

Минобрнауки России

Федеральное государственное бюджетное образовательное учреждение
высшего образования

«Оренбургский государственный университет»

Кафедра алгебры и дискретной математики

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

«Б.1.В.ДВ.3.1 Криптографические свойства булевых функций»

Уровень высшего образования

БАКАЛАВРИАТ

Направление подготовки

02.03.01 Математика и компьютерные науки
(код и наименование направления подготовки)

Алгоритмы и приложения компьютерной математики
(наименование направленности (профиля) образовательной программы)

Тип образовательной программы

Программа академического бакалавриата

Квалификация

Бакалавр

Форма обучения

Очная

Год набора 2018

Рабочая программа рассмотрена и утверждена на заседании кафедры

Кафедра алгебры и дискретной математики
наименование кафедры

протокол № 5 от "23" января 2018 г.

Заведующий кафедрой

Кафедра алгебры и дискретной математики  О.А. Пихтилькова
наименование кафедры подпись расшифровка подписи

Исполнители:

старший преподаватель  А.Н. Благовисная
должность подпись расшифровка подписи

СОГЛАСОВАНО:

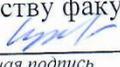
Председатель методической комиссии по направлению подготовки

02.03.01 Математика и компьютерные науки  О.А. Пихтилькова
код наименование личная подпись расшифровка подписи

Заведующий отделом комплектования научной библиотеки

 Н.Н. Грицай
личная подпись расшифровка подписи

Уполномоченный по качеству факультета

 И.В. Крючкова
личная подпись расшифровка подписи

№ регистрации _____

© Благовисная А.Н., 2018
© ОГУ, 2018

1 Цели и задачи освоения дисциплины

Цель (цели) освоения дисциплины:

- формирование у студентов теоретических знаний, практических умений и навыков решения задач теории криптографических булевых функций.

Задачи:

- изучение основных идей и фундаментальных понятий теории криптографических булевых функций;

- овладение способами задания булевых функций, используемых в криптографических конструкциях;

- овладение алгоритмами вычисления криптографических характеристик булевых функций;

- знакомство с основными идеями генерации булевых функций с криптографическими характеристиками и овладение некоторыми из методов генерации криптографических булевых функций;

- приобретение навыков программной реализации методов теории криптографических булевых функций;

- приобретение навыков решения теоретических и практических задач защиты информации, использующих аппарат теории булевых функций с криптографическими свойствами.

2 Место дисциплины в структуре образовательной программы

Дисциплина относится к дисциплинам (модулям) по выбору вариативной части блока 1 «Дисциплины (модули)»

Пререквизиты дисциплины: *Б.1.Б.14 Фундаментальная и компьютерная алгебра, Б.1.Б.16 Дискретная математика, математическая логика и их приложения в информатике и компьютерных науках*

Постреквизиты дисциплины: *Отсутствуют*

3 Требования к результатам обучения по дисциплине

Процесс изучения дисциплины направлен на формирование следующих результатов обучения

Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций	Формируемые компетенции
<p>Знать:</p> <p>- способы задания булевых функций в криптографических конструкциях;</p> <p>- характеристики булевых функций, обеспечивающие криптографическую стойкость шифрам;</p> <p>- области применения булевых функций, обладающих криптографическими свойствами;</p> <p>Уметь:</p> <p>- находить криптографические характеристики булевых функций, в том числе и с применением современных вычислительных систем;</p> <p>- находить булевы функции с требуемыми криптографическими свойствами;</p> <p>Владеть:</p> <p>- методами реализации криптографических конструкций, использующих аппарат теории криптографических булевых функций, на основе современных вычислительных систем.</p>	ОПК-4 способностью находить, анализировать, реализовывать программно и использовать на практике математические алгоритмы, в том числе с применением современных вычислительных систем
<p>Знать:</p> <p>- формулировки классических задач теории криптографических</p>	ПК-2 способностью математически корректно

Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций	Формируемые компетенции
<i>булевых функций;</i> Уметь: <i>- выполнять постановки задач теории криптографических булевых функций</i> Владеть: <i>- навыками исследования задач теории криптографических булевых функций.</i>	ставить естественнонаучные задачи, знание постановок классических задач математики

4 Структура и содержание дисциплины

4.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 5 зачетных единиц (180 академических часов).

Вид работы	Трудоемкость, академических часов	
	8 семестр	всего
Общая трудоёмкость	180	180
Контактная работа:	48,25	48,25
Лекции (Л)	24	24
Лабораторные работы (ЛР)	24	24
Промежуточная аттестация (зачет, экзамен)	0,25	0,25
Самостоятельная работа: <i>- написание реферата (Р);</i> <i>- самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий);</i> <i>- подготовка к лабораторным занятиям;</i> <i>- подготовка к устным и письменным опросам;</i> <i>- подготовка к рубежному контролю)</i>	131,75	131,75
Вид итогового контроля (зачет, экзамен, дифференцированный зачет)	диф. зач.	

Разделы дисциплины, изучаемые в 8 семестре

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
1	Определение, способы задания, числовые и метрические свойства булевых функций	40	8		8	24
2	Криптографические характеристики булевых функций	40	6		6	28
3	Методы генерации криптографических булевых функций	42	4		4	34
4	Приложения криптографических булевых функций	58	6		6	46
	Итого:	180	24		24	132
	Всего:	180	24		24	132

4.2 Содержание разделов дисциплины

№ 1 Определение, способы задания, числовые и метрические свойства булевых функций

Определение булевой функции, способы задания. Алгебраическая нормальная форма. Алгебраическая степень булевой функции. Аффинные и линейные функции. Векторное пространство булевых функций над конечным полем F_2 . Понятие булевых отображений. Вес булевой функции. Расстояние между булевыми функциями. Преобразования Фурье и Уолша-Адамара. Спектральные коэффициенты. Числовая нормальная форма булевой функции. Представление булевых функций как функций над конечными полями характеристики 2. След в конечном поле и трейс-форма булевой функции. Производные булевых функций и их свойства. Взаимная корреляция и автокорреляция. Матрица Адамара типа Сильвестра. Преобразования Уолша-Адамара в матричной форме. Понятие о классификациях булевых функций и их практических приложениях.

№ 2 Криптографические характеристики булевых функций

Понятие криптографических булевых функций. Фундаментальные принципы построения криптографических булевых функций по Шеннону.

Основные криптографические свойства булевых функций (отображений): высокая алгебраическая степень, нелинейность, уравновешенность, устойчивость, корреляционная иммунность, алгебраическая иммунность, критерии распространения. Определения и свойства криптографических характеристик. Практическая значимость каждого из криптографических свойств булевых функций. Алгоритмы нахождения криптографических свойств булевых функций.

Нелинейность как ключевая криптографическая характеристика булевых функций. Различные подходы к определению нелинейности. Максимально-нелинейные булевы функции, их виды и свойства. Роль бент-функций в криптографических преобразованиях.

№ 3 Методы генерации криптографических булевых функций

Сочетания криптографических свойств у булевой функции: проблемы, возникающие при поиске функций, обладающих несколькими криптографическими характеристиками. Основные идеи методов генерации булевых функций с криптографическими свойствами: методы случайной генерации, алгебраические методы, эвристические методы.

Конструкции бент-функций как один из способов построения криптографических булевых функций. Первичные и вторичные конструкции. Комбинации и видоизменения бент-функций при построении криптографических функций, удовлетворяющих нескольким криптографическим свойствам.

№ 4 Приложения криптографических булевых функций

Булевы функции в поточных шифрах. Регистры сдвига с линейной обратной связью. Методы усложнения, основанные на использовании нелинейных булевых функций. Алгоритм А5.

Булевы функции в блочных шифрах. Математическое описание S-блоков, основанное на аппарате булевых функций (отображений). Стандарты ГОСТ Р 34.12-2015, AES, CAST.

Булевы функции в криптографических хэш-функциях.

4.3 Лабораторные работы

№ ЛР	№ раздела	Наименование лабораторных работ	Кол-во часов
1	1	Реализация различных способов задания булевых функций.	4
2	1	Реализация алгоритмов нахождения числовых и метрических характеристик булевых функций.	4
3	2	Реализация алгоритмов нахождения криптографических характеристик булевых функций.	6
4	3	Реализация конструкций бент-функций.	2
5	3	Реализация алгоритмов получения криптографических булевых функций на основе конструкций бент-функций.	2

№ ЛР	№ раздела	Наименование лабораторных работ	Кол-во часов
6	4	Реализация генераторов на регистрах сдвига с обратной связью.	4
7	4	Исследование значений криптографических характеристик булевых функций различных криптографических конструкций.	2
		Итого:	24

5 Учебно-методическое обеспечение дисциплины

5.1 Основная литература

1. Глухов, М.М. Математическая логика. Дискретные функции. Теория алгоритмов: учебное пособие / М. М. Глухов, А. Б. Шишков. – СПб.: Лань, 2012. – 416 с.
2. Фомичев, В.М. Методы дискретной математики в криптологии [Электронный ресурс] / В.М. Фомичев. – Москва: Диалог-МИФИ, 2010. – 436 с. – Режим доступа: <http://biblioclub.ru/index.php?page=book&id=447668>
3. Сمارт, Н. Криптография [Текст] / Н. Смарт; пер. с англ. С. А. Кулешова; под ред. С. К. Ландо. – Москва: Техносфера, 2006. – 528 с.

5.2 Дополнительная литература

1. Марченков, С.С. Основы теории булевых функций: учебное пособие [Электронный ресурс] / С.С. Марченков. – Москва: Физматлит, 2014. – 136 с. – Режим доступа: <http://biblioclub.ru/index.php?page=book&id=275607>
2. Новиков, Ф.А. Дискретная математика для программистов: учеб. пособие для вузов / Ф. А. Новиков. – СПб.: Питер, 2009. – 384 с.
3. Отрыванкина, Т.М. Криптографические свойства булевых функций [Электронный ресурс]: методические указания / Т. М. Отрыванкина, А. Н. Благовисная; М-во образования и науки Рос. Федерации, Федер. гос. бюджет. образоват. учреждение высш. проф. образования «Оренбург. гос. ун-т». – Оренбург: ОГУ, 2014. – Adobe Acrobat Reader 6.0

5.3 Периодические издания

1. Прикладная математика и механика: журнал. - М.: Агентство «Роспечать», 2016.
2. Вычислительные технологии: журнал. - М.: Агентство «Роспечать», 2016.
3. Вестник компьютерных и информационных технологий: журнал. – М.: Агентство «Роспечать», 2017-2018.
4. Информационные технологии: журнал. – М.: Агентство «Роспечать», 2017-2018.

5.4 Интернет-ресурсы

1. <http://cryptography.ru/about/> – сайт посвящен вопросам математической криптографии, содержит календарь конференций, семинаров и т. п., которые полностью или частично посвящены вопросам защиты информации, а также актуальные ссылки на сайты данных научных мероприятий.
2. <http://eqworld.ipmnet.ru/indexr.htm> – международный научно-образовательный сайт «Мир математических уравнений», который содержит обширную учебную физико-математическую библиотеку и предназначен для широкого круга ученых, преподавателей вузов, инженеров, аспирантов и студентов в различных областях математики и других наук; все ресурсы сайта являются бесплатными для его пользователей).
3. <https://arxiv.org/> – крупнейший бесплатный архив электронных публикаций научных статей и их препринтов по физике, математике, астрономии, информатике и биологии.
4. <https://www.gost.ru/portal/gost/> – портал Федерального агентства по техническому регулированию и метрологии.

5.5 Программное обеспечение, профессиональные базы данных и информационные справочные системы современных информационных технологий

1. Операционная система Microsoft Windows.
2. OpenOffice/LibreOffice - свободный офисный пакет программ, включающий в себя текстовый и табличный редакторы, редактор презентаций и другие офисные приложения.
3. Бесплатное средство просмотра файлов PDF Adobe Reader.
4. Microsoft Visual Studio (лицензии по программе Microsoft Dream Spark Premium).
5. SCOPUS [Электронный ресурс]: реферативная база данных / компания Elsevier. – Режим доступа: <https://www.scopus.com/>, в локальной сети ОГУ.
6. Web of Science [Электронный ресурс]: реферативная база данных / компания Clarivate Analytics. – Режим доступа: <http://apps.webofknowledge.com/>, в локальной сети ОГУ.
7. Общероссийский математический портал Math-Net.Ru [Электронный ресурс]: профессиональная база данных для математиков – Режим доступа: http://www.mathnet.ru/index.phtml?option_lang=rus

6 Материально-техническое обеспечение дисциплины

Учебные аудитории для проведения занятий семинарского типа, для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Аудитории оснащены комплектами ученической мебели, техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Для проведения лабораторных занятий используется компьютерный класс, оснащенный компьютерной техникой.

Помещение для самостоятельной работы обучающихся оснащено компьютерной техникой подключенной к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду ОГУ.

К рабочей программе прилагаются:

- Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине;
- Методические указания для обучающихся по освоению дисциплины.