

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

УТВЕРЖДЕНО

**Директор высшей школы
программной инженерии
А.В. Малеев**

	Рабочая программа дисциплины (модуля)
по дисциплине:	Криптография. Часть 1
по направлению:	Программная инженерия
профиль подготовки:	Разработка программно-информационных систем высшая школа программной инженерии высшая школа программной инженерии
курс:	4
квалификация:	бакалавр

Семестр, формы промежуточной аттестации: 7 (осенний) - Экзамен

Аудиторных часов: 60 всего, в том числе:

лекции: 30 час.

семинары: 30 час.

лабораторные занятия: 0 час.

Самостоятельная работа: 18 час.

Подготовка к экзамену: 30 час.

Всего часов: 108, всего зач. ед.: 3

Программу составил: А.А. Жмуров, канд. физ.-мат. наук, доцент

Программа обсуждена на заседании высшей школы программной инженерии 19.03.2025

Аннотация

Курс предназначен для изучения базовых криптографических алгоритмов и схем, которые лежат в основе современных систем защиты информации. В рамках курса рассматриваются блочные шифры, хэш-функции, режимы работы шифров, протоколы защищенного обмена и методы управления криптографическими ключами. Особое внимание уделяется фундаментальным криптографическим принципам и современным подходам к анализу и построению надежных криптографических систем. Курс включает как теоретические занятия, так и практические упражнения, направленные на развитие навыков применения криптографических механизмов для обеспечения конфиденциальности, целостности и аутентичности данных.

1. Цели и задачи

Цель дисциплины

Формирование у студентов базовых знаний и понимания фундаментальных криптографических концепций, алгоритмов и схем, лежащих в основе современных криптографических систем, а также развитие навыков анализа и применения криптографических механизмов для обеспечения конфиденциальности, целостности и аутентичности информации.

Задачи дисциплины

- изучить принципы и задачи современной криптографии;
- разобрать блочные шифры и их режимы работы;
- освоить методы обеспечения конфиденциальности и целостности данных;
- изучить хэш-функции и их применение;
- познакомиться с протоколами защищенного обмена сообщениями;
- разобрать генерацию и управление криптографическими ключами;
- изучить основы криптоанализа и построения криптографической инфраструктуры.

2. Перечень формируемых компетенций

Освоение дисциплины направлено на формирование следующих компетенций:

Код и наименование компетенции	Индикаторы достижения компетенции
УК-1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	УК-1.2 Находит, критически анализирует и выбирает информацию, необходимую для решения поставленной задачи
	УК-1.3 Рассматривает различные варианты решения задачи, оценивает их преимущества и недостатки
ОПК-1 Способен применять естественнонаучные и общетехнические знания, методы математического анализа и моделирования, теоретического и экспериментального исследования в профессиональной деятельности	ОПК-1.1 Способен анализировать поставленную задачу, намечать пути ее решения
	ОПК-1.3 Способен определять границы применимости полученных результатов
ОПК-6 Способен разрабатывать алгоритмы и программы, пригодные для практического использования, применять основы информатики и программирования к проектированию, конструированию и тестированию программных продуктов	ОПК-6.3 Знает методы тестирования программного кода на ошибки и способен проводить тестирование на различных уровнях (модульное, интеграционное, системное)
ОПК-7 Способен применять в практической деятельности основные концепции, принципы, теории и факты, связанные с информатикой	ОПК-7.1 Обладает навыками создания и выполнения тестовых сценариев для выявления ошибок в программном обеспечении
	ОПК-7.2 Понимает принципы работы баз данных и умеет проектировать структуру данных для эффективного хранения информации
ОПК-8 Способен осуществлять поиск, хранение, обработку и анализ информации	ОПК-8.1 Понимает принципы, по которым работают базы данных, и умеет создавать структуру данных, оптимизированную для эффективного хранения и обработки информации

из различных источников и баз данных, представлять ее в требуемом формате с использованием информационных, компьютерных и сетевых технологий	ОПК-8.2 Умеет применять технологии машинного обучения в различных прикладных областях
	ОПК-8.3 Умеет оптимизировать и проводить рефакторинг существующего кода для улучшения производительности и поддержки
ПК-3 Способен проектировать, разрабатывать, интегрировать, проверять на работоспособность программное обеспечение	ПК-3.2 Умеет выбирать языки программирования для написания программного кода с учетом технического задания

3. Перечень планируемых результатов обучения по дисциплине (модулю)

В результате освоения дисциплины обучающиеся должны

знать:

- основные принципы и задачи современной криптографии;
- устройство и принципы работы блочных шифров, режимов их работы;
- основы хэш-функций и механизмы обеспечения целостности данных;
- принципы работы криптографических протоколов защищенного обмена сообщениями;
- методы генерации, хранения и использования криптографических ключей;
- основы криптоанализа и построения криптографической инфраструктуры.

уметь:

- анализировать и выбирать криптографические алгоритмы для решения задач защиты информации;
- применять блочные шифры и режимы их работы на практике;
- использовать хэш-функции для обеспечения целостности данных;
- разрабатывать и применять протоколы защищенного обмена сообщениями;
- работать с криптографическими ключами.

владеть:

- методами анализа надежности криптографических схем;
- навыками проектирования криптографически устойчивых решений;
- инструментами обеспечения конфиденциальности и целостности информации.

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	Современная криптография: задачи, принципы, подходы	3	3		2
2	Блочные шифры	3	3		2
3	Конфиденциальность	4	4		2
4	Режимы работы блочных шифров	4	4		2
5	Хэш-функции	4	4		2
6	Целостность	4	4		2
7	Протоколы обеспечения защищенного обмена сообщениями	4	4		3
8	Криптографические ключи: генерация и нагрузка	4	4		3
Итого часов		30	30		18
Подготовка к экзамену		30 час.			

Общая трудоёмкость	108 час., 3 зач.ед.
--------------------	---------------------

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

Семестр: 7 (Осенний)

1. Современная криптография: задачи, принципы, подходы

Введение в криптографию, основные задачи (конфиденциальность, целостность, аутентификация), симметричное и асимметричное шифрование, основные криптографические модели и угрозы.

2. Блочные шифры

Принципы работы блочных шифров, их структура, распространённые алгоритмы (AES, DES), основные свойства безопасности и методы атаки.

3. Конфиденциальность

Определение конфиденциальности в криптографии, методы её обеспечения, примеры алгоритмов и атак, защита данных при передаче и хранении.

4. Режимы работы блочных шифров

Различные режимы шифрования (ECB, CBC, CFB, OFB, CTR), их особенности, достоинства и недостатки, области применения.

5. Хэш-функции

Принципы построения и применения криптографических хэш-функций, примеры алгоритмов (SHA, MD5), стойкость к коллизиям, использование хэширования в цифровых подписях и аутентификации.

6. Целостность

Методы обеспечения целостности данных, контрольные суммы, коды аутентификации сообщений (HMAC), защита от несанкционированных изменений.

7. Протоколы обеспечения защищенного обмена сообщениями

Основные криптографические протоколы (TLS, IPsec, PGP), их структура и принципы работы, механизмы защиты информации при передаче по незащищённым каналам.

8. Криптографические ключи: генерация и нагрузка

Методы генерации криптографических ключей, их распределение и управление, ключевые центры, защита ключей от компрометации.

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

Для изучения дисциплины используется компьютерная техника с необходимым программным обеспечением для симуляции криптографических алгоритмов, работы с криптографическими библиотеками, а также специализированные средства для анализа безопасности систем.

6. Перечень рекомендуемой литературы

Основная литература

1. Криптография и безопасность в технологии .NET / П. Торстейнсон, Г. А. Ганеш . — М., Лаборатория знаний, 2020.— URL: <http://books.mipt.ru/book/301447> (дата обращения: 20.02.2021). - Полный текст (Режим доступа : из сети МФТИ / Удаленный доступ)

Фонд библиотеки МФТИ:

1. Романьков, В. А. Введение в криптографию : курс лекций / В.А. Романьков. — 2-е изд., испр. и доп. — Москва : ФОРУМ : ИНФРА-М, 2025. — 240 с. — (Высшее образование). - ISBN 978-5-00091-493-9. - Текст : электронный. - URL: <https://znanium.ru/catalog/product/2178770>

Дополнительная литература

-

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

<http://dm.fizteh.ru/>

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

Используются криптографические библиотеки, среды разработки и инструменты для анализа безопасности.

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

Для успешного освоения дисциплины рекомендуется:

- изучать теоретический материал и активно участвовать в практических занятиях;
- работать с криптографическими библиотеками для закрепления знаний;
- применять полученные знания на примерах решения задач по криптографическому анализу и протоколам;
- регулярно выполнять домашние задания и участвовать в обсуждениях на семинарах.

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

по направлению:	Программная инженерия
профиль подготовки:	Разработка программно-информационных систем высшая школа программной инженерии высшая школа программной инженерии
курс:	<u>4</u>
квалификация:	бакалавр

Семестр, формы промежуточной аттестации: 7 (осенний) - Экзамен

Разработчик: А.А. Жмуров, канд. физ.-мат. наук, доцент

1. Компетенции, формируемые в процессе изучения дисциплины

Код и наименование компетенции	Индикаторы достижения компетенции
УК-1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	УК-1.2 Находит, критически анализирует и выбирает информацию, необходимую для решения поставленной задачи
	УК-1.3 Рассматривает различные варианты решения задачи, оценивает их преимущества и недостатки
ОПК-1 Способен применять естественнонаучные и общетехнические знания, методы математического анализа и моделирования, теоретического и экспериментального исследования в профессиональной деятельности	ОПК-1.1 Способен анализировать поставленную задачу, намечать пути ее решения
	ОПК-1.3 Способен определять границы применимости полученных результатов
ОПК-6 Способен разрабатывать алгоритмы и программы, пригодные для практического использования, применять основы информатики и программирования к проектированию, конструированию и тестированию программных продуктов	ОПК-6.3 Знает методы тестирования программного кода на ошибки и способен проводить тестирование на различных уровнях (модульное, интеграционное, системное)
ОПК-7 Способен применять в практической деятельности основные концепции, принципы, теории и факты, связанные с информатикой	ОПК-7.1 Обладает навыками создания и выполнения тестовых сценариев для выявления ошибок в программном обеспечении
	ОПК-7.2 Понимает принципы работы баз данных и умеет проектировать структуру данных для эффективного хранения информации
ОПК-8 Способен осуществлять поиск, хранение, обработку и анализ информации из различных источников и баз данных, представлять ее в требуемом формате с использованием информационных, компьютерных и сетевых технологий	ОПК-8.1 Понимает принципы, по которым работают базы данных, и умеет создавать структуру данных, оптимизированную для эффективного хранения и обработки информации
	ОПК-8.2 Умеет применять технологии машинного обучения в различных прикладных областях
	ОПК-8.3 Умеет оптимизировать и проводить рефакторинг существующего кода для улучшения производительности и поддержки
ПК-3 Способен проектировать, разрабатывать, интегрировать, проверять на работоспособность программное обеспечение	ПК-3.2 Умеет выбирать языки программирования для написания программного кода с учетом технического задания

2. Показатели оценивания компетенций

В результате изучения дисциплины «Криптография. Часть 1» обучающийся должен:

знать:

- основные принципы и задачи современной криптографии;
- устройство и принципы работы блочных шифров, режимов их работы;
- основы хэш-функций и механизмы обеспечения целостности данных;
- принципы работы криптографических протоколов защищенного обмена сообщениями;
- методы генерации, хранения и использования криптографических ключей;
- основы криптоанализа и построения криптографической инфраструктуры.

уметь:

- анализировать и выбирать криптографические алгоритмы для решения задач защиты информации;
- применять блочные шифры и режимы их работы на практике;
- использовать хэш-функции для обеспечения целостности данных;
- разрабатывать и применять протоколы защищенного обмена сообщениями;
- работать с криптографическими ключами.

владеть:

- методами анализа надежности криптографических схем;
- навыками проектирования криптографически устойчивых решений;
- инструментами обеспечения конфиденциальности и целостности информации.

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

Перечень типовых контрольных заданий:

- решение задач по выбору криптографических алгоритмов;
- анализ безопасности криптографических систем;
- реализация и тестирование протоколов защищенного обмена.

Критерии оценивания:

- полнота и правильность выполнения задания;
- оригинальность и обоснованность подходов;
- точность и качество реализации.

Методические рекомендации:

- использовать литературу и криптографические библиотеки для выполнения заданий;
- обращать внимание на безопасность реализации алгоритмов;
- регулярно консультироваться с преподавателем по возникающим вопросам.

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

1. Основные задачи криптографии: Какие задачи решает современная криптография и какие методы используются для их решения?
2. Блочные шифры: Описание принципа работы блочного шифра, примеры (AES, DES). Чем отличаются различные режимы работы блочных шифров?
3. Хэш-функции: Какие задачи решают хэш-функции, особенности их применения и примеры (SHA, MD5)?
4. Режимы работы блочных шифров: Рассмотреть различные режимы (ECB, CBC, CFB) и их преимущества и недостатки.
5. Протоколы защищенного обмена сообщениями: Основные принципы работы протоколов TLS, IPsec и их роль в обеспечении безопасности.
6. Криптографические ключи: Методы генерации, хранения и защиты криптографических ключей. Почему важно защищать ключи?
7. Криптоанализ: Основные методы криптоанализа, как атаки на криптографические системы, и как их избежать.
8. Конфиденциальность и целостность данных: Как криптография обеспечивает эти параметры, примеры алгоритмов для их защиты.
9. Криптографическая инфраструктура: Как строится безопасная криптографическая инфраструктура, включая управление ключами и сертификатами.
10. Применение криптографии в реальных системах: Примеры использования криптографии в интернет-протоколах, электронной коммерции и защите персональных данных.

Примеры билетов:

Билет 1.

1. Блочные шифры.
2. Принципы построения надежной криптографической инфраструктуры.

Билет 2.

3. Хэш-функции.
4. Режимы работы блочных шифров.

Критерии оценивания

- оценка «отлично (10)» 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 (9)» выставляется студенту, показавшему всесторонние, систематизированные, глубокие знания учебной программы дисциплины и умение применять их на практике при решении конкретных задач, свободное и правильное обоснование принятых решений
- оценка «отлично (8)» выставляется студенту, показавшему всесторонние систематизированные, глубокие знания учебной программы дисциплины и умение применять их на практике при решении конкретных задач, и правильное обоснование принятых решений
- оценка «хорошо (7)» 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 (6)» выставляется студенту, если он 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)» выставляется студенту, если он знает материал, и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе или в решении задач некоторые неточности;
- оценка «удовлетворительно (4)» выставляется студенту, показавшему фрагментарный, разрозненный характер знаний, недостаточно правильные формулировки базовых понятий, нарушения логической последовательности в изложении программного материала, но при этом он владеет основными разделами учебной программы, необходимыми для дальнейшего обучения и может применять полученные знания по образцу в стандартной ситуации;
- оценка «удовлетворительно (3)» выставляется студенту, показавшему фрагментарный, разрозненный характер знаний, недостаточно правильные формулировки базовых понятий, нарушения логической последовательности в изложении программного материала, но при этом он владеет фрагментарно основными разделами учебной программы, необходимыми для дальнейшего обучения и может применять полученные знания по образцу в стандартной ситуации;
- оценка «неудовлетворительно (2)» выставляется студенту, который не знает большей части основного содержания учебной программы дисциплины, допускает грубые ошибки в формулировках основных понятий дисциплины и не умеет использовать полученные знания при решении типовых практических задач
- оценка «неудовлетворительно (1)» выставляется студенту, который не знает формулировок основных понятий дисциплины.

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

Итоговый контроль проводится в формате устного и (или) письменного экзамена.

Время отведенное на экзамен: 4 академических часа.