что еще не взломанный криптографический алгоритм более стоек, чем взломанный?

1.4. Сложные системы подвержены ошибкам. Назовите еще одну причину, по которой сложные системы безопасности более уязвимы.

2. Шифры простой замены

1.1. Почему алгоритм шифрования не должен содержать секретных компонентов?

1.2. Постройте пример подстановочного шифра в алфавите русского языка и оцените его стойкость.

1.3. Является ли аффинный шифр более стойким, чем подстановочный шифр?

1.4. Укажите назначение перестановочного шифра в алгоритме DES.

3. Многоалфавитные шифры простой замены

1.1. Постройте пример многоалфавитного шифра простой замены.

1.2. Является ли шифр Вернама подстановочным?

1.3. Почему многоалфавитные шифры простой замены не являются совершенными?

1.4. Может ли шифр Виженера быть совершенным?

4. **Совершенные шифры**

1.1. Постройте алгорим вычисления энтропии естественного языка.

1.2. Постройте пример совершенного шифра с конечным числом открытых и шифртекстов.

1.3. Может ли подстановочный шифр быть совершенным?

1.4. Почему многие реальные шифры не являются совершенными?

5. **Поточные шифры**

1.1. Построить расширение поля F_3 с помощью полинома x^2+2x+1.

1.2. Построить генератор линейной рекуррентной последовательности над простым конечным полем.

1.3. Разработать код над полем F_5.

1.4. На основе разработанного кода и генератора построить и реализовать на компьютере поточный шифр.

6. **Блочные шифры**

1.1 Сравнить криптографические характеристики поточных и блочных шифров.

1.2 Охарактеризовать алгоритм Фейстеля с криптографической точки зрения.

1.3 Оценить стойкость блочного шифра DES относительно атаки перебором ключей.

1.4 Построить аффинный блочный шифр размерности 5 над простым полем из пяти элементов.

7. **Шифры с открытым ключом**

1.1. Провести сравнительный анализ симметричных шифров и шифров с открытым ключом.

1.2. Привести пример алгоритма для решения проблемы факторизации целого числа.

1.3. Написать программу для вычислений с большими целыми числами.

1.4. Реализовать на компьютере алгоритм RSA.

8. **Хеш функции**

1.1. Почему практически невозможно инвертировать функцию хеширования?

1.2. Как можно имитировать случайный оракул в реальных приложениях?

1.3. Допустим, что пространство значений функции хеширования имеет размер 2^{160}. Какое время потребуется для обнаружения коллизии?

1.4. Построить пример функции хеширования.