

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

**УТВЕРЖДЕНО**

**Директор физтех-школы  
прикладной математики и  
информатики**

**А.М. Райгородский**

	<b>Рабочая программа дисциплины (модуля)</b>
<b>по дисциплине:</b>	Криптография на эллиптических кривых и решетках
<b>по направлению:</b>	Информатика и вычислительная техника
<b>профиль подготовки:</b>	Системное программирование и прикладная математика Физтех-школа Прикладной Математики и Информатики кафедра дискретной математики
<b>курс:</b>	4
<b>квалификация:</b>	бакалавр

Семестр, формы промежуточной аттестации: 8 (весенний) - Дифференцированный зачет

Аудиторных часов: 30 всего, в том числе:

лекции: 15 час.

семинары: 15 час.

лабораторные занятия: 0 час.

Самостоятельная работа: 15 час.

Всего часов: 45, всего зач. ед.: 1

Программу составил: А.М. Райгородский, д-р физ.-мат. наук, доцент

Программа обсуждена на заседании кафедры дискретной математики 16.03.2023

## Аннотация

Любая криптосистема с открытым ключом основана на сложности решения некоторой задачи. Первоначально асимметричные шифры основывались на сложности решения задачи факторизации и задачи дискретного логарифмирования в группе вычетов по простому модулю. В настоящий момент, ввиду наличия субэкспоненциальных алгоритмов решения этих задач, широко используются алгоритмы, основанные на сложности решения задачи дискретного логарифмирования в группе точек эллиптической кривой (над конечным полем). Еще в 1994 г. П. Шор указал на возможность эффективного решения задач факторизации и дискретного логарифмирования в группе вычетов с помощью квантового компьютера. Начиная с этого момента идет интенсивный поиск задач, которые были бы трудно решаемыми с точки зрения квантовых вычислений. Одним из наиболее перспективных считаются задачи, связанные с решетками (объект теории чисел). В курсе предлагается познакомиться с криптографическими алгоритмами как на эллиптических кривых, так и на решетках. Для этого предварительного будут изучены некоторые основные свойства эллиптических кривых (над полем вычетов по простому модулю) и решеток.

## 1. Цели и задачи

### Цель дисциплины

В результате освоения дисциплины студент должен знать определение и основные свойства эллиптических кривых над конечными полями

### Задачи дисциплины

- освоение студентами базовых знаний (понятий, концепций, методов и моделей) в области криптографии;
- приобретение теоретических знаний и практических умений и навыков в области криптографии;
- оказание консультаций и помощи студентам в проведении собственных теоретических исследований в области криптографии.

## 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-1.1 Анализирует задачу, выделяя этапы ее решения, действия по решению задачи
	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
	УК-1.4 Грамотно, логично, аргументированно формирует собственные суждения и оценки
	УК-1.5 Определяет и оценивает практические последствия возможных вариантов решения задачи
ОПК-1 Способен применять фундаментальные знания, полученные в области физико-математических и (или) естественных наук, и использовать их в профессиональной деятельности	ОПК-1.1 Способен анализировать поставленную задачу, намечать пути ее решения
	ОПК-1.2 Способен строить математические модели, производить количественные расчеты и оценки
	ОПК-1.3 Способен определять границы применимости полученных результатов
ОПК-2 Способен использовать современные информационные технологии и программные средства при решении задач профессиональной деятельности, соблюдая требования информационной безопасности	ОПК-2.2 Знает и умеет применять численные математические методы и прикладное программное обеспечение для решения научных задач в профессиональной области
	ОПК-2.1 Способен применять современные вычислительную технику и сервисы сети Интернет в области (сфере) профессиональной деятельности

	ОПК-2.3 Знает основные требования информационной безопасности
ОПК-3 Способен составлять и оформлять научные и (или) технические (технологические, инновационные) отчеты (публикации, проекты)	ОПК-3.1 Знает основные правила оформления научных публикаций и научно-технической документации, в том числе с использованием прикладного программного обеспечения
	ОПК-3.2 Владеет на практике методологией составления научно-технических отчетов (проектов)
	ОПК-3.3 Владеет методами визуального и графического представления результатов научной (научно-технической, инновационной технологической) деятельности в виде отчетов, научных публикаций
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
ПК-2 Способен самостоятельно или в качестве члена (руководителя) малого коллектива организовывать и проводить научные исследования и их апробацию	ПК-2.1 Знает принципы построения научной работы, методы сбора и анализа полученного материала, способы аргументации
	ПК-2.2 Способен планировать и проводить научные исследования самостоятельно или в качестве члена (руководителя) малого научного коллектива
	ПК-2.3 Способен проводить апробацию результатов научно-исследовательской работы посредством публикации научных статей и участия в конференциях

### 3. Перечень планируемых результатов обучения по дисциплине (модулю)

В результате освоения дисциплины обучающиеся должны

знать:

- определение и основные свойства эллиптических кривых над конечными полями;
- основные криптографические алгоритмы, использующие эллиптические кривые;
- требования, предъявляемые к эллиптическим кривым в криптографии;
- определение и основные свойства решеток;
- определение и основные свойства мю- и L-приведенных базисов;
- алгоритмы построения мю- и L-приведенных базисов;
- алгоритм Эрмита нахождения короткого вектора решетки;
- LLL-алгоритм;
- алгоритмические задачи на решетках, используемые в криптографии;
- криптосистемы на решетках (GGH, NTRU).

уметь:

- доказывать основные свойства эллиптических кривых, решеток, базисов решеток;
- оценивать сложность и корректность алгоритмов на решетках и эллиптических кривых.

владеть:

- основ геометрии чисел;
- использования эллиптических кривых и решеток в криптографии.

### 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	Эллиптические кривые в криптографии	3	3		3
2	Современные стандарты цифровой подписи РФ и США.	3	3		3
3	Криптография на решетках	3	3		3
4	Минимумы решеток. Постоянная Эрмита	3	3		3
5	Алгоритмические задачи на решетках, используемые в криптографии	3	3		3
Итого часов		15	15		15
Подготовка к экзамену		0 час.			
Общая трудоёмкость		45 час., 1 зач.ед.			

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

Семестр: 8 (Весенний)

##### 1. Эллиптические кривые в криптографии

Понятие сложности алгоритмов. Полиномиальные и экспоненциальные алгоритмы. Проблема  $N=NP$ . Эллиптические кривые над полем  $R$ . Геометрическая и алгебраическая интерпретация сложения. Ассоциативность сложения. Эллиптические кривые над произвольным полем. Мощность группы точек эллиптической кривой над полем вычетов по простому модулю (теорема Хассе). Аналоги криптографических алгоритмов Диффи-Хеллмана и Эль-Гамала в группе точек на эллиптической кривой над конечным полем.

##### 2. Современные стандарты цифровой подписи РФ и США.

Криптостойкость криптографических алгоритмов, использующих эллиптические кривые. Построение «хороших» эллиптических кривых. Использование проективных координат для оптимизации вычислений. Возможности дальнейшего развития.

##### 3. Криптография на решетках

Решетки, базис и определитель: основные свойства. Теорема Минковского о выпуклом теле. Процесс ортогонализации Грамма-Шмидта. Мю-приведенные базисы и их построение.

##### 4. Минимумы решеток. Постоянная Эрмита

Алгоритм Лагранжа построения  $L$ -приведенного базиса. Алгоритм Эрмита нахождения короткого вектора решетки.

##### 5. Алгоритмические задачи на решетках, используемые в криптографии

LLL-приведенный базис и его свойства. LLL-алгоритм. Криптосистема GGH. Цифровая подпись GGH. Шифр NTRU. Цифровая подпись NTRUSign.

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

Стандартная учебная аудитория.

## **6. Перечень рекомендуемой литературы**

### **Основная литература**

1. Основы современной криптографии для специалистов в информационных технологиях [Текст] / Б. Я. Рябко, А. Н. Фионов ; Ин-т вычислительных технологий СО РАН ; Сибирский гос. ун-т телекоммуникаций и информатики .— М. : Научный мир, 2004 .— 173 с.
2. Криптография [Текст] / Н. Смарт ; пер. с англ. С. А. Кулешова ; под ред. С. К. Ландо .— М. : Техносфера, 2006 .— 528 с.

### **Дополнительная литература**

1. Основы криптографии [Текст] : учеб. пособие для вузов / А. П. Алферов [и др.] .— 3-е изд., испр. и доп. — М. : Гелиос АРВ, 2005 .— 480 с.

## **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)**

На лекционных занятиях используются мультимедийные технологии, включая демонстрацию презентаций.

В процессе самостоятельной работы обучающихся возможно использование таких программных средств, как Mathcad, MATLAB, Maple и др.

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

Рекомендуется успешно сдавать контрольные работы, так как это упрощает итоговую аттестацию по предмету.

Для подготовки к итоговой аттестации по предмету лучше всего пользоваться материалами лекций.

**ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)**

<b>по направлению:</b>	Информатика и вычислительная техника
<b>профиль подготовки:</b>	Системное программирование и прикладная математика Физтех-школа Прикладной Математики и Информатики кафедра дискретной математики
<b>курс:</b>	4
<b>квалификация:</b>	бакалавр

Семестр, формы промежуточной аттестации: 8 (весенний) - Дифференцированный зачет

**Разработчик:** А.М. Райгородский, д-р 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-1.1 Анализирует задачу, выделяя этапы ее решения, действия по решению задачи
	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
	УК-1.4 Грамотно, логично, аргументированно формирует собственные суждения и оценки
	УК-1.5 Определяет и оценивает практические последствия возможных вариантов решения задачи
ОПК-1 Способен применять фундаментальные знания, полученные в области физико-математических и (или) естественных наук, и использовать их в профессиональной деятельности	ОПК-1.1 Способен анализировать поставленную задачу, намечать пути ее решения
	ОПК-1.2 Способен строить математические модели, производить количественные расчеты и оценки
	ОПК-1.3 Способен определять границы применимости полученных результатов
ОПК-2 Способен использовать современные информационные технологии и программные средства при решении задач профессиональной деятельности, соблюдая требования информационной безопасности	ОПК-2.2 Знает и умеет применять численные математические методы и прикладное программное обеспечение для решения научных задач в профессиональной области
	ОПК-2.1 Способен применять современные вычислительную технику и сервисы сети Интернет в области (сфере) профессиональной деятельности
	ОПК-2.3 Знает основные требования информационной безопасности
ОПК-3 Способен составлять и оформлять научные и (или) технические (технологические, инновационные) отчеты (публикации, проекты)	ОПК-3.1 Знает основные правила оформления научных публикаций и научно-технической документации, в том числе с использованием прикладного программного обеспечения
	ОПК-3.2 Владеет на практике методологией составления научно-технических отчетов (проектов)
	ОПК-3.3 Владеет методами визуального и графического представления результатов научной (научно-технической, инновационной технологической) деятельности в виде отчетов, научных публикаций
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
ПК-2 Способен самостоятельно или в качестве члена (руководителя) малого коллектива организовывать и проводить научные исследования и их апробацию	ПК-2.1 Знает принципы построения научной работы, методы сбора и анализа полученного материала, способы аргументации
	ПК-2.2 Способен планировать и проводить научные исследования самостоятельно или в качестве члена (руководителя) малого научного коллектива

## 2. Показатели оценивания компетенций

В результате изучения дисциплины «Криптография на эллиптических кривых и решетках» обучающийся должен:

### знать:

- определение и основные свойства эллиптических кривых над конечными полями;
- основные криптографические алгоритмы, использующие эллиптические кривые;
- требования, предъявляемые к эллиптическим кривым в криптографии;
- определение и основные свойства решеток;
- определение и основные свойства мю- и L-приведенных базисов;
- алгоритмы построения мю- и L-приведенных базисов;
- алгоритм Эрмита нахождения короткого вектора решетки;
- LLL-алгоритм;
- алгоритмические задачи на решетках, используемые в криптографии;
- криптосистемы на решетках (GGH, NTRU).

### уметь:

- доказывать основные свойства эллиптических кривых, решеток, базисов решеток;
- оценивать сложность и корректность алгоритмов на решетках и эллиптических кривых.

### владеть:

- основ геометрии чисел;
- использования эллиптических кривых и решеток в криптографии.

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

Домашние задания: часть материала из лекций будет предлагаться учащимся в виде задач для самостоятельного решения. Желаящие могут получить задание, связанное с реализацией на ЭВМ алгоритмов из лекций.

Коллоквиум: в середине семестра планируется провести коллоквиум, который будет заключаться в письменном ответе на один теоретический вопрос.

Примерный список вопросов к коллоквиуму

1. Понятие сложности алгоритмов. Полиномиальные и экспоненциальные алгоритмы. Проблема  $N=NP$
2. Эллиптические кривые над полем  $R$ . Геометрическая и алгебраическая интерпретация сложения.
3. Ассоциативность сложения в группе точек на эллиптической кривой
4. Эллиптические кривые над произвольным полем.
5. Мощность группы точек эллиптической кривой над полем вычетов по простому модулю (теорема Хассе)
6. Аналоги криптографических алгоритмов Диффи-Хеллмана и Эль-Гамала в группе точек на эллиптической кривой над конечным полем.
7. Современные стандарты цифровой подписи РФ и США.
8. Криптостойкость криптографических алгоритмов, использующих эллиптические кривые.
9. Построение «хороших» эллиптических кривых.

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

1. Понятие сложности алгоритмов. Полиномиальные и экспоненциальные алгоритмы. Проблема  $N=NP$
2. Эллиптические кривые над полем  $R$ . Геометрическая и алгебраическая интерпретация сложения.
3. Ассоциативность сложения в группе точек на эллиптической кривой



4. Эллиптические кривые над произвольным полем.
5. Мощность группы точек эллиптической кривой над полем вычетов по простому модулю (теорема Хассе)
6. Аналоги криптографических алгоритмов Диффи-Хеллмана и Эль-Гамала в группе точек на эллиптической кривой над конечным полем.
7. Современные стандарты цифровой подписи РФ и США.
8. Криптостойкость криптографических алгоритмов, использующих эллиптические кривые.
9. Построение «хороших» эллиптических кривых.
10. Использование проективных координат для оптимизации вычислений.
11. Решетки, базис и определитель: основные свойства.
12. Базисы двумерных решеток
13. Теорема Минковского о выпуклом теле и ее следствия
14. Процесс ортогонализации Грамма-Шмидта
15. Мю-приведенные базисы и их построение.
16. Минимумы решеток. Постоянная Эрмита
17. Алгоритм Лагранжа построения L-приведенного базиса.
18. Алгоритм Эрмита нахождения короткого вектора решетки.
19. Алгоритмические задачи на решетках, используемые в криптографии
20. LLL-приведенный базис и его свойства
21. LLL-алгоритм.
22. Криптосистема GGH
23. Цифровая подпись GGH
24. Шифр NTRU
25. Цифровая подпись NTRUSign
1. Понятие сложности алгоритмов. Полиномиальные и экспоненциальные алгоритмы. Проблема  $P=NP$
2. Эллиптические кривые над полем  $R$ . Геометрическая и алгебраическая интерпретация сложения.
3. Ассоциативность сложения в группе точек на эллиптической кривой
4. Эллиптические кривые над произвольным полем.
5. Мощность группы точек эллиптической кривой над полем вычетов по простому модулю (теорема Хассе)
6. Аналоги криптографических алгоритмов Диффи-Хеллмана и Эль-Гамала в группе точек на эллиптической кривой над конечным полем.
7. Современные стандарты цифровой подписи РФ и США.
8. Криптостойкость криптографических алгоритмов, использующих эллиптические кривые.
9. Построение «хороших» эллиптических кривых.
10. Использование проективных координат для оптимизации вычислений.
11. Решетки, базис и определитель: основные свойства.
12. Базисы двумерных решеток
13. Теорема Минковского о выпуклом теле и ее следствия
14. Процесс ортогонализации Грамма-Шмидта
15. Мю-приведенные базисы и их построение.
16. Минимумы решеток. Постоянная Эрмита
17. Алгоритм Лагранжа построения L-приведенного базиса.
18. Алгоритм Эрмита нахождения короткого вектора решетки.
19. Алгоритмические задачи на решетках, используемые в криптографии
20. LLL-приведенный базис и его свойства
21. LLL-алгоритм.
22. Криптосистема GGH
23. Цифровая подпись GGH
24. Шифр NTRU
25. Цифровая подпись NTRUSign

- 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**

Во время проведения дифференцированного зачета обучающиеся могут пользоваться программой дисциплины.