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 /
«27» сентября 2022г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине

Математические основы криптологии

Уровень высшего образования:

бакалавриат

Направление подготовки / специальность:

01.03.02 "Прикладная математика и информатика" (3++)

Направленность (профиль) ОПОП:

Искусственный интеллект и анализ данных

Форма обучения:

очная

Рассмотрен и утвержден

на заседании Ученого совета факультета ВМК

(протокол №7, от 27 сентября 2022 года)

Москва 2022

1. ФОРМЫ И ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

В процессе и по завершении изучения дисциплины оценивается формирование у студентов следующих компетенций:

Планируемые результаты обучения по дисциплине (модулю)		
Содержание и код компетенции.	**Индикатор (показатель) достижения компетенции**	**Планируемые результаты обучения по дисциплине, сопряженные с индикаторами достижения компетенций**
ОПК-2. Способен использовать и адаптировать существующие математические методы и системы программирования для разработки и реализации алгоритмов решения прикладных задач	ОПК-2.1. Знание приемов написания и анализа алгоритмов и компьютерных программ; ОПК-2.2. Способность анализировать и конструировать конкретные алгоритмы на языке высокого уровня для решения разнообразных математических задач на компьютере. ОПК-2.3. Знание парадигм структурного, процедурно-модульного и объектно-ориентированного программирования на языке высокого уровня.	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;

1.1. Текущий контроль успеваемости

Текущий контроль успеваемости осуществляется путем оценки результатов выполнения заданий практических (семинарских) занятий, самостоятельной работы, предусмотренных учебным планом и посещения занятий/активность на занятиях.

В качестве оценочных средств текущего контроля успеваемости предусмотрены:

контрольная работа

Контрольная работа № 1	
Вариант 1	
1. Доказать, что $37 \mid 2^{2^{6n+2}} + 21$. 2. Доказать, что если p = 2q + 1, p,q– простые q ≡ 1 (mod 4), то <2> = $\mathbb{Z}_p^*$. 3. Доказать, что если p | (b^n – 1), (b, p) = 1, то 1) либо p | (b^d – 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 $x^2 \equiv a(\mathrm{mod}p)$ имеет решение $x \equiv \pm a^{m+1}(\mathrm{mod}p)$.	
Контрольная работа № 2	
Вариант 1	
1. Выписать характеристическое уравнение и цикловую структуру ЛРП, заданной характеристическим уравнением $f(x) = x^8 + x^6 + x^2 + x + 1$. 2. Доказать, что РП, заданная рекуррентным уравнением: $x_i = x_{i-3} \oplus x_{i-5} \oplus \overline{x_{i-1}x_{i-2}x_{i-3}x_{i-4}}$, i = 6, … имеет период T = 32 3. Найти все значения параметров a, b, спри которых многочлен $f(x) = x^{27} + ax^{17} + bx + c$ биективен по модулю 3^n.	
Контрольная работа № 3	
Вариант 1	
1. Подсчитать число всех силовских подгрупп группы S_5. 2. Определить строение группы $\mathbb{Z}_{189}^*$. 3. Пусть |G| = p^2q, 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 $x \equiv b(-1)^{a-1}\left(\frac{p-1}{a-1}\right) (\mathrm{mod}\ p)$решение сравнения $ax \equiv b \ (\mathrm{mod}\ p)$.

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> = $\mathbb{Z}_p^*$.

7. Убедившись, что f(x) = x4 + x + 2 - примитивный над GF(3), выписать все подполя поля GF(81) = $\mathbb{Z}_3[\theta]$ / θ4 + θ + 2.

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

9. Найти все силовы 2-группы группы S_6.

1.2. Промежуточная аттестация

Промежуточная аттестация осуществляется в форме экзамена
В качестве средств, используемых на промежуточной аттестации предусматривается:
Билеты

1.3. Типовые задания 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.

Пример экзаменационного билета

1. Квадратичные вычеты. Символы Лежандра и Якоби. Алгоритм решения квадратичных сравнений в кольце вычетов.
2. Линейный конгруэнтный метод построения псевдослучайных последовательностей. Биективные и транзитивные многочлены над кольцом вычетов. Критерий транзитивности многочлена по примарному модулю.

2. КРИТЕРИИ ОЦЕНКИ ПО ДИСЦИПЛИНЕ

ШКАЛА И КРИТЕРИИ ОЦЕНИВАНИЯ результатов обучения (РО) по дисциплине				
Оценка виды оценочных средств	**2 (не зачтено)**	**3 (зачтено)**	**4 (зачтено)**	**5 (зачтено)**
Знания **(виды оценочных средств: приведены в п. 1.2.)**	Отсутствие знаний	Фрагментарные знания	Общие, но не структурированные знания	Сформированные систематические знания
Умения **(виды оценочных средств: приведены в п. 1.2.)**	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)** **(виды оценочных средств: приведены в п. 1.2..)**	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