Федеральное государственное бюджетное образовательное

учреждение высшего образования

Московский государственный университет имени М.В. Ломоносова

Факультет вычислительной математики и кибернетики

**УТВЕРЖДАЮ**

декан факультета вычислительной математики и кибернетики

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_/И.А. Соколов /**

**«\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_\_г.**

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**

**Наименование дисциплины:**

**Математические основы криптологии**

**Уровень высшего образования:**

**бакалавриат**

**Направление подготовки / специальность:**

**01.03.02 «Прикладная математика и информатика» (3++)**

**Направленность (профиль):**

**Математические методы обработки информации и принятия решений**

**Форма обучения:**

**очная**

**Москва 2023**

Рабочая программа дисциплины (модуля) разработана в соответствии с самостоятельно установленным МГУ образовательным стандартом (ОС МГУ) для реализуемых основных профессиональных образовательных программ высшего образования по направлению подготовки 01.03.02, 01.04.02 "Прикладная математика и информатика" программы бакалавриата Утвержден приказом МГУ от 30 августа 2019 года № 1041 (в редакции приказов МГУ от 11 сентября 2019 года № 1109, от 10 июня 2021 года № 609, от 7 октября 2021 года № 1048, от 21 декабря 2021 года № 1404, от 2 ноября 2022 года № 1299)

**1.** Дисциплина относится к вариативной части ОПОП ВО.

**2.** Входные требования для освоения дисциплины (модуля): учащиеся должны владеть знаниями по математическому анализу и линейной алгебре, теории вероятностей в объеме, соответствующем программе первого и второго года обучения основных образовательных программ бакалавриата по укрупненным группам направлений и специальностей 01.00.00 «Математика и механика», 02.00.00 «Компьютерные и информационные науки».

**3.** Результаты обучения по дисциплине (модулю), соотнесенные с требуемыми компетенциями выпускников*.*

Компетенции выпускников, частично формируемые при реализации дисциплины (модуля):

* **ОПК-1.Б** Способность применять и адаптировать существующие математические и компьютерные методы для разработки и реализации алгоритмов решения актуальных задач в области фундаментальной и прикладной математики.
* **ПК-2.Б** Способность понимать и применять в научно-исследовательской деятельности современный математический аппарат.
* **ПК-5.Б** Способность определить совокупность математических методов и программных решений для отдельного этапа решения прикладной задачи в рамках заданной схемы.

Планируемые результаты обучения по дисциплине (модулю):

**Знать:**

1. основные понятия, определения и факты теории чисел и алгебры применяемые в криптологии.

**Уметь:**

1. применять на практике основные методы алгебры и теории чисел, при синтезе и анализе криптосистем защиты информации;
2. применять на практике компьютерные технологии для решения различных задач обеспечения защиты информации в компьютерных системах;
3. находить, анализировать и обрабатывать научно-техническую информацию;
4. извлекать полезную научно-техническую информацию из электронных библиотек, реферативных журналов;
5. демонстрировать способность к анализу и синтезу;
6. демонстрировать способность к письменному и устному общению на русском языке;
7. публично представить собственные и известные научные результаты;
8. представить математические знания в устной форме;

**Владеть:**

1. навыками решения практических задач, возникающих при синтезе и анализе криптоалгоритмов;
2. теоретико-числовыми и алгебраическими методами при решении задач защиты информации в компьютерных системах, проблемно-задачной формой представления математических знаний;
3. проблемно-задачной формой представления естественнонаучных знаний;

**4.** Формат обучения: занятия проводятся с использованием меловой или маркерной доски, интерактивные материалы демонстрируются с помощью ноутбука и проектора.

**5.** Объем дисциплины (модуля) составляет 4 з.е., в том числе 72 академических часов, отведенных на контактную работу обучающихся с преподавателем, 72 академических часов на самостоятельную работу обучающихся.

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

|  |  |  |
| --- | --- | --- |
| **Наименование и краткое содержание разделов и тем дисциплины (модуля),****Форма промежуточной аттестации по дисциплине (модулю)** | **Всего****(часы**) | В том числе |
| **Контактная работа (работа во взаимодействии с преподавателем)****Виды контактной работы, часы** | **Самостоятельная работа обучающегося,** **часы**  |
| Занятия лекционного типа\* | Занятия семинарского типа\* | **Всего** |  |
| 1. Основные задачи криптографии.

 Исторический экскурс. Математические модели шифров, методы и алгоритмы их построения. | **12** | 4 | 4 | **8** | **4** |
| 1. Теоретико-числовые алгоритмы и методы в криптологии.

Кольцо целых чисел. Делимость, алгоритм Евклида, сравнения и их свойства. Группа обратимых элементов кольца вычетов. Теорема Эйлера. Теорема об однозначности расшифрования в криптосистеме RSA. Строение группы обратимых элементов по примарному модулю. Квадратичные вычеты. Символы Лежандра и Якоби и их свойства. Алгоритмы решения квадратичных сравнений в кольцах вычетов. Алгоритмы порождения простых чисел и тесты проверки на простоту. | **24** | 8 | 8 | **16** | **8** |
| 1. Конечные поля и их свойства.

Минимальные и примитивные многочлены. Группа автоморфизмов конечного поля. Рекуррентные последовательности над конечным полем. Регистры сдвига. Алгоритмы построения рекуррентных последовательностей большого периода. Линейный конгруэнтный метод построения псевдослучайной последовательности. | **24** | 8 | 8 | **16** | **8** |
| 1. Конечные группы

Теорема Лагранжа. Нормализатор и централизатор, сопряженные элементы. Теорема о числе множеств, сопряженных с данным. Теорема о разложении абелевой группы в прямое произведение своих циклических подгрупп. Теорема Коши. Теорема о центре примарной группы. Двойные смежные классы. Силовская подгруппа конечной группы. Теоремы Силова. | **24** | 8 | 8 | **16** | **8** |
| 1. Конечные группы подстановок.

Орбита, стабилизатор, транзитивность. Теорема о порядке конечной группы подстановок. Полурегулярные, регулярные группы и их свойства. Блоки группы подстановок и их свойства. Импримитивные группы подстановок. Критерий импримитивности. Кратная транзитивность. Группа подстановок с регулярным нормальным делителем. Простая группа. Теорема о простоте знакопеременной группы. Системы образующих симметрических и знакопеременных групп. Теорема Софи Пикар. | **24** | 8 | 8 | **16** | **8** |
| Промежуточная аттестация: устный экзамен | **36** | 0 | 0 | **0** | **36** |
| **Итого** | **144** | **36** | **36** | **72** | **72** |

7. Фонд оценочных средств (ФОС)для оценивания результатов обучения по дисциплине (модулю)

7.1. Типовые контрольные задания или иные материалы для проведения текущего контроля успеваемости.

|  |
| --- |
| Контрольная работа № 1 |
| Вариант 1 |  |
| 1. Доказать, что $37 | 2^{2^{6n+2}}+ 21.$2. Доказать, что если p = 2q + 1, p,q– простые q ≡ 1 (mod 4), то <2> = $Z\_{p}^{\*}$.3. Доказать, что если p | (bn – 1), (b, p) = 1, то 1) либо p | (bd – 1), где d | n, либо p ≡ 1 (modn); 2) если p>2 и n- нечетное, то p ≡ 1 (mod2n).4. Доказать, что если p = 4m + 3, p–простое, m≥ 1, $\left(\frac{a}{p}\right)$ = 1, сравнение x2 ≡ a(modp) имеет решение x ≡ ±am + 1 (modp). |  |
| Контрольная работа № 2 |
| Вариант 1 |  |
| 1. Выписать характеристическое уравнение и цикловую структуру ЛРП, заданной характеристическим уравнением f(x) = x8+ x6 + x2 + x + 1.2. Доказать, что РП, заданная рекуррентным уравнением:$x\_{i}= x\_{i-3} ⊕ x\_{i-5} ⊕ \overline{x\_{i-1}}\overline{x\_{i-2}}\overline{x\_{i-3}}\overline{x\_{i-4}}$, i = 6, … имеет период T = 323. Найти все значения параметров a, b, cпри которых многочленf(x) = x27+ax17+ bx+c биективен по модулю 3n. |  |
| Контрольная работа № 3 |
| Вариант 1 |  |
|  1. Подсчитать число всех силовских подгрупп группы S5. 2. Определить строение группы $Z\_{189}^{\*}$. 3. Пусть |G| = p2q, q>p>2. Подсчитать число элементов порядка q в группе G. |  |

***Список дополнительных задач.***

 1. Доказать, что если (k, p) = 1, то $\sum\_{x=0}^{p-1}\left(\frac{x(x-k)}{p}\right)= -1.$

 2. Доказать, что если (a, p) = 1, то x≡$b(-1)^{a-1}\left(\frac{p-1}{a-1}\right) (mod p)$решение сравнения ax≡b (mod p).

 3. Выписать характеристическое уравнение и соответствующее начальное заполнение ЛРП ранга 5 с периодом 21.

 4. Доказать, что группа < (1 2 3 4 5 6 7 8 ) >импримитивна и выписать все системы блоков этой группы.

 5. Доказать, что если простое p | и n≥ 2, то p≡ 1 (mod 2n + 2)

 6. Доказать, что если простое p= ,k≥ 1, то <5> = $Z\_{p}^{\*}$.

 7. Убедившись, что f(x) = x4 + x + 2 - примитивный над GF(3), выписать все подполя поля GF(81) = $Z\_{3}\left[θ\right]$ / $θ$4 + $θ+2.$

 8. Доказать, что множество всех 3-циклов порождает группу An, n> 3.

 9. Найти все силовы 2-группы группы S6.

7.2. Типовые контрольные задания или иные материалы для проведения промежуточной аттестации.

Вопросы к экзамену.

1. Определение математической модели шифра. Симметрические и асимметрические криптосистемы. Примеры.

2. Кольцо вычетов. Критерий взаимной простоты. Теорема Эйлера. Алгоритм вычисления обратного элемента. Теорема о корректности криптосистемы РСА. Группа обратимых элементов в кольце вычетов по примарному модулю.

3. Квадратичные вычеты. Символы Лежандра и Якоби. Алгоритм решения квадратичных сравнений в кольце вычетов.

4. Алгоритмы порождения простых чисел.

5. Тесты Соловея - Штрассена и Миллера – Рабина.

6. Конечные поля, характеристика поля, строение, вычисление обратного элемента. Теорема о примитивном элементе. Минимальные и примитивные многочлены и их свойства.

7. Подполе конечного поля. Критерий принадлежности элемента подполю. Группа автоморфизмов конечного поля.

8. Линейные рекуррентные последовательности (ЛРП) над конечным полем. Характеристический и минимальный многочлены ЛРП и их свойства. Теорема о ЛРП максимального периода.

9. Регистры сдвига, линейный и нелинейные. Построение регистров полного цикла над полем GF(2).

10. Линейный конгруэнтный метод построения псевдослучайных последовательностей. Биективные и транзитивные многочлены над кольцом вычетов. Критерий транзитивности многочлена по примарному модулю.

11. Абелевы группы. Теорема о разложении конечной абелевой группы в прямое произведение своих циклических подгрупп.

12. Нормализатор и централизатор конечной группы. Классы сопряженных элементов. Теорема Коши. Силовские подгруппы конечной группы. Теоремы Силова.

13. Конечные группы подстановок: орбиты, стабилизаторы, транзитивность, теорема о порядке группы подстановок. Лемма Бернсайда.

14. Полурегулярные, регулярные и импримитивные группы подстановок и их свойства.

15. Примитивные и кратно-транзитивные группы. Группа подстановок с регулярным нормальным делителем.

16. Простые группы. Теорема о простоте знакопеременной группы.

17. Базисы симметрической и знакопеременной групп. Теорема Софи Пикар.

|  |
| --- |
| **ШКАЛА И КРИТЕРИИ ОЦЕНИВАНИЯ результатов обучения (РО) по дисциплине (модулю)**  |
| ОценкаРО исоответствующие виды оценочных средств  | 2 | 3 | 4 | 5 |
| **Знания***Экзамен* | Отсутствие знаний | Фрагментарные знания | Общие, но не структурированные знания | Сформированные систематические знания |
| **Умения***Контрольная работа*  | Отсутствие умений | В целом успешное, но не систематическое умение | В целом успешное, но содержащее отдельные пробелы умение (допускает неточности непринципиального характера) | Успешное и систематическое умение |
| **Навыки (владения, опыт деятельности)***Экзамен* | Отсутствие навыков (владений, опыта) | Наличие отдельных навыков (наличие фрагментарного опыта) | В целом, сформированные навыки (владения), но используемые не в активной форме | Сформированные навыки (владения), применяемые при решении задач |

|  |
| --- |
| **Соответствие результатов обучения и компетенций, в развитии которых участвует дисциплина (модуль)** |
| Результаты обучения | Компетенция, с частичным формированием которой связано достижение результата обучения |
| **Знать:**1. основные понятия, определения и факты теории чисел и алгебры применяемые в криптологии.

**Уметь:**1. применять на практике основные методы алгебры и теории чисел, при синтезе и анализе криптосистем защиты информации;
2. применять на практике компьютерные технологии для решения различных задач обеспечения защиты информации в компьютерных системах;
3. находить, анализировать и обрабатывать научно-техническую информацию;
4. извлекать полезную научно-техническую информацию из электронных библиотек, реферативных журналов;
5. демонстрировать способность к письменному и устному общению на русском языке;

**Владеть:**1. навыками решения практических задач, возникающих при синтезе и анализе криптоалгоритмов;
 | ОПК-1.Б |
| **Уметь:**1. демонстрировать способность к анализу и синтезу;
2. публично представить собственные и известные научные результаты;
 | ПК-2.Б |
| **Уметь:**1. представить математические знания в устной форме;

**Владеть:**1. теоретико-числовыми и алгебраическими методами при решении задач защиты информации в компьютерных системах, проблемно-задачной формой представления математических знаний;
2. проблемно-задачной формой представления естественнонаучных знаний;
 | ПК-5.Б |

8. Ресурсное обеспечение:

Основная литература:

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

2. Кострикин А.И. Введение в алгебру. М.: Наука, 1972

3. Применко Э.А. Алгебраические основы криптографии: учебное пособие. М.: Книжный дом «Либроком», 2013

4. Гашков С.Б., Применко Э.А. Криптографические методы защиты информации. Учебное пособие. М.: Академия, 2010

Информационные справочные системы: https://cryptography.ru/

Материально-техническое обеспечение: аудитория с партами, меловой или маркерной доской.

9. Язык преподавания: русский.

10. Преподаватели: доцент факультета ВМК МГУ Э.А.Применко

11. Авторы программы: доцент факультета ВМК МГУ Э.А.Применко