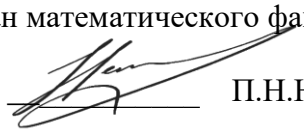
МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Ярославский государственный университет им. П.Г. Демидова

Кафедра компьютерной безопасности и математических методов обработки информации

УТВЕРЖДАЮ

Декан математического факультета


П.Н.Нестеров

«18» мая 2021 г.

Рабочая программа дисциплины
«Избранные вопросы асимметричной криптографии»

Направление подготовки
10.06.01 Информационная безопасность

Направленность (профиль)
«Методы и системы защиты информации,
информационная безопасность»

Форма обучения очная

Программа рассмотрена
на заседании кафедры компьютерной безопасности
и математических методов обработки информации
от «16» апреля 2021 года, протокол № 8

Ярославль

1. Цели освоения дисциплины

Дисциплина «Избранные вопросы асимметричной криптографии» обеспечивает приобретение фундаментальных и профессиональных знаний, умений и навыков, содействует дальнейшей фундаментализации образования, развитию логического мышления и формированию математического и общенаучного мировоззрения. Целью изучения дисциплины является овладение базовыми понятиями и методами асимметричной криптографии (криптографии с открытым ключом), ознакомление с применениями в области обеспечения информационной безопасности, решения проблем конфиденциальности, целостности и аутентификации.

2. Место дисциплины в структуре программы аспирантуры

Дисциплина «Избранные вопросы асимметричной криптографии» является факультативной дисциплиной вариативной части. Она играет важную роль для общематематической и общепрофессиональной подготовки специалиста. При ее изучении используются знания, полученные при изучении таких математических дисциплин, как “Алгебра”, "Теория чисел", "Дискретная математика", "Информатика", "Математическая логика и теория алгоритмов" и "Криптографические методы защиты информации".

3. Планируемые результаты обучения по дисциплине – знания, умения, навыки и (или) опыт деятельности, характеризующие этапы формирования компетенций и обеспечивающие достижение планируемых результатов освоения программы аспирантуры, и критерии их оценивания

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Профессиональные компетенции:

– способностью разрабатывать защитные механизмы и средства обеспечения информационной безопасности, осуществлять их настройку, регулировку, восстановление работоспособности (ПК-2);

Результаты обучения выпускника формулируются в следующих категориях:
«знать» – означает способность выпускника воспроизводить учебный материал с требуемой степенью научной точности (формулировать определение, с достаточной полнотой описывать процесс и явление);
«уметь» – означает способность выпускника решать типовые (адаптированные) задачи на основе воспроизведения алгоритма решения и его применения в конкретных стандартных условиях;
«владеть» – означает способность выпускника решать усложненные, в том числе комплексные задачи. Задачи данного уровня решаются на основе ранее приобретенных знаний и умений, с их трансформацией и применением в новых нетиповых условиях.

Код компетенции	**Планируемые результаты обучения**	**Критерии оценивания результатов обучения**		
		Пороговый уровень	**Продвинутый уровень**	**Высокий Уровень**
Способностью разрабатывать защитные механизмы и средства	**Знать:** защитные механизмы и средства обеспечения	**Знает:** защитные механизмы и средства обеспечения	**Знает:** защитные механизмы и средства обеспечения	**Знает:** защитные механизмы и средства обеспечения

обеспечения информационной безопасности, осуществлять их настройку, регулирование, восстановление работоспособности (ПК-2)	информационной безопасности. **Уметь:** осуществлять настройку, регулирование и восстановление работоспособности защитных механизмов и средств обеспечения информационной безопасности. **Владеть:** навыками настройки, регулирования и восстановления работоспособности защитных механизмов и средств обеспечения информационной безопасности.	информационной безопасности, основные понятия, результаты и методы асимметричной криптографии (криптографии с открытым ключом).	информационной безопасности, основные понятия, результаты и методы асимметричной криптографии (криптографии с открытым ключом). **Умеет:** осуществлять настройку, регулирование и восстановление работоспособности защитных механизмов и средств обеспечения информационной безопасности.	информационной безопасности, основные понятия, результаты и методы асимметричной криптографии (криптографии с открытым ключом). **Умеет:** осуществлять настройку, регулирование и восстановление работоспособности защитных механизмов и средств обеспечения информационной безопасности. **Владеет:** навыками настройки, регулирования и восстановления работоспособности защитных механизмов и средств обеспечения информационной безопасности.

4. Объем, структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 2 зачетные единицы, 72 акад.часа.

Дисциплина изучается в течение четвертого семестра. Формой итоговой промежуточной аттестации по дисциплине является зачет.

№ п/п	Темы (разделы) дисциплины, их содержание	Семестр	Виды учебных занятий и их трудоемкость (в академических часах)	Формы текущего контроля успеваемости

			лекции	практические	лабораторные	консультации	самостоятельная работа	**Форма промежуточной аттестации** ***(по семестрам)***
		4						
1	Системы шифрования с открытым ключом.	4	1				8	
2	Цифровая подпись документов.	4					8	
3	Хеш-функции.	4					8	
4	Криптосистемы на эллиптических кривых**.**	4					10	
5	Дискретное логарифмирование в мультипликативной группе конечного поля.	4					8	
6	Дискретное логарифмирование в группе точек эллиптической кривой над конечным полем.	4	1				8	
7	Протоколы распределения ключей**.**	4					8	
8	Некоторые современные направления криптографических исследований.	4	2				10	Зачет
	Всего		**4**				**68**	

Содержание разделов программы дисциплины
" Избранные вопросы асимметричной криптографии"

Тема № 1. Системы шифрования с открытым ключом.

Понятие односторонней функции и односторонней функции с «лазейкой».

Криптосистемы с открытым ключом - асимметричные системы шифрования. Вычислительно сложные задачи математики.

Ранцевые алгоритмы шифрования с открытым ключом, криптосистема Меркля-Хеллмана.

Криптосистема RSA и ее анализ. Система RSA и задача разложения натурального числа на множители.

Детерминированные методы разложения: метод пробного деления, метод “giant step – babe step”, метод Ферма, метод диофантовой аппроксимации.

Вероятностные методы разложения: р-метод Полларда (метод «Монте-Карло»),

метод непрерывных дробей, метод квадратичного решета, разложение на эллиптической кривой.

Атаки на систему RSA, не требующие разложения: случай малого секретного показателя, случай специальных открытых показателей. Атаки на основе эндоморфизмов.

Шифрование с открытым ключом для группы вычислимого порядка: бесключевое шифрование Месси – Омуры, протокол Эль-Гамаля шифрования с открытым ключом.

Криптосистема Мак-Эллиса.

Шифрование с открытым ключом для группы трудновычислимого порядка: протокол шифрования Рабина, вероятностное шифрование.

Генераторы псевдослучайных последовательностей.

Тема № 2. Цифровая подпись документов.

Подписи на группе трудновычислимого порядка.
Схема подписи RSA.
Схема подписи Рабина.
Схема подписи Фиата – Шамира.
Подписи на группе вычислимого порядка.
Схема подписи Эль-Гамаля.
Схема подписи Шнора.
Стандарты ГОСТ Р 34.10-94, ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012.
Другие схемы подписи: схема "неоспоримой" подписи.
Схема подписи "вслепую".
Сравнительный анализ схем подписи.
Скрытый канал.
Электронные платежи.
Схема подписи с восстановлением сообщения.

Тема № 3. Хеш-функции.

Ключевые и бесключевые хеш-функции. Итеративные способы построения хеш-функций. Конструкции хеш-функций.

Использование хеш-функций и блочных шифров в системах аутентификации сообщений.

Коды аутентификации сообщений MAC и коды обнаружения ошибок MDC и MIC.

Изучение стандартов современных хеш-функций ГОСТ Р 34.11-2012.

Тема № 4. Криптосистемы на эллиптических кривых.

Алгебраические кривые на евклидовой плоскости. Квадратичные кривые (квадрики, коники). Сложение точек, его свойства.

Кубические кривые, 2-местная операция сложения точек, ее свойства.

Понятие о проективном пространстве.

Проективная плоскость. Алгебраические кривые на проективной плоскости.

Особые и неособые кубические кривые. Форма Вейерштрасса.

Эллиптические кривые, свойства операции сложения точек на них.

Группа точек на эллиптической кривой.

Эллиптические кривые над конечными полями.

Порядок группы точек эллиптической кривой над конечным полем, алгоритм Чуфа.

Протоколы на эллиптических кривых: аналог системы RSA, установление сеансового ключа.

Встраивание открытого текста в координату точки.

Шифрование. Цифровая подпись.

Понятие об эллиптических функциях. Функция Вейерштрасса. Параметризация эллиптической кривой над полем комплексных чисел.

Эллиптические кривые над полем рациональных чисел, рациональные и целочисленные точки на них.

Расчет числа точек эллиптической кривой в общем случае: многочлены деления, алгоритм Чуфа

Расчет числа точек эллиптической кривой над расширенным полем.

Расчет числа точек эллиптической кривой над простыми полями.

Эллиптические кривые с комплексным умножением.

Протоколы для электронных платежей.

Тема № 5. Дискретное логарифмирование в мультипликативной группе конечного поля.

Метод базы разложения.

Логарифмирование в простом поле методом решета числового поля.

Логарифмирование в расширенном поле.

Группа классов квадратичного поля.

Логарифмирование в группе функций Лукаша.

Связь между задачами Диффи – Хеллмана и дискретного логарифмирования.

Тема № 6. Дискретное логарифмирование в группе точек эллиптической кривой над конечным полем.

Задача дискретного логарифмирования на эллиптической кривой.

Универсальные методы логарифмирования.

Метод Гельфонда.

Метод встреч посередине и “giant step – babe step”.

Метод Полларда.

Метод встречи на случайном дереве.

Сравнение сложности логарифмирования на эллиптической кривой и в конечном поле.

Влияние комплексного умножения на сложность логарифмирования.

Логарифмирование с использованием функции Вейля.

Время жизни общего открытого ключа криптосистемы, основанной на дискретном логарифмировании: мультипликативная группа поля, группа точек эллиптической кривой.

Логарифмирование якобиане гиперэллиптической кривой.

Требования к эллиптической кривой.

Тема № 7. Протоколы распределения ключей.

Понятие криптографического протокола.

Передача ключей с использованием симметричной системы шифрования. Двусторонние и трехсторонние протокола. Протокол Kerberos.

Передача ключей с использованием асимметричной системы шифрования. Сертификаты открытых ключей.

Открытое распределение ключей.

Предварительное распределение ключевых материалов, схема Блома.

Возможные атаки на протоколы распределения ключей. Управление ключами.

Тема № 8. Некоторые современные направления криптографических исследований.

Криптография, базирующаяся на группах.

Задание групп образующими и определяющими соотношениями. .

Группы кос и криптопротоколы на их основе.

Криптосистемы на базе групп, заданных образующими и определяющими соотношениями.

Протокол Anschel-Anschel-Goldfeld выработки общего секретного ключа на базе коммутаторов элементов групп.

Протокол Ko -- Lee -- Cheon -- Han -- Kang -- Park выработки общего секретного ключа на базе проблемы сопряженности для группы кос.

Протокол Wang -- Cao -- Okamoto -- Shao выработки общего секретного ключа на базе некоммутативного моноида.

Протокол Сидельникова В. М. -- Черепнева М. А. -- Ященко В. Ю на базе некоммутативных полугрупп.

Протокол Stickel на базе конечной (периодической) некоммутативной группы.

Протоколы, базирующиеся на групповых автоморфизмах и эндоморфизмах: протокол Mahalanobis, протокол Habeeb -- Kahrobaei -- Koupparis -- Shpilrain.

Протоколы аутентификации, основанные на некоторых "трудных" алгоритмических проблемах теории групп: протокол Романькова -- Григорьева -- Шпильрайна, протокол Шпильрайна -- Ушакова, протокол Мегрелишвили -- Джинджихадзе.

Криптосистема Росошека.

5. Образовательные технологии, используемые при осуществлении образовательного процесса по дисциплине

В процессе обучения используются следующие образовательные технологии:

Вводная лекция – дает первое целостное представление о дисциплине и ориентирует студента в системе изучения данной дисциплины. Студенты знакомятся с назначением и задачами курса, его ролью и местом в системе учебных дисциплин и в системе подготовки в целом. Дается краткий обзор курса, история развития науки и практики, достижения в этой сфере, имена известных ученых, излагаются перспективные направления исследований. На этой лекции высказываются методические и организационные особенности работы в рамках данной дисциплины, а также дается анализ рекомендуемой учебно-методической литературы.

Академическая лекция (или лекция общего курса) – последовательное изложение материала, осуществляемое преимущественно в виде монолога преподавателя. Требования к академической лекции: современный научный уровень и насыщенная информативность, убедительная аргументация, доступная и понятная речь, четкая структура и логика, наличие ярких примеров, научных доказательств, обоснований, фактов.

Практическое занятие – занятие, посвященное освоению конкретных умений и навыков и закреплению полученных на лекции знаний.

6. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного программного обеспечения и информационных справочных систем (при необходимости).

В процессе осуществления образовательного процесса используются:

– для формирования текстов материалов для промежуточной и текущей аттестации
– программы Microsoft Office, издательская система MikTex;

– для поиска учебной литературы библиотеки ЯрГУ – Автоматизированная библиотечная информационная система "БУКИ-NEXT" (АБИС "Буки-Next").

7. Перечень основной и дополнительной учебной литературы, необходимых для освоения дисциплины

а) основная литература

1. Алферов А.П. Основы криптографии. Учебное пособие. / А.П. Алферов, А. Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. М.: Гелиос АРВ, 2002. 480 с.
2. Коблиц Н. Курс теории чисел и криптографии / Н. Коблиц. М.: Научное издательство "ТВП", 2001. 254 с.
3. Маховенко Е.Б. Теоретическая криптография / Е.Б. Маховенко, А.Г. Ростовцев. Санкт-Петербург. АНО НПО "Профессионал". ООО "Интерлайн", 2004
4. Романьков В.А. Введение в криптографию. Курс лекций / В.А. Романьков. - М.: ФОРУМ, 2012. - 240 с.
5. Ростовцев А.Г. Введение в криптографию с открытым ключом / А.Г. Ростовцев, Е.Б.Маховенко. Санкт-Петербург. НПО "Мир и семья". ООО "Интерлайн", 2001. 336 с.
6. Саломаа А. Криптография с открытым ключом. М: Мир, 1996.
7. Кукина Е.Г. Сборник задач и упражнений по криптографии / Е.Г. Кукина, В.А. Романьков, Омск, Изд-во. ОГУ им. Ф.М. Достоевского, 2013. 148 с.
8. Введение в криптографию: новые математические дисциплины / под ред. В. В. Ященко, СПб., Питер, 2001, 287с.
9. Черемушкин А.В. Криптографические протоколы. Основные свойства и уязвимости / А.В. Черемушкин. М.: Издательский дом "Академия", 2009.
10. Чмора А. Современная прикладная криптография / А.Л. Чмора. М.: Гелиос АРВ, 2002. 256 с.
11. Хенк К.А. ван Тилборг. Основы криптологии. Профессиональное руководство и интерактивный учебник. М.: Мир, 2005. 465 с.

б) дополнительная литература

1. Зензин О.С. Стандарт криптографической защиты AES. Конечные поля / О.С. Зензин, М.А. Иванов. КУДИЦ-ОБРАЗ, 2003.
2. Столлингс В. Криптография и защита сетей. Принципы и практика.-- 2-е изд. М.: Гелиос АРВ, 2001.
3. Бабаш А.В., Шанкин Г.П. История криптографии. Учебное пособие. М.: “Гелиос АРВ”, 2002
4. Нечаев В.И. Элементы криптографии. Основы теории защиты информации. М.: Высшая школа, 1999.
5. Ноден П., Китте К. Алгебраическая алгоритмика /под ред. Л.С. Казарина. М: Мир, 1999.
6. Ростовцев А.Г. Алгебраические основы криптографии / А.Г. Ростовцев. Санкт-Петербург. НПО "Мир и семья". ООО "Интерлайн", 2000. 354 с.
7. Мао В. Современная криптография. Теория и практика / В. Мао. М.: Издательский дом "Вильямс", 2005. 768 с.
8. Харин Ю.С. Математические и компьютерные основы криптологии / Харин Ю.С., Берник В.И., Матвеев Г.В., Агиевич С.В. Минск: ООО "Новое знание", 2003. 382 с.
9. Шнайер Б. Прикладная криптография / Б. Шнайер. М.: Триумф, 2002. 816 с.
10. Под ред. Погорелова Б.А., Сачкова В.Н. Словарь криптографических терминов. М.: МЦНМО, 2006.

в) ресурсы сети «Интернет»

1.Электронные каталоги НБ ЯрГУ

(http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php) содержат библиографические записи всех видов документов, составляющих фонд библиотеки, на русском и иностранных языках.

2. Личный кабинет (http://lib.uniyar.ac.ru/opac/bk_login.php) возможность получения on-line доступа к списку выданной в автоматизированном режиме литературы, просмотра и копирования электронных версий изданий сотрудников университета (учеб. и метод. пособия, тексты лекций и т.д.) Для работы в «Личном кабинете» необходимо зайти на сайт Научной библиотеки ЯрГУ с любой точки, имеющей доступ в Internet, в пункт меню *«Электронный каталог»*; пройти процедуру авторизации, выбрав вкладку *«Авторизация»*, и заполнить представленные поля информации.

3.Электронная библиотека учебных материалов ЯрГУ

(http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php) содержит более 2500 полных текстов учебных и учебно-методических материалов по основным изучаемым дисциплинам, изданных в университете. Доступ в сети университета, либо по логину/паролю.

4.Электронный архив ЯрГУ

(http://elar.uniyar.ac.ru/jspui/community-list) представляет собой коллекцию полнотекстовых электронных публикаций в области научных исследований. База данных предназначена для использования в учебных и научных целях, облегчая доступ к информации о научных работах и их содержанию.

5. Электронная картотека «Книгообеспеченность»

(http://www.lib.uniyar.ac.ru/opac/bk_bookreq_find.php)

раскрывает учебный фонд научной библиотеки ЯрГУ, предоставляет оперативную информацию о состоянии книгообеспеченности дисциплин основной и дополнительной литературой, а также цикла дисциплин и специальностей. Электронная картотека «Книгообеспеченность» доступна в сети университета и через Личный кабинет.

Русскоязычные электронные ресурсы (внешние)

1. Научная электронная библиотека (НЭБ) (http://elibrary.ru) – это крупнейший российский информационный портал, содержащий рефераты и полные тексты более 12 млн. научных статей и публикаций. **ЯрГУ выписывает в электронном виде 66 журналов,** более 2 500 наименований журналов на английском и русском языках находятся в свободном доступе. Для работы с полными текстами необходимо зарегистрироваться. Доступ к полным текстам журналов в сети университета.

2. Электронная библиотека диссертаций Российской государственной библиотеки (http://diss.rsl.ru) содержит более 580 000 полных текстов диссертаций и авторефератов. Доступ осуществляется в сети университета.

8. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине включает в свой состав специальные помещения:

-учебные аудитории для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации;

-помещения для самостоятельной работы;
-помещения для хранения и профилактического обслуживания оборудования.

Специальные помещения укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления информации большой аудитории.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду организации.

Число посадочных мест в лекционной аудитории больше либо равно списочному составу потока, а в аудитории для практических занятий (семинаров) – списочному составу группы обучающихся.

Автор(ы) :

Зав. кафедрой компьютерной безопасности и математических методов обработки информации, д.ф.-м.н. Дурнев В.Г.

_____
(подпись)

Приложение к №1 рабочей программе дисциплины
«Избранные вопросы асимметричной криптографии»

Оценочные средства
для проведения текущей и/или промежуточной аттестации аспирантов
по дисциплине

1. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Алферов А.П. Основы криптографии. Учебное пособие. / А.П. Алферов, А. Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. М.: Гелиос АРВ, 2002. 480 с.
Романьков В.А. Введение в криптографию. Курс лекций / В.А. Романьков. - М.: ФОРУМ, 2012. - 240 с.
Кукина Е.Г. Сборник задач и упражнений по криптографии / Е.Г. Кукина, В.А. Романьков, Омск, Изд-во. ОГУ им. Ф.М. Достоевского, 2013. 148 с.

Домашние задания по теме № 1 **"Системы шифрования с открытым ключом. "**
Задания для самостоятельного решения № 86 - 99 из параграфа 9 и № 100 - 123 из параграфа 10 сборника задач
Кукина Е.Г. Сборник задач и упражнений по криптографии / Е.Г. Кукина, В.А. Романьков, Омск, Изд-во. ОГУ им. Ф.М. Достоевского, 2013. 148 с.
Задания для самостоятельного решения № 1 - 6 из главы IX учебника
Алферов А.П. Основы криптографии. Учебное пособие. / А.П. Алферов, А. Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. М.: Гелиос АРВ, 2002. 480 с.
Задания для самостоятельного решения № 1 - 5 из главы XIV учебника
Алферов А.П. Основы криптографии. Учебное пособие. / А.П. Алферов, А. Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. М.: Гелиос АРВ, 2002. 480 с.

Домашние задания по теме № 3 **"Хеш-функции. "**
Задания для самостоятельного решения № 192 - 194 из параграфа 23 сборника задач
Кукина Е.Г. Сборник задач и упражнений по криптографии / Е.Г. Кукина, В.А. Романьков, Омск, Изд-во. ОГУ им. Ф.М. Достоевского, 2013. 148 с.
Задания для самостоятельного решения № 1 - 6 из главы XIII учебника
Алферов А.П. Основы криптографии. Учебное пособие. / А.П. Алферов, А. Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. М.: Гелиос АРВ, 2002. 480 с.

Домашние задания по теме № 7 **"Протоколы распределения ключей."**
Задания для самостоятельного решения № 171 - 173 из параграфа 18 сборника задач
Кукина Е.Г. Сборник задач и упражнений по криптографии / Е.Г. Кукина, В.А. Романьков, Омск, Изд-во. ОГУ им. Ф.М. Достоевского, 2013. 148 с.
Задания для самостоятельного решения № 1 - 10 из главы XV учебника
Алферов А.П. Основы криптографии. Учебное пособие. / А.П. Алферов, А. Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. М.: Гелиос АРВ, 2002. 480 с.
Задания для самостоятельного решения № 1 - 5 из главы XVI учебника
Алферов А.П. Основы криптографии. Учебное пособие. / А.П. Алферов, А. Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. М.: Гелиос АРВ, 2002. 480 с.

1.1 Список вопросов и (или) заданий для проведения промежуточной аттестации

Вопросы к зачету по дисциплине

"Избранные вопросы асимметричной криптографии "
(4 семестр)

Тема № 1. Системы шифрования с открытым ключом.

Понятие односторонней функции и односторонней функции с «лазейкой».

Криптосистемы с открытым ключом - асимметричные системы шифрования. Вычислительно сложные задачи математики.

Ранцевые алгоритмы шифрования с открытым ключом, криптосистема Меркля-Хеллмана.

Криптосистема RSA и ее анализ. Система RSA и задача разложения натурального числа на множители.

Детерминированные методы разложения: метод пробного деления, метод “giant step – babe step”, метод Ферма, метод диофантовой аппроксимации.

Вероятностные методы разложения: р-метод Полларда (метод «Монте-Карло»), метод непрерывных дробей, метод квадратичного решета, разложение на эллиптической кривой.

Атаки на систему RSA, не требующие разложения: случай малого секретного показателя, случай специальных открытых показателей. Атаки на основе эндоморфизмов.

Шифрование с открытым ключом для группы вычислимого порядка: бесключевое шифрование Месси – Омуры, протокол Эль-Гамаля шифрования с открытым ключом.

Криптосистема Мак-Эллиса.

Шифрование с открытым ключом для группы трудновычислимого порядка: протокол шифрования Рабина, вероятностное шифрование.

Генераторы псевдослучайных последовательностей.

Тема № 2. Цифровая подпись документов.

Подписи на группе трудновычислимого порядка.
Схема подписи RSA.
Схема подписи Рабина.
Схема подписи Фиата – Шамира.
Подписи на группе вычислимого порядка.
Схема подписи Эль-Гамаля.
Схема подписи Шнора.
Стандарты ГОСТ Р 34.10-94, ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012.
Другие схемы подписи: схема "неоспоримой" подписи.
Схема подписи "вслепую".
Сравнительный анализ схем подписи.
Скрытый канал.
Электронные платежи.
Схема подписи с восстановлением сообщения.

Тема № 3. Хеш-функции.

Ключевые и бесключевые хеш-функции. Итеративные способы построения хеш-функций. Конструкции хеш-функций.

Использование хеш-функций и блочных шифров в системах аутентификации сообщений.

Коды аутентификации сообщений MAC и коды обнаружения ошибок MDC и MIC.

Изучение стандартов современных хеш-функций ГОСТ Р 34.11-2012.

Тема № 4. Криптосистемы на эллиптических кривых.

Алгебраические кривые на евклидовой плоскости. Квадратичные кривые (квадрики, коники). Сложение точек, его свойства.

Кубические кривые, 2-местная операция сложения точек, ее свойства.

Понятие о проективном пространстве.

Проективная плоскость. Алгебраические кривые на проективной плоскости.

Особые и неособые кубические кривые. Форма Вейерштрасса.

Эллиптические кривые, свойства операции сложения точек на них.

Группа точек на эллиптической кривой.

Эллиптические кривые над конечными полями.

Порядок группы точек эллиптической кривой над конечным полем, алгоритм Чуфа.

Протоколы на эллиптических кривых: аналог системы RSA, установление сеансового ключа.

Встраивание открытого текста в координату точки.

Шифрование. Цифровая подпись.

Понятие об эллиптических функциях. Функция Вейерштрасса. Параметризация эллиптической кривой над полем комплексных чисел.

Эллиптические кривые над полем рациональных чисел, рациональные и целочисленные точки на них.

Расчет числа точек эллиптической кривой в общем случае: многочлены деления, алгоритм Чуфа

Расчет числа точек эллиптической кривой над расширенным полем.

Расчет числа точек эллиптической кривой над простыми полями.

Эллиптические кривые с комплексным умножением.

Протоколы для электронных платежей.

Тема № 5. Дискретное логарифмирование в мультипликативной группе конечного поля.

Метод базы разложения.

Логарифмирование в простом поле методом решета числового поля.

Логарифмирование в расширенном поле.

Группа классов квадратичного поля.

Логарифмирование в группе функций Лукаша.

Связь между задачами Диффи – Хеллмана и дискретного логарифмирования.

Тема № 6. Дискретное логарифмирование в группе точек эллиптической кривой над конечным полем.

Задача дискретного логарифмирования на эллиптической кривой.

Универсальные методы логарифмирования.

Метод Гельфонда.

Метод встреч посередине и “giant step – babe step”.

Метод Полларда.

Метод встречи на случайном дереве.

Сравнение сложности логарифмирования на эллиптической кривой и в конечном поле.

Влияние комплексного умножения на сложность логарифмирования.

Логарифмирование с использованием функции Вейля.

Время жизни общего открытого ключа криптосистемы, основанной на дискретном логарифмировании: мультипликативная группа поля, группа точек эллиптической кривой.

Логарифмирование якобиане гиперэллиптической кривой.

Требования к эллиптической кривой.

Тема № 7. Протоколы распределения ключей.

Понятие криптографического протокола.

Передача ключей с использованием симметричной системы шифрования. Двусторонние и трехсторонние протокола. Протокол Kerberos.

Передача ключей с использованием асимметричной системы шифрования. Сертификаты открытых ключей.

Открытое распределение ключей.

Предварительное распределение ключевых материалов, схема Блома.

Возможные атаки на протоколы распределения ключей. Управление ключами.

Тема № 8. Некоторые современные направления криптографических исследований.

Криптография, базирующаяся на группах.

Задание групп образующими и определяющими соотношениями. .

Группы кос и криптопротоколы на их основе.

Криптосистемы на базе групп, заданных образующими и определяющими соотношениями.

Протокол Anschel-Anschel-Goldfeld выработки общего секретного ключа на базе коммутаторов элементов групп.

Протокол Ko -- Lee -- Cheon -- Han -- Kang -- Park выработки общего секретного ключа на базе проблемы сопряженности для группы кос.

Протокол Wang -- Cao -- Okamoto -- Shao выработки общего секретного ключа на базе некоммутативного моноида.

Протокол Сидельникова В. М. -- Черепнева М. А. -- Ященко В. Ю на базе некоммутативных полугрупп.

Протокол Stickel на базе конечной (периодической) некоммутативной группы.

Протоколы, базирующиеся на групповых автоморфизмах и эндоморфизмах: протокол Mahalanobis, протокол Habeeb -- Kahrobaei -- Koupparis -- Shpilrain.

Протоколы аутентификации, основанные на некоторых "трудных" алгоритмических проблемах теории групп: протокол Романькова -- Григорьева -- Шпильрайна, протокол Шпильрайна -- Ушакова, протокол Мегрелишвили -- Джинджихадзе.

Криптосистема Росошека.

Приложение № 2 к рабочей программе дисциплины
"Избранные вопросы асимметричной криптографии"

Методические указания для аспирантов по освоению дисциплины

Для успешного освоения дисциплины важно самостоятельное изучение теоретического материала, решение достаточно большого набора хорошо подобранных задач, как в аудитории, так и самостоятельно в качестве домашних заданий. Примеры решения задач разбираются на практических занятиях, при необходимости по наиболее трудным темам проводятся дополнительные консультации. Основная цель решения задач – помочь усвоить фундаментальные понятия, методы и теоремы теории алгоритмов, научиться определять сложность вычислений. Для решения задач необходимо не только знать, но и понимать теоретический материал. Поэтому в процессе изучения дисциплины рекомендуется регулярная работа с рекомендованной литературой.

Большое внимание должно быть уделено выполнению домашней работы. В качестве заданий для самостоятельной работы дома аспирантам предлагаются задачи, аналогичные разобранным на практических занятиях или более сложные, которые являются результатом объединения нескольких базовых задач.

Для проверки и контроля усвоения теоретического материала, приобретенных практических навыков работы с основными понятиями в течение обучения проводятся мероприятия текущей аттестации в виде устного опроса на занятиях и консультациях и разбору некоторых заданий для самостоятельной работы.

Аспиранты сдают зачет во втором семестре. Зачет проводится на основании выполнения домашних заданий, контрольной работы и собеседования на основании списка вопросов к зачету, который охватывает полностью всю программу дисциплины.

Учебно-методическое обеспечение самостоятельной работы аспирантов по дисциплине

В качестве учебно-методического обеспечения рекомендуется использовать литературу, указанную в разделе № 7 данной рабочей программы