БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ

Ректор Белорусского
государственного университета

_____А.Д.Король

10 июня 2024 г.

Регистрационный №УД-13254/уч.

ТЕОРЕТИКО-ЧИСЛОВЫЕ МЕТОДЫ В КРИПТОГРАФИИ

Учебная программа учреждения образования
по учебной дисциплине для специальности:

1-31 03 08 Математика и информационные технологии (по направлениям)

2024 г.

Учебная программа составлена на основе ОСВО 1-31 03 08-2021 и учебных планов № G-31-1-011/уч от 25.05.2021, № G-31-1-017/уч от 25.05.2021, № G-31-1-003/уч.з от 31.05.2021, № G-31-1-004/уч.з от 31.05.2021.

СОСТАВИТЕЛИ:

Беняш-Кривец Валерий Вацлавович – профессор кафедры высшей алгебры и защиты информации механико-математического факультета Белорусского государственного университета, доктор физико-математических наук, профессор;
Тихонов Сергей Викторович – заведующий кафедрой высшей алгебры и защиты информации механико-математического факультета Белорусского государственного университета, кандидат физико-математических наук, доцент.

РЕЦЕНЗЕНТЫ:

Васильев Денис Владимирович, заведующий отделом теории чисел и дискретной математики Института математики НАН Беларуси, кандидат физико-математических наук.
Базылев Дмитрий Федорович – заведующий кафедрой геометрии, топологии и методики преподавания математики механико-математического факультета Белорусского государственного университета, кандидат физико-математических наук, доцент.

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:

Кафедрой высшей алгебры и защиты информации БГУ
(протокол № 12 от 29.05.2024);

Научно-методическим советом БГУ
(протокол № 8 от 31.05.2024)

Заведующий кафедрой _____ С.В. Тихонов

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Цели и задачи учебной дисциплины

За последнее время компьютерная безопасность и криптография стали особенно актуальны для развития современного общества. Эти дисциплины находятся на стыке нескольких научных направлений, но особо важную роль в них играют математические методы и алгоритмы обеспечения информационной безопасности. Программа дисциплины “Теоретико-числовые методы в криптографии” непосредственно посвящена математическим методам, используемым при построении современных криптосистем. Целью курса является обучение магистрантов теоретико-числовым и алгебраическим методам, лежащим в основе построения и работы современных криптосистем.

Образовательная цель: ознакомить студентов с теоретико-числовыми и алгебраическими методами обеспечения компьютерной безопасности; дать математическое обоснование алгоритмов криптографии с открытым ключом.

Развивающая цель: формирование у учащихся понимания принципов построения и работы современных систем защиты информации.

Основные задачи, решаемые в рамках изучения дисциплины «Теоретико-числовые методы в криптографии»:

– ознакомить студентов с фундаментальными понятиями алгебры и теории чисел, используемыми в криптографии с открытым ключом;

– изучить основы теории эллиптических кривых;

– ознакомить студентов с основными принципами построения криптосистем с открытым ключом;

– ознакомить студентов с некоторыми алгоритмами факторизации и проверки чисел на простоту;

– развить у студентов аналитическое мышление и общую математическую культуру;

– привить студентам умение самостоятельно изучать учебную и научную литературу в области математики и ее приложений.

Место учебной дисциплины в системе подготовки специалиста с высшим образованием.

Учебная дисциплина относится **к модулю** «Алгебра и геометрия» **2** компонента учреждения высшего образования.

Связи с другими учебными дисциплинами, включая учебные дисциплины компонента учреждения высшего образования, дисциплины специализации и др.

Данная дисциплина опирается и использует изученные ранее сведения из дисциплины «Алгебра и теория чисел».

Требования к компетенциям

Освоение учебной дисциплины «Теоретико-числовые методы в криптографии» должно обеспечить формирование следующих компетенций:

Специализированные компетенции:

Применять основные алгоритмы компьютерной геометрии и современные математические средства визуализации изображений и анимации.

В результате изучения учебной дисциплины студент должен:

знать:

– общие математические основы построения криптосистем с открытым ключом;

– протоколы работы широко используемых криптосистем;

уметь:

– производить вычисления в конечных полях;

– находить символы Лежандра и Якоби;

– находить порядок группы точек специальных эллиптических кривых над конечными полями;

– строить конечные поля заданного порядка;

– строить расширения полей и выполнять вычисления в них;

владеть:

– основными навыками решения задач, связанных с эллиптическими кривыми и конечными полями;

– методами доказательств основных теорем, встречающихся в дисциплине «Теоретико-числовые методы в криптографии».

– навыками самообразования и способами использования аппарата алгебры и теории чисел для проведения математических и междисциплинарных исследований.

Структура учебной дисциплины

Дисциплина изучается в 7 семестре для очной формы и в 8 семестре для заочной формы. Всего на изучение учебной дисциплины «Теоретико-числовые методы в криптографии» отведено:

7 семестр:

– для очной формы получения высшего образования: 90 часов, в том числе 54 аудиторных часа, из них: лекции – 18 часов, лабораторные занятия – 32 часа, управляемая самостоятельная работа (УСР) – 4 часа.

8 семестр:

– для заочной формы получения высшего образования: 90 часов, в том числе 12 аудиторных часов, из них: лекции – 4 часа, лабораторные занятия – 8 часов, контрольная работа.

Трудоемкость учебной дисциплины составляет 3 зачетные единицы.

Формой промежуточной аттестации – зачет.

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

Тема 1. Алгебраические основы

Группа. Подгруппа. Факторгруппа. Алгоритмы возведения в степень. Задача дискретного логарифмирования. Кольцо. Идеал. Простые и максимальные идеалы. Факторкольцо. Теорема о гомоморфизме колец. Поле. Характеристика поля. Степень расширения полей. Алгебраические расширения.

Тема 2. Конечные поля

Число элементов в конечном поле. Мультипликативная группа конечного поля. Автоморфизм Фробениуса. Критерий неприводимости многочленов над конечным полем. Алгоритм Берлекэмпа. Построение неприводимых многочленов над конечным полем.

Тема 3. Теоретико-числовые основы

Алгоритм Евклида. Функция Эйлера. Теорема Эйлера. Квадратичные вычеты по модулю p. Символ Лежандра. Квадратичный закон взаимности. Символ Якоби. Вычисление символа Якоби. Китайская теорема об остатках.

Тема 4. Эллиптические кривые

Аффинное и проективное пространства. Уравнение Вейерштрасса над полями различной характеристики. Определение эллиптической кривой. Групповой закон на множестве точек эллиптической кривой. Формулы сложения точек в аффинных и проективных координатах. Вычисление кратной точки. Эллиптические кривые над кольцами классов вычетов.

Тема 5. Вычисление порядка группы точек эллиптической кривой над конечным полем

Кольцо формальных степенных рядов. Дзета-функция эллиптической кривой. Теорема Вейля для эллиптической кривой. Теорема Хассе о порядке группы точек эллиптической кривой над конечным полем.

Тема 6. Алгоритмы факторизации и проверки числа на простоту

Детерминированные тесты на простоту. Числа Мерсенна. Вероятностные тесты Соловея-Штрассена и Миллера-Рабина на простоту. Факторизация целых чисел с помощью эллиптических кривых. Тестирование чисел на простоту с помощью эллиптических кривых.

Тема 7. Криптосистемы с открытым ключом

Понятия односторонней функции и односторонней функции с секретом. Протокол обмена ключами Диффи–Хеллмана. Криптосистема Эль-Гамаля. Криптосистема RSA. Атаки на криптосистему RSA. Криптосистема Рабина.

Тема 8. Электронная цифровая подпись

Общая схема электронной цифровой подписи. Схема электронной цифровой подписи Эль-Гамаля. Схема электронной цифровой подписи на эллиптических кривых.

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА УЧЕБНОЙ ДИСЦИПЛИНЫ

Очная (дневная) форма получения высшего образования с применением дистанционных образовательных технологий (ДОТ)

Номер раздела, темы	Название раздела, темы	Количество аудиторных часов					Количество часов УСР	Форма контроля
		Лекции	Практические занятия	Семинарские занятия	Лабораторные занятия	Иное		
1	2	3	4	5	6	7	8	9
1.	Алгебраические основы	2			4			Устный опрос
2.	Конечные поля	2			4			Устный опрос
3.	Теоретико-числовые основы	2			4		2	Устный опрос, контрольная работа
4.	Эллиптические кривые	2			4			Устный опрос
5.	Вычисление порядка группы точек эллиптической кривой над конечным полем	4			4			Устный опрос, коллоквиум
6.	Алгоритмы факторизации и проверки числа на простоту	2			4			Устный опрос
7.	Криптосистемы с открытым ключом	2			4		2	Устный опрос, контрольная работа
8.	Электронная цифровая подпись	2			4			Устный опрос
	Итого	**18**			**32**		**4**	

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА УЧЕБНОЙ ДИСЦИПЛИНЫ

Заочная форма получения высшего образования

Номер раздела, темы	Название раздела, темы	Количество аудиторных часов					Форма контроля
		Лекции	Практические занятия	Семинарские занятия	Лабораторные занятия	Иное	
1	2	3	4	5	6	7	8
1.	Алгебраические основы	1			1		Устный опрос
2.	Конечные поля				1		Устный опрос
3.	Теоретико-числовые основы	1			1		Устный опрос
4.	Эллиптические кривые	1			1		Устный опрос
5.	Вычисление порядка группы точек эллиптической кривой над конечным полем				1		Устный опрос
6.	Алгоритмы факторизации и проверки числа на простоту				1		Устный опрос
7.	Криптосистемы с открытым ключом	1			1		Устный опрос
8.	Электронная цифровая подпись				1		Устный опрос
	Итого	**4**			**8**		

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

Основная литература

1. Криптология : учебник для студентов учреждений высшего образования по математическим и техническим специальностям / [Ю. С. Харин и др.] ; БГУ. - 2-е изд., пересмотр. - Минск : БГУ, 2023. - 511 с. - URL: https://elib.bsu.by/handle/123456789/309839.
2. Глухов, М. М. Алгебра : учебник для студентов вузов, обучающихся по укрупненной группе направлений подготовки и специальностей "Информационная безопасность" / М. М. Глухов, В. П. Елизаров, А. А. Нечаев. - Изд. 4-е, стер. - Санкт-Петербург ; Москва ; Краснодар : Лань, 2022. - 606 с. - URL: https://e.lanbook.com/book/187793.
3. Мартынов, Л. М. Алгебра и теория чисел для криптографии : учебное пособие [для вузов] / Л. М. Мартынов. - Изд. 2-е, стер. - Санкт-Петербург ; Москва ; Краснодар : Лань, 2022. - 454 с. - URL: https://e.lanbook.com/book/189446.
4. Нестеров, С. А. Основы информационной безопасности : учебник / С. А. Нестеров. - Изд. 2-е, стер. - Санкт-Петербург ; Москва ; Краснодар : Лань, 2023. - 320 с. - URL: https://e.lanbook.com/book/206279.
5. Деза, Е. И. Введение в криптографию. Теоретико-числовые основы защиты информации : [учебное пособие] / Е. И. Деза, Л. В. Котова. - Изд. стер. - Москва : URSS : ЛЕНАНД, 2022. - 368 с.

Дополнительная литература

1. Виноградов, И. М. Основы теории чисел : учебное пособие [для вузов] / И. М. Виноградов. - Изд. 15-е, стер. - Санкт-Петербург ; Москва ; Краснодар : Лань, 2023. - 176 с. - URL: https://e.lanbook.com/book/298499.
2. Коблиц Н. Введение в эллиптические кривые и модулярные формы. М.: Мир, 1988.
3. Ленг С. Алгебра. М.: Мир, 1968.
4. Koblitz N. Algebraic aspects of cryptography. Springer-Verlag, 1998.
5. Silverman J.H. The arithmetic of elliptic curves. Springer-Verlag, 1985.
6. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. М.: Гелиос АРВ, 2001.
7. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии. МЦНМО, 2003.
8. Ростовцев А.Г., Маховенко Е.Б. Теоретическая криптография. АНО НПО Профессионал, 1985.

Перечень рекомендуемых средств диагностики и методика формирования итоговой отметки

Объектом диагностики компетенций студентов являются знания, умения, полученные ими в результате изучения учебной дисциплины. Выявление учебных достижений студентов осуществляется с помощью мероприятий текущей и промежуточной аттестации.

Для диагностики компетенций могут использоваться следующие средства текущей аттестации: контрольная работа; коллоквиум; устный опрос на аудиторных занятиях.

Формой промежуточной аттестации по дисциплине «Теоретико-числовые методы в криптографии» учебным планом предусмотрен **зачет**.

Зачет по дисциплине выставляется в случае сдачи всех контрольных работ и коллоквиума.

Примерный перечень заданий для управляемой самостоятельной работы

Тема 3. Теоретико-числовые основы. (2 ч)

1. Сколько элементов в поле, являющемся расширением степени 2 поля F_9?
2. Содержит ли поле F_{625} поле F_{16}?
3. Содержит ли поле F_{32} поле F_{27}?
4. Найдите степень расширения полей $[F_{64} : F_4]$
5. Какая характеристика у расширения степени 3 поля F_{49}?
6. Сколько корней в поле F_{81} имеет многочлен x^3+2x+1?
7. Сколько корней в поле F_{125} имеет многочлен x^3+x+1?
8. Является ли идеал $(x^2 - 2)$ максимальным в кольце $F_7[x]$?
9. Приводим ли над полем F_3 многочлен x^4-2. Если приводим, разложить этот многочлен на множители.
10. Построить неприводимый многочлен степени 127 над полем F_2.
11. Является ли 237 квадратом в поле F_{1973}^{2022}?
12. Вычислите значение функции Эйлера для числа a: а) $a = 142560$; б) $a = 421200$.
13. С помощью алгоритма Евклида вычислите $НОД(a,b)$ и выразите его через исходные числа. Используя связь НОД и НОК двух натуральных чисел, вычислите $НОК(a,b)$: а) $a = 5544, b = 7644$; б) $a = 1188, b = 3080$; в) $a = 1296, b = 6600$.
14. Найдите остаток от деления 23^{519} на 9.
15. Найдите символ Якоби $\left(\frac{136}{21}\right)$.
16. Найти такое натуральное n, что $n \equiv 2 (mod\ 9)$, $n \equiv 1 (mod\ 4)$ и $n \equiv 3 (mod\ 5)$.
17. Является ли 20 первообразным корнем по модулю 9?
18. Является ли 237 квадратом в поле F_{1973}^{2023}?

Форма контроля – устный опрос, контрольная работа.

Тема 7. Криптосистемы с открытым ключом. (2 ч)

1. Сколько элементов второго порядка в группе E(Q), где E – эллиптическая кривая, заданная над полем рациональных чисел уравнением $y^2 = x^3-8$?
2. Пусть эллиптическая кривая E задана над полем F_2 уравнением $y^2+y = x^3+x^2$. Найдите $|E(F_8)|$.
3. Найдите порядок точки P=(0,4) на эллиптической кривой, заданной над полем рациональных чисел уравнением $y^2 = x^3+16$.
4. Найдите все точки второго порядка на эллиптической кривой, заданной над полем характеристики 5 уравнением $y^2 = x^3+ x$.
5. Является ли проективная кривая, заданная над полем рациональных чисел уравнением $zy^2 = x^3 - xz^2$, эллиптической кривой?
6. Алиса опубликовала свои открытые ключи: $N = 2038667$, $e = 103$.

а) Боб хочет отправить Алисе сообщение $m = 892383$. Какое цифровое сообщение пошлет Боб Алисе?

б) Алиса знает, что ее модуль делится на простое число $p = 1301$. Найти секретную экспоненту d для Алисы.

в) Алиса получила зашифрованный текст $c = 317730$ от Боба. Расшифруйте сообщение.

Форма контроля – устный опрос, контрольная работа.

Примерные варианты контрольных работ

Контрольная работа 1.

1. Сколько элементов в мультипликативной группе поля, являющегося расширением степени 5 поля F_9?
2. Пусть степень расширения $F(\alpha)/F$ нечетная. Докажите, что $F(\alpha^2)= F(\alpha)$.
3. Сколько корней в поле F_{125} имеет многочлен x^3+x+1?
4. Разложите многочлен x^4+x^3+x+2 на неприводимые множители над полем F_3.
5. Содержит ли поле F_{625} поле F_{125}?

Контрольная работа 2.

1. С помощью алгоритма Евклида вычислите *НОД* (554, 762) и выразите его через исходные числа.
2. Найдите символ Якоби $\left(\frac{136}{21}\right)$
3. Найдите остаток от деления 19^{315} на 8.
4. Сколько элементов второго порядка в группе E(Q), где E – эллиптическая кривая, заданная над полем рациональных чисел уравнением $y^2=x^3-8$?

5. Пусть эллиптическая кривая E задана над полем F_2 уравнением $y^2+y=x^3+x^2$. Найдите $|E(F_8)|$.

Примерная тематика лабораторных занятий
(очная (дневная) форма получения высшего образования)

Лабораторное занятие 1. Группа. Подгруппа. Факторгруппа. Алгоритмы возведения в степень. Задача дискретного логарифмирования.

Лабораторное занятие 2. Кольцо. Идеал. Простые и максимальные идеалы. Факторкольцо. Теорема о гомоморфизме колец. Поле. Характеристика поля. Степень расширения полей. Алгебраические расширения.

Лабораторное занятие 3. Число элементов в конечном поле. Мультипликативная группа конечного поля. Автоморфизм Фробениуса.

Лабораторное занятие 4. Критерий неприводимости многочленов над конечным полем. Алгоритм Берлекэмпа. Построение неприводимых многочленов над конечным полем.

Лабораторное занятие 5. Алгоритм Евклида. Функция Эйлера. Теорема Эйлера. Квадратичные вычеты по модулю *p*.

Лабораторное занятие 6. Символ Лежандра. Квадратичный закон взаимности. Символ Якоби. Вычисление символа Якоби. Китайская теорема об остатках.

Лабораторное занятие 7. Аффинное и проективное пространства. Уравнение Вейерштрасса над полями различной характеристики. Определение эллиптической кривой. Групповой закон на множестве точек эллиптической кривой.

Лабораторное занятие 8. Формулы сложения точек в аффинных и проективных координатах. Вычисление кратной точки. Эллиптические кривые над кольцами классов вычетов.

Лабораторное занятие 9. Кольцо формальных степенных рядов.

Лабораторное занятие 10. Дзета-функция эллиптической кривой. Теорема Вейля для эллиптической кривой. Теорема Хассе о порядке группы точек эллиптической кривой над конечным полем.

Лабораторное занятие 11. Детерминированные тесты на простоту. Числа Мерсенна. Вероятностные тесты Соловея-Штрассена и Миллера-Рабина на простоту.

Лабораторное занятие 12. Факторизация целых чисел с помощью эллиптических кривых. Тестирование чисел на простоту с помощью эллиптических кривых.

Лабораторное занятие 13. Понятия односторонней функции и односторонней функции с секретом. Протокол обмена ключами Диффи–Хеллмана. Криптосистема Эль-Гамаля.

Лабораторное занятие 14. Криптосистема RSA. Атаки на криптосистему RSA. Криптосистема Рабина.

Лабораторное занятие 15. Общая схема электронной цифровой подписи. Схема электронной цифровой подписи Эль-Гамаля.

Лабораторное занятие 16. Схема электронной цифровой подписи на эллиптических кривых.

Примерная тематика лабораторных занятий
(заочная форма получения высшего образования)

Лабораторное занятие 1. Группа. Подгруппа. Факторгруппа. Алгоритмы возведения в степень. Задача дискретного логарифмирования. Кольцо. Идеал. Простые и максимальные идеалы. Факторкольцо. Теорема о гомоморфизме колец. Поле. Характеристика поля. Степень расширения полей. Алгебраические расширения.

Лабораторное занятие 2. Число элементов в конечном поле. Мультипликативная группа конечного поля. Автоморфизм Фробениуса. Критерий неприводимости многочленов над конечным полем. Алгоритм Берлекэмпа. Построение неприводимых многочленов над конечным полем.

Лабораторное занятие 3. Алгоритм Евклида. Функция Эйлера. Теорема Эйлера. Квадратичные вычеты по модулю p. Символ Лежандра. Квадратичный закон взаимности. Символ Якоби. Вычисление символа Якоби. Китайская теорема об остатках.

Лабораторное занятие 4. Аффинное и проективное пространства. Уравнение Вейерштрасса над полями различной характеристики. Определение эллиптической кривой. Групповой закон на множестве точек эллиптической кривой. Формулы сложения точек в аффинных и проективных координатах. Вычисление кратной точки. Эллиптические кривые над кольцами классов вычетов.

Лабораторное занятие 5. Кольцо формальных степенных рядов. Дзета-функция эллиптической кривой. Теорема Вейля для эллиптической кривой. Теорема Хассе о порядке группы точек эллиптической кривой над конечным полем.

Лабораторное занятие 6. Детерминированные тесты на простоту. Числа Мерсенна. Вероятностные тесты Соловея-Штрассена и Миллера-Рабина на простоту. Факторизация целых чисел с помощью эллиптических кривых. Тестирование чисел на простоту с помощью эллиптических кривых.

Лабораторное занятие 7. Понятия односторонней функции и односторонней функции с секретом. Протокол обмена ключами Диффи–Хеллмана. Криптосистема Эль-Гамаля. Криптосистема RSA. Атаки на криптосистему RSA. Криптосистема Рабина.

Лабораторное занятие 8. Общая схема электронной цифровой подписи. Схема электронной цифровой подписи Эль-Гамаля. Схема электронной цифровой подписи на эллиптических кривых.

Описание инновационных подходов и методов к преподаванию учебной дисциплины

При организации образовательного процесса используется **практико-ориентированный подход**, который предполагает:

– освоение содержание образования через решения практических задач;

– приобретение навыков эффективного выполнения разных видов профессиональной деятельности;

– ориентацию на генерирование идей, реализацию групповых студенческих проектов, развитие предпринимательской культуры;

– использованию процедур, способов оценивания, фиксирующих сформированность профессиональных компетенций.

Методические рекомендации по организации самостоятельной работы

Для организации самостоятельной работы студентов по учебной дисциплине «Теоретико-числовые методы в криптографии» используются современные информационные ресурсы: размещается на образовательном портале комплекс учебных и учебно-методических материалов (учебно-программные материалы, учебное издание для теоретического изучения дисциплины, материалы текущего контроля и текущей аттестации, позволяющие определить соответствие учебной деятельности обучающихся требованиям образовательных стандартов высшего образования и учебно-программной документации, в т.ч. вопросы для подготовки к зачету, задания, вопросы для самоконтроля и др., список рекомендуемой литературы, информационных ресурсов и др.).

При изучении дисциплины до сведения студентов вначале семестра доводится информация, которая включает: методы и формы контроля знаний и правила начисления баллов. Для активации работы студентов в семестре используется:

– организация непрерывного текущего контроля качества знаний студентов в течение всего срока изучения дисциплины;

– стимулирование работы студентов в течение семестра на основе использования накопительной рейтинговой системы;

– повышение значимости самостоятельной и индивидуальной работы путем разработки и выдачи студентам индивидуальных вариантов заданий, возможность получить консультацию и индивидуальную помощь при их выполнении;

– дифференцированный подход к оценке знаний студентов, стимулирование высокого рейтинга по дисциплине.

Примерный перечень вопросов к зачету

1. Группа. Определение. Примеры.
2. Подгруппа. Факторгруппа.

3. Гомоморфизм групп. Теорема о гомоморфизме групп.
4. Порядок элемента группы. Циклическая группа. Примеры.
5. Кольца. Определение. Примеры.
6. Мультипликативная группа кольца.
7. Идеал. Факторкольцо.
8. Гомоморфизм колец. Теорема о гомоморфизме колец.
9. Простые и максимальные идеалы.
10. Идеалы в кольце целых чисел.
11. Идеалы в кольце многочленов.
12. Поле. Определение. Примеры.
13. Критерии простоты и максимальности идеалов.
14. Характеристика поля. Определение. Примеры.
15. Степень расширения полей.
16. Число элементов в конечном поле.
17. Существование конечного поля, состоящего из p^n элементов.
18. Мультипликативная группа конечного поля.
19. Автоморфизм Фробениуса.
20. Критерий неприводимости многочленов над конечными полями.
21. Алгоритм Берлекэмпа.
22. Построение неприводимых многочленов над конечным полем.
23. Алгоритм Евклида.
24. Функция Эйлера. Теорема Эйлера.
25. Квадратичные вычеты по модулю p.
26. Символ Лежандра. Определение. Критерий Эйлера.
27. Свойства символа Лежандра.
28. Символ Якоби. Определение и свойства.
29. Китайская теорема об остатках.
30. Первообразные корни. Существование первообразных корней по модулям p^n и $2p^n$.
31. Аффинное и проективное пространства.
32. Определение эллиптической кривой.
33. Групповой закон на множестве точек эллиптической кривой.
34. Формулы сложения точек эллиптической кривой. Аффинные и проективные координаты.
35. Бинарный метод вычисления кратной точки. Задача дискретного логарифмирования.
36. Дзета-функция эллиптической кривой. Теорема Вейля для эллиптической кривой.
37. Теорема Хассе о порядке группы точек эллиптической кривой над конечным полем.
38. Детерминированные тесты на простоту. Числа Мерсенна.
39. Тест Соловея-Штрассена проверки числа на простоту.
40. Тест Миллера-Рабина проверки числа на простоту.
41. Факторизация целых чисел с помощью эллиптических кривых.
42. Тестирование чисел на простоту с помощью эллиптических кривых.

43. Протоколом обмена ключами Диффи-Хеллмана.
44. Понятие односторонней функции. Криптосистема Эль-Гамаля.
45. Криптосистема RSA.
46. Криптосистема Рабина.
47. Электронная цифровая подпись Эль-Гамаля.
48. Электронная цифровая подпись на эллиптических кривых.

ПРОТОКОЛ СОГЛАСОВАНИЯ УЧЕБНОЙ ПРОГРАММЫ УО

Название учебной дисциплины, с которой требуется согласование	Название кафедры	Предложения об изменениях в содержании учебной программы учреждения высшего образования по учебной дисциплине	Решение, принятое кафедрой, разработавшей учебную программу (с указанием даты и номера протокола)
Учебная дисциплина не требует согласования			

Заведующий кафедрой
кандидат физико- математических наук, доцент _____ С.В. Тихонов

29. мая 2024 г.

ДОПОЛНЕНИЯ И ИЗМЕНЕНИЯ К УЧЕБНОЙ ПРОГРАММЕ ПО ИЗУЧАЕМОЙ УЧЕБНОЙ ДИСЦИПЛИНЕ

на _____/_____ учебный год

№ п/п	Дополнения и изменения	Основание

Учебная программа пересмотрена и одобрена на заседании кафедры
_____(протокол № ____ от _____ 202_ г.)
(название кафедры)

Заведующий кафедрой

_____ _____
(ученая степень, ученое звание) (И.О.Фамилия)

УТВЕРЖДАЮ
Декан факультета

_____ _____
(ученая степень, ученое звание) (И.О.Фамилия)