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 протоколы

Направление подготовки: 01.04.01 Математика
Форма подготовки: очная

Школа естественных наук
Кафедра алгебры, геометрии и анализа

курс 2 семестр 4
лекции не предусмотрены.
практические занятия 36 час.
семинарские занятия ___час.
лабораторные работы __ час.
самостоятельная работа 72 час.
всего часов аудиторной нагрузки 36 час.
контрольные работы предусмотрены
зачет 4 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 (ая) кафедрой к.ф.-м.н., профессор Р.П.Шепелева
Составитель (ли): 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 протоколы»

Рабочая программа учебной дисциплины «Криптографические протоколы» разработана для студентов 1 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 3 ЗЕ (108 час.). Учебным планом предусмотрены практические занятия (36 час.), самостоятельная работа студента (72 час). Дисциплина «Криптографические протоколы» входит в обязательную часть цикла дисциплин образовательной программы, реализуется на 2 курсе, во 4 семестре.

Дисциплина «Криптографические протоколы» логически и содержательно связана с такими курсами, как «Криптографические методы защиты информации», «Алгебраические основы криптографии», «Аксиоматические теории». Содержание дисциплины охватывает круг вопросов, связанных с проблемой формализации понятия криптографического протокола, оценкой стойкости протоколов по отношению к атакам, построением протоколов. Курс построен на таких ранее изученных дисциплинах как «Криптографические методы защиты информации», «Математическая логика».

Цель преподавания дисциплины: - знакомство студентов с современными криптографическими протоколами.

Задачи преподавания дисциплины:

1. овладение основными концепциями информационной безопасности;

2. ознакомление с современными криптографическими протоколами;

3. изучение основных понятий и конструкций для построения протоколов;

4. применение полученных знаний при построении моделей каналов связи.

Для успешного изучения дисциплины «Криптографические протоколы» у обучающихся должны быть сформированы следующие предварительные компетенции:

- способность видеть прикладные аспекты таких математических теорий как алгебра, теория вероятностей, теория чисел;

- умение строить примеры абстрактных математических конструкций;

- умение анализировать теоретическую и практическую возможность реализации сложных алгоритмов;

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

Общепрофессиональные компетенции выпускников и индикаторы их достижения:

Наименование категории (группы) общепрофессиональных компетенций	**Код и наименование общепрофессиональной компетенции**	**Код и наименование индикатора достижения общепрофессиональной компетенции**
Теоретические и практические основы профессиональной деятельности	ОПК-2 способен строить и анализировать математические модели в современном естествознании, технике, экономике и управлении	ОПК-2.1 умеет: строить и анализировать математические модели в современном естествознании, технике, экономике и управлении ОПК-2.2 знает: Основные методы построения и анализа математических моделей ОПК-2.3 владеет: методами построения и анализа математических моделей в современном естествознании, технике,

Профессиональные компетенции выпускников и индикаторы их достижения:

Задача профессиональной деятельности	Объект или область знания	Код и наименование профессиональной компетенции	Код и наименование индикатора достижения профессиональной компетенции
Тип задач профессиональной деятельности: Научно-исследовательский			
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-5 способен разрабатывать и применять математические методы для решения задач научной и проектно-технологической деятельности	ПК-5.1. Умеет: анализировать поставленную задачу и находить алгоритм ее решения; выбирать оптимальные системы программирования, наиболее подходящие для решения поставленной задачи ПК-5.2. Знает: современные методы цифровой обработки изображений и средства компьютерной графики ПК-5.3. Владеет: методами моделирования информационных процессов; навыками работы над производственным проектом в составе группы научных специалистов

I. СТРУКТУРА И СОДЕРЖАНИЕ ТЕОРЕТИЧЕСКОЙ ЧАСТИ КУРСА

Лекции не предусмотрены

II. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКОЙ ЧАСТИ КУРСА

Практические занятия (36 час.)

Занятие 1. Введение (4 часа).

Рассматриваются примеры криптографических протоколов. Строятся собственные простейшие протоколы и оцениваются их сильные и слабые стороны.

Занятие 2. Криптографические хеш-функции (4 часа).

Рассматриваются примеры хеш функций. Строятся примеры хеш-функций. Оценивается криптографическая стойкость функций хеширования.

Занятие 3. Коды аутентификации (4 часа).

На основе комбинаторных и алгебраических объектов строятся коды аутентификации. Изучаются примеры оптимальных кодов аутентификации.

Занятие 4. Схемы цифровых подписей (4 часа).

Рассматриваются примеры цифровых подписей основанных на симметричных и асимметричных шифрах.

Занятие 5. Протоколы идентификации (4 часа).

Протоколы слабой парольной идентификации. Протоколы типа «запрос-ответ».

Занятие 6. Протоколы с нулевым разглашением (4 часа).

Протоколы привязки к биту. Игровые протоколы. Аргумент с нулевым разглашением.

Занятие 7. Протоколы передачи ключей (4 часа).

Передача ключей с использованием симметричного шифрования. Передача ключей с использованиес асимметричного шифрования.

Занятие 8. Открытое распределение ключей (4 часа).

Виды протоколов открытого распределения ключей и их свойства. Протокол Диффи-Хеллмана и его усиление. Аутентифицированные протоколы.

Занятие 9. Предварительное распределение ключей (4 часа).

Схемы предварительного распределения ключей в сети связи. Групповые протоколы.

III. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине «Криптографические протоколы» 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 строить и анализировать математические модели в современном естествознании, технике, экономике и управлении (ОПК-2); способен разрабатывать и применять математические методы решения задач научной и проектно-технологической деятельности (ПК-5)	УО-3 УО-4	УО-2

2	Хеш-функции	способен строить и анализировать математические модели в современном естествознании, технике, экономике и управлении (ОПК-2); способен разрабатывать и применять математические методы решения задач научной и проектно-технологической деятельности (ПК-5)	ПР-2	УО-2
3	Коды аутентификации	способен строить и анализировать математические модели в современном естествознании, технике, экономике и управлении (ОПК-2); способен разрабатывать и применять математические методы решения задач научной и проектно-технологической деятельности (ПК-5)	ПР-2	ПР-4
4	Схемы цифровой подписи	способен строить и анализировать математические модели в современном естествознании, технике, экономике и управлении (ОПК-2); способен разрабатывать и применять математические методы решения задач научной и проектно-технологической деятельности (ПК-5)	УО-3 УО-4	ПР-4
5	Протоколы идентификации	способен строить и анализировать математические модели в современном естествознании, технике, экономике и управлении (ОПК-2);	УО-3 УО-4	УО-2

		способен разрабатывать и применять математические методы решения задач научной и проектно-технологической деятельности (ПК-5)		
6	Протоколы с нулевым разглашением	способен строить и анализировать математические модели в современном естествознании, технике, экономике и управлении (ОПК-2); способен разрабатывать и применять математические методы решения задач научной и проектно-технологической деятельности (ПК-5)	ПР-2	УО-2
7	Протоколы передачи ключей	способен строить и анализировать математические модели в современном естествознании, технике, экономике и управлении (ОПК-2); способен разрабатывать и применять математические методы решения задач научной и проектно-технологической деятельности (ПК-5)	ПР-2	ПР-4
8	Открытое распределение ключей	способен строить и анализировать математические модели в современном естествознании, технике, экономике и управлении (ОПК-2); способен разрабатывать и применять математические методы решения задач научной и проектно-технологической деятельности (ПК-5)	УО-3 УО-4	УО-2

9	Предварительное распределение ключей	способен строить и анализировать математические модели в современном естествознании, технике, экономике и управлении (ОПК-2); способен разрабатывать и применять математические методы решения задач научной и проектно-технологической деятельности (ПК-5)	ПР-2	УО-2

Типовые контрольные задания и экзаменационные вопросы представлены в Приложении 2.

V. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

1. а) основная литература:

1. Черемушкин А.В. Криптографические протоколы. Основные свойства и уязвимости: учебное пособие. – М.: «Академия», 2009, 272 http://lib.dvfu.ru:8080/lib/item?id=chamo:291200&theme=FEFU
2. Б. Я. Рябко, А. Н. Фионов. Криптографические методы защиты информации: учебное пособие для вузов. Москва: Горячая линия - Телеком, 2005. http://lib.dvfu.ru:8080/lib/item?id=chamo:238870&theme=FEFU
3. О.Р. Лапонина Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия; учеб. пособие для студ. вузов [под ред. В.А. Сухомлина] М.: Интернет-Университет Информационных Технологий : БИНОМ. Лаборатория знаний, 2007 http://lib.dvfu.ru:8080/lib/item?id=chamo:382720&theme=FEFU

б) дополнительная литература:

1. Виноградов И.М. Основы теории чисел. – М.: Наука, 1972 – 176 с.

2. Кострикин А.И. и др. Сборник задач по алгебре. – СПб.: Лань, 2011. – 450 с.

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

VI. МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

На изучение дисциплины отводится 126 часов аудиторных занятий. На лекциях преподаватель объясняет теоретический материал. Вводит основные понятия, определения, свойства. Формулирует и доказывает теоремы. Приводит примеры. Необходимо поддерживать непрерывный контакт с аудиторией, отвечать на возникающие у студентов вопросы. 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 лекцию. 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..

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 протоколы»
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. Хеш-функции	28.09 - 5.10	индивидуальное домашнее задание	1 неделя
3. Коды аутентификации	6.10 - 13.10	индивидуальное домашнее задание	1 неделя
4. Схемы цифровой подписи	14.10 - 21.10	индивидуальное домашнее задание	1 неделя
5. Протоколы идентификации	22.10 - 29.10	индивидуальное домашнее задание	1 неделя
6. Протоколы с нулевым разглашением	30.10 - 8.11	индивидуальное домашнее задание	1 неделя
7. Протоколы передачи ключей	8.11 -28.11	индивидуальное домашнее задание	1 неделя
8. Распределение ключей	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.

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 протоколы»
Направление подготовки: 01.04.01 «Математика»
Форма подготовки очная

Владивосток
2019

Паспорт фонда оценочных средств

по дисциплине «Криптографические протоколы»

Общепрофессиональные компетенции выпускников и индикаторы их достижения:

Наименование категории (группы) общепрофессиональных компетенций	**Код и наименование общепрофессиональной компетенции**	**Код и наименование индикатора достижения общепрофессиональной компетенции**
Теоретические и практические основы профессиональной деятельности	ОПК-2 способен строить и анализировать математические модели в современном естествознании, технике, экономике и управлении	ОПК-2.1 умеет: строить и анализировать математические модели в современном естествознании, технике, экономике и управлении ОПК-2.2 знает: Основные методы построения и анализа математических моделей ОПК-2.3 владеет: методами построения и анализа математических моделей в современном естествознании, технике,

Профессиональные компетенции выпускников и индикаторы их достижения:

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

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-5 способен разрабатывать и применять математические методы для решения задач научной и проектно-технологической деятельности	ПК-5.1. Умеет: анализировать поставленную задачу и находить алгоритм ее решения; выбирать оптимальные системы программирования, наиболее подходящие для решения поставленной задачи ПК-5.2. Знает: современные методы цифровой обработки изображений и средства компьютерной графики ПК-5.3. Владеет: методами моделирования информационных процессов; навыками работы над производственным проектом в составе группы научных специалистов

№ п/п	Контролируемые разделы / темы дисциплины	Коды и этапы формирования компетенций	Оценочные средства	
			текущий контроль	промежуточная аттестация
1	Введение	способен строить и анализировать математические модели в современном естествознании, технике, экономике и управлении (ОПК-2); способен разрабатывать и применять математические	УО-3 УО-4	УО-2

		методы решения задач научной и проектно-технологической деятельности (ПК-5)		
2	Хеш-функции	способен строить и анализировать математические модели в современном естествознании, технике, экономике и управлении (ОПК-2); способен разрабатывать и применять математические методы решения задач научной и проектно-технологической деятельности (ПК-5)	ПР-2	УО-2
3	Коды аутентификации	способен строить и анализировать математические модели в современном естествознании, технике, экономике и управлении (ОПК-2); способен разрабатывать и применять математические методы решения задач научной и проектно-технологической деятельности (ПК-5)	ПР-2	ПР-4
4	Схемы цифровой подписи	способен строить и анализировать математические модели в современном естествознании, технике, экономике и управлении (ОПК-2); способен разрабатывать и применять математические методы решения задач научной и проектно-технологической деятельности (ПК-5)	УО-3 УО-4	ПР-4

5	Протоколы идентификации	способен строить и анализировать математические модели в современном естествознании, технике, экономике и управлении (ОПК-2); способен разрабатывать и применять математические методы решения задач научной и проектно-технологической деятельности (ПК-5)	УО-3 УО-4	УО-2
6	Протоколы с нулевым разглашением	способен строить и анализировать математические модели в современном естествознании, технике, экономике и управлении (ОПК-2); способен разрабатывать и применять математические методы решения задач научной и проектно-технологической деятельности (ПК-5)	ПР-2	УО-2
7	Протоколы передачи ключей	способен строить и анализировать математические модели в современном естествознании, технике, экономике и управлении (ОПК-2); способен разрабатывать и применять математические методы решения задач научной и проектно-технологической деятельности (ПК-5)	ПР-2	ПР-4
8	Открытое распределение ключей	способен строить и анализировать математические модели в современном естествознании, технике, экономике и управлении	УО-3 УО-4	УО-2

		(ОПК-2); способен разрабатывать и применять математические методы решения задач научной и проектно-технологической деятельности (ПК-5)		
9	Предварительное распределение ключей	способен строить и анализировать математические модели в современном естествознании, технике, экономике и управлении (ОПК-2); способен разрабатывать и применять математические методы решения задач научной и проектно-технологической деятельности (ПК-5)	ПР-2	УО-2

Наименование категории (группы) общепрофессиональных компетенций	**Код и наименование общепрофессиональной компетенции**	**Код и наименование индикатора достижения общепрофессиональной компетенции**
Теоретические и практические основы профессиональной деятельности	ОПК-2 способен строить и анализировать математические модели в современном естествознании, технике, экономике и управлении	ОПК-2.1 умеет: строить и анализировать математические модели в современном естествознании, технике, экономике и управлении ОПК-2.2 знает: Основные методы построения и анализа математических моделей ОПК-2.3 владеет: методами построения и анализа математических моделей в современном естествознании, технике, экономике и управлении

Профессиональные компетенции выпускников и индикаторы их достижения:

Задача профессиональной деятельности	Объект или область знания	Код и наименование профессиональной компетенции	Код и наименование индикатора достижения профессиональной компетенции
Тип задач профессиональной деятельности: Научно-исследовательский			
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-5 способен разрабатывать и применять математические методы для решения задач научной и проектно-технологической деятельности	ПК-5.1. Умеет: анализировать поставленную задачу и находить алгоритм ее решения; выбирать оптимальные системы программирования, наиболее подходящие для решения поставленной задачи ПК-5.2. Знает: современные методы цифровой обработки изображений и средства компьютерной графики ПК-5.3. Владеет: методами моделирования информационных процессов; навыками работы над производственным проектом в составе группы научных специалистов

II. Шкала оценивания уровня сформированности компетенций по дисциплине «Криптографические протоколы»

Код и формулировка компетенции	**Этапы формирования компетенции**		**критерии**	**показатели**	**баллы**
ОПК-2 способен строить и анализировать математические модели в современном естествознании, технике, экономике и управлении	знает (пороговый уровень)	Основные методы построения и анализа математических моделей	знает основные методы построения и анализа математических моделей	доклад	60 - 74
	умеет (продвинутый)	строить и анализировать математические модели в современном естествознании, технике, экономике и управлении	умеет строить и анализировать математические модели в современном естествознании, технике, экономике и управлении	Участие в дискуссии	75 - 89
	владеет (высокий)	методами построения и анализа математических моделей в современном естествознании, технике, экономике и управлении	владеет методами построения и анализа математических моделей в современном естествознании, технике, экономике и управлении	реферат	90 - 100
ПК-5 способен разрабатывать и применять математические методы для решения задач научной и проектно-технологической деятельности	знает (пороговый уровень)	современные методы цифровой обработки изображений и средства компьютерной графики	знание современных методов цифровой обработки изображений и средств компьютерной графики	доклад	60 - 74
	умеет (продвинутый)	анализировать поставленную задачу и находить алгоритм ее решения; выбирать оптимальные системы программирования, наиболее подходящие для решения поставленной задачи	умение анализировать поставленную задачу и находить алгоритм ее решения; выбирать оптимальные системы программирования, наиболее подходящие для решения поставленной	Участие в дискуссии	75 - 89

			задачи		
	владеет (высокий)	методами моделирования информационных процессов; навыками работы над производственным проектом в составе группы научных специалистов	владение методами моделирования информационных процессов; навыками работы над производственным проектом в составе группы научных специалистов	реферат	90 - 100

Вопросы к зачету

1. Свойства формирующие безопасность протокола.
2. Основные атаки на безопасность протокола.
3. Формальные методы анализа протоколов.
4. Целостность данных и функции хеширования.
5. Хеш-функции на основе дискретного логарифмирования.
6. Атаки на функции хеширования.
7. Ортогональные массивы и коды аутентификации.
8. Оптимальные коды аутентификации.
9. Цифровые подписи на основе симметричных шифров.
10. Цифровые подписи на основе шифров с открытым ключом.
11. Протоколы идентификации использующие пароли.
12. Протоколы решения математических задач.
13. Протокол Диффи-Хеллмана.
14. Протоколы передачи ключей.
15. Схемы предварительного распределения ключей.

Примеры индивидуальныз заданий

1. Введение

1.1. Описать основные виды криптографических протоколов.
1.2. Построить пример криптографического протокола.
1.3. Построить модель для оценки стойкости протоколов.
1.4. Привести пример атаки на протокол.

2. 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.

3. Коды аутентификации

1.1. Укажите разницу между следующими понятиями: целостность данных, аутентификация сообщений, аутентификация сущностей.
1.2. Укажите нестандартную конструкцию в протоколе Ву-Лама.
1.3. Каждый ASCII-символ в компьютере представляется с помощью восьми бит. Почему, как правило, в восьми ASCII-символах содкржится намного меньше информации, чем в 64 битах?
1.4. Построить пример кода аутентификации на основе линейного кода над конечным полем.

4. Схемы цифровой подписи

1.1. Что представляет собой «прикладная» стойкость цифровой подписи?
1.2. Пусть алгоритм PSS подписывает одно и то же сообщение дважды. Какова вероятность, что он создаст одну и ту же подпись?
1.3. Почему две полосы пропускания в схеме шифрования отличаются друг от друга?
1.4. Построить пример алгоритма цифровой подписи.

5. Протоколы идентификации

1.1. В чем состоят недостатки систем с фиксированным паролем?
1.2. Каковы возможные уязвимости схемы использования одноразовых паролей?
1.3. Постройте пример протокола с нулевым разглашением.
1.4. В каких целях используют временную метку в протоколе типа «запрос – ответ»?

6. Протоколы с нулевым разглашением

1.1. Что означают свойства связывания и сокрытия для схем привязки к биту?
1.2. Покажите, что если при нескольких повторениях протокола проверки принадлежности подгруппе участник А использует случайное число дважды, то участник В сможет определить это число.
1.3. Как можно переделать протокол доказательства знания в схему цифровой подписи?

7. Протоколы передачи кдючей

1.1. Каковы преимущества централизованного распределения ключей?
1.2. Каков недостаток протокола NS?
1.3. Приведите примеры атак на протоколы передачи ключей?
1.4. Определите назначение второго сервера в протоколе Kerberos.

8. Распределение ключей

1.1. В чем состоят цели управления ключами?
1.2. Постройте классификацию ключей по предназначению и срокам действия.
1.3. Приведите примеры атак на протоколы распределения ключей?
1.4. Постройте пример протокола с участием третьей доверенной стороны.