

**Федеральное государственное автономное образовательное
учреждение высшего образования
«Московский физико-технический институт
(национальный исследовательский университет)»**

УТВЕРЖДЕНО

**Директор физтех-школы физики
и исследований им. Ландау
А.В. Рогачев**

	Рабочая программа дисциплины (модуля)
по дисциплине:	Прикладная криптография
по направлению:	Прикладные математика и физика
профиль подготовки:	Общая и прикладная физика Физтех-школа физики и исследований им. Ландау кафедра фундаментальных проблем физики квантовых технологий
курс:	1
квалификация:	магистр

Семестр, формы промежуточной аттестации: 1 (осенний) - Экзамен

Аудиторных часов: 30 всего, в том числе:

лекции: 15 час.

семинары: 15 час.

лабораторные занятия: 0 час.

Самостоятельная работа: 30 час.

Подготовка к экзамену: 30 час.

Всего часов: 90, всего зач. ед.: 2

Программу составили:

А.И. Колыбельников, старший научный сотрудник

Г.Б. Лесовик, д-р физ.-мат. наук, старший научный сотрудник

Программа обсуждена на заседании кафедры фундаментальных проблем физики квантовых технологий
29.03.2025

Аннотация

Прикладная криптография – это раздел криптографии о правильном применении криптографических алгоритмов, корректном построении протоколов защиты информации, о методах математического доказательства стойкости криптографических алгоритмов и протоколов.

1. Цели и задачи

Цель дисциплины

Дать студентам представление о фундаментальных принципах построения криптографических алгоритмов, протоколов и методах их применения.

Задачи дисциплины

- выработать у студентов представление о защите информации как о точной науке, основанной на Шенноновской теории информации;
- дать представление о существующих криптографических примитивах и протоколах, а также их современных реализациях (российских и международных стандартов);
- дать представление о применении теории групп и теории конечных полей в криптографии.

2. Перечень формируемых компетенций

Освоение дисциплины направлено на формирование следующих компетенций:

Код и наименование компетенции	Индикаторы достижения компетенции
УК-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	УК-1.1 Анализирует проблемную ситуацию как систему, выявляя ее составляющие и связи между ними
	УК-1.2 Осуществляет поиск вариантов решения поставленной проблемной ситуации на основе доступных источников информации
	УК-1.3 Разрабатывает стратегию достижения поставленной цели как последовательность шагов, предвидя результат каждого из них и оценивая их влияние на внешнее окружение планируемой деятельности и на взаимоотношения участников этой деятельности
ОПК-1 Владеет системой фундаментальных научных знаний в области физико-математических наук	ОПК-1.1 Знает и способен использовать в профессиональной деятельности фундаментальные научные знания в области физико-математических наук
	ОПК-1.2 Способен обобщать и критически оценивать опыт и результаты научных исследований в области профессиональной деятельности
	ОПК-1.3 Понимает междисциплинарные связи в области математики и физики и способен их применять при решении задач профессиональной деятельности
ПК-1 Способен ставить, формализовывать и решать задачи, в том числе разрабатывать и исследовать математические модели изучаемых явлений и процессов, системно анализировать научные проблемы, получать новые научные результаты	ПК-1.1 Способен находить, анализировать и обобщать информацию об актуальных результатах исследований в рамках тематической области своей профессиональной деятельности
	ПК-1.2 Способен выдвигать гипотезы, строить математические модели для описания изучаемых явлений и процессов, оценивать качество разработанной модели
	ПК-1.3 Способен применять теоретические и (или) экспериментальные методы исследований к конкретной научной задаче и интерпретировать полученные результаты

3. Перечень планируемых результатов обучения по дисциплине (модулю)

В результате освоения дисциплины обучающиеся должны

знать:

- общие принципы организации защиты информации;
- основы классической криптографии с секретным ключом;
- основы криптографии на открытых ключах;
- современные криптографические примитивы, математические основы их работы;
- простейшие, классические и современные криптографические протоколы, в том числе протоколы аутентификации и авторизации;
- основы криптоанализа примитивов и протоколов.

уметь:

- анализировать соответствие степени защищённости криптографических примитивов современному уровню развития криптоанализа;
- выбирать подходящие криптографические примитивы и протоколы для использования в информационных системах и процессах организации.

владеть:

- простейшими методами оценки надёжности информационных систем с использованием криптографических средств;
- навыками совместного выполнения проектов.

4. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1. Разделы дисциплины (модуля) и трудоемкости по видам учебных занятий

№	Тема (раздел) дисциплины	Трудоемкость по видам учебных занятий, включая самостоятельную работу, час.			
		Лекции	Семинары	Лаборат. работы	Самост. работа
1	Математические основы симметричной криптографии.	2	2		4
2	Методы доказательства стойкости симметричных криптоалгоритмов.	2	2		4
3	Симметричные криптоалгоритмы.	2	2		2
4	Хеш- функции.	2	2		2
5	Математические основы асимметричной криптографии.	2	2		4
6	Классические асимметричные криптоалгоритмы.	1	1		2
7	Постквантовые асимметричные криптоалгоритмы.	1	1		4
8	Алгоритмы обмена ключами.	1	1		2
9	Криптографические протоколы.	1	1		2
10	Инфраструктура применения криптографии.	1	1		4
Итого часов		15	15		30
Подготовка к экзамену		30 час.			
Общая трудоёмкость		90 час., 2 зач.ед.			

4.2. Содержание дисциплины (модуля), структурированное по темам (разделам)

Семестр: 1 (Осенний)

1. Математические основы симметричной криптографии.

Понятия и определения, моно- и полиалфавитные шифры, теория Шеннона, формула Хартли, поточные и блочные симметричные шифры. Методы построения симметричных шифров.

2. Методы доказательства стойкости симметричных криптоалгоритмов.

Классификация шифров с точки зрения стойкости. Методы криптоанализа симметричных шифров. Оценка показателя качества шифров и криптопримитивов. Оценка перемешивающих свойств линейных перестановок, оценка качества бент-функций с точки зрения криптографии. Алгоритмы Гровера и Саймона.

3. Симметричные криптоалгоритмы.

История развития. Классификация. Поточные шифры – синхронные, самосинхронизирующиеся. Блочные симметричные шифры, цепь Фейстеля, SP структура, SPN структура, Схема Лей Месси, Схема Эвен-Мансур. Генераторы ключей – случайные и псевдослучайные, методы оценки качества. Контейнеры ключей. Режимы работы блочных шифров. Оценка нагрузки на ключ.

4. Хеш- функции.

История создания, парадокс Дня рождения. Общие принципы построения хеш-функций, классификация, область применения. Схема Миагути-Пренеля, Девиса-Мейера, Матиса-Мейера-Осеаса, Меркла-Дамгарда. Примеры хеш-функций, криптоанализ хеш-функций.

5. Математические основы асимметричной криптографии.

Оценка сложности дискретного логарифмирования, оценка сложности разложения составного числа на простые. Генерация простых чисел. Гипотеза Римана и распределение простых чисел в множестве целых чисел. Расширенный алгоритм Эвклида, функция Эйлера. Атаки и защита от атак.

6. Классические асимметричные криптоалгоритмы.

Алгоритмы El-Gamal и RSA. Криптоанализ и оценка стойкости. Алгоритм Шора. Эллиптические кривые. Классификация асимметричных алгоритмов и подходы к их созданию.

7. Постквантовые асимметричные криптоалгоритмы.

Одноразовые электронные подписи на примере функции Лэмпорта. ML-DSA. Дерево хешей, решетки, подписи на двоичных кодах.

8. Алгоритмы обмена ключами.

Diffie-Hellman и его модификации. ML-KEM. E2EE и PFS.

9. Криптографические протоколы.

TLS, QUIC, IPSec - принципы построения криптографических протоколов, оценка стойкости, фреймворки оценки стойкости. Типовые ошибки проектирования.

10. Инфраструктура применения криптографии.

PKI – инфраструктура открытых ключей, управление симметричными ключами. Жизненный цикл ключей и управление ими. SDLC.

5. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

Учебная аудитория, оснащенная доской, мультимедиапроектором и экраном.

6. Перечень рекомендуемой литературы

Основная литература

1. Криптографические методы защиты информации [Текст], учеб. пособие для вузов / С. М. Владимиров [и др.] , М., МФТИ, 2016
2. Введение в криптографию [Текст] : [учеб. пособие для вузов] / под ред. В. В. Ященко .— 4-е изд., доп. — М. : МЦНМО, 2012 .— 348 с.

Дополнительная литература

1. Криптография [Текст] / Н. Смарт ; пер. с англ. С. А. Кулешова ; под ред. С. К. Ландо .— М. : Техносфера, 2006 .— 528 с.
2. Криптография и безопасность сетей [Текст] : учеб. пособие для вузов / Б. А. Фороузан ; пер. с англ. под ред. А. Н. Берлина .— М. : Интернет-ун-т информ. технологий : БИНОМ. Лаб. знаний, 2010 .— 784 с.

7. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (модуля)

1. <https://tensornetwork.org/>
2. <https://www.tensors.net/>

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

Язык программирования python.

9. Методические указания для обучающихся по освоению дисциплины (модуля)

Студент, изучающий дисциплину, должен, с одной стороны, овладеть общим понятийным аппаратом, а с другой стороны, должен научиться применять теоретические знания на практике. В результате изучения дисциплины студент должен знать основные определения и понятия, уметь применять полученные знания для решения различных задач.

Успешное освоение курса требует:

- посещения всех занятий, предусмотренных учебным планом по дисциплине;
- ведения конспекта занятий;
- напряжённой самостоятельной работы студента.

Самостоятельная работа включает в себя:

- чтение рекомендованной литературы;
- проработку учебного материала, подготовку ответов на вопросы, предназначенных для самостоятельного изучения;
- решение задач, предлагаемых студентам на занятиях;
- подготовку к выполнению заданий текущей и промежуточной аттестации.

Показателем владения материалом служит умение без конспекта отвечать на вопросы по темам дисциплины.

Важно добиться понимания изучаемого материала, а не механического его запоминания. При затруднении изучения отдельных тем, вопросов, следует обращаться за консультациями преподавателю.

Возможен промежуточный контроль знаний студентов в виде решения задач в соответствии с тематикой занятий.

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

по направлению:	Прикладные математика и физика
профиль подготовки:	Общая и прикладная физика Физтех-школа физики и исследований им. Ландау кафедра фундаментальных проблем физики квантовых технологий
курс:	<u>1</u>
квалификация:	магистр

Семестр, формы промежуточной аттестации: 1 (осенний) - Экзамен

Разработчики:

А.И. Колыбельников, старший научный сотрудник

Г.Б. Лесовик, д-р физ.-мат. наук, старший научный сотрудник

1. Компетенции, формируемые в процессе изучения дисциплины

Код и наименование компетенции	Индикаторы достижения компетенции
УК-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	УК-1.1 Анализирует проблемную ситуацию как систему, выявляя ее составляющие и связи между ними
	УК-1.2 Осуществляет поиск вариантов решения поставленной проблемной ситуации на основе доступных источников информации
	УК-1.3 Разрабатывает стратегию достижения поставленной цели как последовательность шагов, предвидя результат каждого из них и оценивая их влияние на внешнее окружение планируемой деятельности и на взаимоотношения участников этой деятельности
ОПК-1 Владеет системой фундаментальных научных знаний в области физико-математических наук	ОПК-1.1 Знает и способен использовать в профессиональной деятельности фундаментальные научные знания в области физико-математических наук
	ОПК-1.2 Способен обобщать и критически оценивать опыт и результаты научных исследований в области профессиональной деятельности
	ОПК-1.3 Понимает междисциплинарные связи в области математики и физики и способен их применять при решении задач профессиональной деятельности
ПК-1 Способен ставить, формализовывать и решать задачи, в том числе разрабатывать и исследовать математические модели изучаемых явлений и процессов, системно анализировать научные проблемы, получать новые научные результаты	ПК-1.1 Способен находить, анализировать и обобщать информацию об актуальных результатах исследований в рамках тематической области своей профессиональной деятельности
	ПК-1.2 Способен выдвигать гипотезы, строить математические модели для описания изучаемых явлений и процессов, оценивать качество разработанной модели
	ПК-1.3 Способен применять теоретические и (или) экспериментальные методы исследований к конкретной научной задаче и интерпретировать полученные результаты

2. Показатели оценивания компетенций

В результате изучения дисциплины «Прикладная криптография» обучающийся должен:

знать:

- общие принципы организации защиты информации;
- основы классической криптографии с секретным ключом;
- основы криптографии на открытых ключах;
- современные криптографические примитивы, математические основы их работы;
- простейшие, классические и современные криптографические протоколы, в том числе протоколы аутентификации и авторизации;
- основы криптоанализа примитивов и протоколов.

уметь:

- анализировать соответствие степени защищённости криптографических примитивов современному уровню развития криптоанализа;
- выбирать подходящие криптографические примитивы и протоколы для использования в информационных системах и процессах организации.

владеть:

- простейшими методами оценки надёжности информационных систем с использованием криптографических средств;
- навыками совместного выполнения проектов.

3. Перечень типовых (примерных) вопросов, заданий, тем для подготовки к текущему контролю

С целью контроля освоения обучающимися учебного материала проводится устный опрос в начале занятия по теме прошлого занятия.

4. Перечень типовых (примерных) вопросов и тем для проведения промежуточной аттестации обучающихся

1. Реализация шифра « \llcorner ».
2. Распределение ключа.
3. Создание ключа, распределение между узлами, смена ключа безопасное хранение.
4. Гомоморфное шифрование.
5. Реализация гомоморфного шифра, оценка объема ключа в зависимости от объема сообщений, создание, смена ключей. Оценка скорости шифрования.
6. защиты для IoT.
7. Выбор протокола для защиты. Обеспечение конфиденциальности и целостности. Смена ключей и паролей на устройствах..
8. Атаки на существующие протоколы.
9. Симметричный шифр для IoT.
10. Контроль целостности для IoT.
11. Управление паролями в IoT.
12. Управление ключами в IoT.
13. Физически не клонируемые функции.
14. Реализация и сравнение физически неклонируемых функций.
15. Реализация атак на PUF.
16. Системы голосования.
17. Реализация и оценка качества и скорости системы голосования.
18. Атаки на существующие системы голосования.
19. Оценка стойкости отечественной криптографии.
20. Атаки на поиск коллизий в Стрибоге.
- 21 Реализация атак на Кузнечик.
22. Анализ S-блоков Кузнечика.
23. Обзор методов создания S-блоков и реализация генератора с изменяемым набором проверок.
24. Оценка стойкости электронной подписи.
25. Оценка XSL структур.
26. Оценка XL структур.
27. Формирование списка нелинейных функций для блока 4-8 бит и оценка их нелинейности Симметричные шифры.
28. Анализ стойкости одного из существующих и эксплуатируемых симметричных шифров.
29. Оценка шифрующих свойств криптопримитивов.

Примеры билетов для проведения устного экзамена:

Билет №1.

- 1) Цели, задачи и методы защиты информации. Примеры выполнения целей по защите информации без использования криптографических средств.
- 2) Группы точек эллиптической кривой над множеством рациональных чисел и над конечными полями. Построение, операции, свойства. Теорема Хассе. Использование в криптографии.

Билет №2.

1) Крптология, криптоанализ, криптография. Криптографические примитивы. Основные определения и примеры использования. Код, шифр, ключ, хеш-функция, криптографический протокол, цифровая подпись, etc. Принцип Керкгоффа.

2) Поля Галуа вида $GF(p)$ и $GF(2^n)$. Построение, операции, свойства, использование в криптографии.

Критерии оценивания

Оценка отлично 10 баллов - выставляется студенту, показавшему всесторонние, систематизированные, глубокие знания учебной программы дисциплины, проявляющему интерес к данной предметной области, продемонстрировавшему умение уверенно и творчески применять их на практике при решении конкретных задач, свободное и правильное обоснование принятых решений.

Оценка отлично 9 баллов - выставляется студенту, показавшему всесторонние, систематизированные, глубокие знания учебной программы дисциплины и умение уверенно применять их на практике при решении конкретных задач, свободное и правильное обоснование принятых решений.

Оценка отлично 8 баллов - выставляется студенту, показавшему всесторонние, систематизированные, глубокие знания учебной программы дисциплины и умение уверенно применять их на практике при решении конкретных задач, правильное обоснование принятых решений, с некоторыми недочетами.

Оценка хорошо 7 баллов - выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но недостаточно грамотно обосновывает полученные результаты.

Оценка хорошо 6 баллов - выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе или в решении задач некоторые неточности.

Оценка хорошо 5 баллов - выставляется студенту, если он в основном знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе или в решении задач достаточно большое количество неточностей.

Оценка удовлетворительно 4 балла - выставляется студенту, показавшему фрагментарный, разрозненный характер знаний, недостаточно правильные формулировки базовых понятий, нарушения логической последовательности в изложении программного материала, но при этом он освоил основные разделы учебной программы, необходимые для дальнейшего обучения, и может применять полученные знания по образцу в стандартной ситуации.

Оценка удовлетворительно 3 балла - выставляется студенту, показавшему фрагментарный, разрозненный характер знаний, допускающему ошибки в формулировках базовых понятий, нарушения логической последовательности в изложении программного материала, слабо владеет основными разделами учебной программы, необходимыми для дальнейшего обучения и с трудом применяет полученные знания даже в стандартной ситуации.

Оценка неудовлетворительно 2 балла - выставляется студенту, который не знает большей части основного содержания учебной программы дисциплины, допускает грубые ошибки в формулировках основных принципов и не умеет использовать полученные знания при решении типовых задач.

Оценка неудовлетворительно 1 балл - выставляется студенту, который не знает основного содержания учебной программы дисциплины, допускает грубейшие ошибки в формулировках базовых понятий дисциплины и вообще не имеет навыков решения типовых практических задач.

5. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Оценка за курс выставляется на основании оценивания практических работ и устного ответа во время экзамена. Экзамен проводится по билетам в устной форме. В каждом билете представлен два теоретических вопроса. При проведении экзамена обучающемуся предоставляется 30 минут на подготовку. Опрос обучающегося не должен превышать одного астрономического часа.