Министерство науки и высшего образования Российской Федерации
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ (НИ ТГУ)

Институт прикладной математики и компьютерных наук

УТВЕРЖДЕНО:
Директор
А. В. Замятин

Оценочные материалы по дисциплине

Теоретико-числовые методы в криптографии

по направлению подготовки / специальности

10.05.01 Компьютерная безопасность

Направленность (профиль) подготовки/ специализация:
Анализ безопасности компьютерных систем

Форма обучения
Очная

Квалификация
Специалист по защите информации

Год приема
2025

СОГЛАСОВАНО:
Руководитель ОП
В.Н. Тренькаев

Председатель УМК
С.П. Сущенко

Томск – 2025

1. Компетенции и индикаторы их достижения, проверяемые данными оценочными материалами

Целью освоения дисциплины является формирование следующих компетенций:

ОПК-10 Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности.

ОПК-3 Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности.

ПК-2 Способен разрабатывать требования к программно-аппаратным средствам защиты информации компьютерных систем и сетей.

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

ИОПК-10.1 Осуществляет анализ тенденций развития методов и средств криптографической защиты информации

ИОПК-3.2 Осуществляет применение основных понятий, фактов, концепций, принципов математики и информатики для решения задач профессиональной деятельности

ИОПК-3.3 Выявляет научную сущность проблем, возникающих в ходе профессиональной деятельности, и применяет соответствующий математический аппарат для их формализации, анализа и выработки решения

ИПК-2.2 Разрабатывает математические модели, реализуемые в средствах защиты информации

2. Оценочные материалы текущего контроля и критерии оценивания

Элементы текущего контроля:
– лабораторные работы;
– контрольные работы;

Лабораторные работы (ИОПК-3.2, ИОПК-3.3, ИПК-2.2)

1. Алгоритмы возведения в степень
2. Методы приведения по модулю
3. Быстрые алгоритмы умножения чисел
4. Тесты на простоту: Ферма, Соловея — Штрассена, Миллера — Рабина
5. Методы генерации простых, надёжных простых и сильных простых чисел
6. Методы факторизации: пробных делений, Олвея, Ферма, Полларда.
7. Методы дискретного логарифмирования: Гельфонда, Полларда.
8. Проверка полиномов на неприводимость
9. Проверка полиномов на примитивность

Контрольные работы (ИОПК-3.2, ИОПК-3.3, ИПК-2.2)

Контрольная работа состоит из 1 – 2 практических задач. Алгоритмы, выносимые на контрольные работы:

1. Методы умножения Карацубы и Тоома – Кука
2. Дискретное преобразование Фурье
3. Факторизация методом случайных квадратов: метод Диксона, метод квадратичного решета, метод цепных дробей.
4. Дискретное логарифмирование: методы Полига – Хеллмана, Адлемана
5. Факторизация многочленов методом Берлекэмпа

Контрольная работа 1

1. Методом Карацубы умножить числа 125 и 356
2. Методом Тоома – Кука умножить числа 123 и 112.

Контрольная работа 2

1. Методом Шёнхаге – Штрассена умножить числа 123 и 112.

Контрольная работа 3

1. Найти делитель числа n = 1969, используя метод Диксона (метод квадратичного решета, метод цепных дробей).

Контрольная работа 4

1. Пусть $G = \mathbb{Z}^*_{73} = < g >$, где $g = 5$. С помощью алгоритма Адлемана (Полига – Хеллмана) найти $\log_g 36$.
2. Факторизовать многочлен $f(x) = x^5 + 4x^4 + x + 4 \in \mathbb{Z}_5[x]$.

Критерии оценивания.

Результаты лабораторных работ оцениваются «отлично», «хорошо» или «удовлетворительно».

Оценка «отлично» выставляется, если программа выдает верный ответ, студент выбрал оптимальный алгоритм решения, проверил корректность входных данных, код программы оптимален.

Оценка «хорошо» выставляется, если программа выдает верный ответ, студент выбрал оптимальный алгоритм решения, но не проверил корректность входных данных или код программы не оптимален.

Оценка «удовлетворительно» выставляется, если программа выдает верный ответ, но студент выбрал не оптимальный алгоритм решения, не проверил корректность входных данных.

Для каждого задания устанавливается срок выполнения. Задания, сданные позже установленного срока без уважительной причины, оцениваются на балл ниже реальной оценки.

Результаты контрольной работы оцениваются «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Оценка «отлично» выставляется, если при реализации алгоритма не допущено никаких ошибок и получен правильный ответ.

Оценка «хорошо» выставляется, если реализация алгоритма не оптимальна, но итоговый результат верен.

Оценка «удовлетворительно» выставляется, если при реализации алгоритма допущены арифметические ошибки, не влияющие на его дальнейшую реализацию. В результате допущенной ошибки верный результат не получен, но его искажение – незначительное.

Оценка «неудовлетворительно» выставляется, если при реализации алгоритма допущены серьезные ошибки, влияющие на дальнейшую реализацию алгоритма и приведшие к тому, что ответ существенно отличается от верного или вообще не получен.

3. Оценочные материалы итогового контроля (промежуточной аттестации) и критерии оценивания

Экзаменационный билет состоит из двух частей.

Первая часть представляет собой два теоретических вопроса. Ответы на вопросы даются в развернутой форме и проверяют ИОПК-10.1.

Вторая часть представляет собой практическое задание и проверяет ИОПК-3.2, ИОПК-3.3 и ИПК-2.2. Ответ предполагает выбор алгоритма для решения задачи, получение решения и интерпретацию полученного результата.

Продолжительность экзамена 1,5 часа.

а) Примерный перечень теоретических вопросов к экзамену.

6 семестр

1. Дихотомический алгоритм возведения в степень
2. Алгоритм Барретта приведения чисел по модулю (с обоснованием)
3. Приведение по модулю специального вида
4. Преобразование Монтгомери
5. Произведение Монтгомери
6. Возведение в степень методом Монтгомери
7. Вычисление наибольшего общего делителя: бинарный алгоритм
8. Теорема о вычислении целой части квадратного корня
9. Быстрое умножение: метод Карацубы
10. Быстрое умножение: метод Тоома - Кука
11. Примитивные корни из 1, их свойства.
12. Теорема о матрице Вандермонда, её следствия
13. Теорема о примитивных корнях из 1
14. Дискретное преобразование Фурье: определение, содержательный смысл. Доказать обратимость ДПФ
15. Свертка. Теорема о свертке
16. Быстрое вычисление ДПФ: ключевые идеи
17. Алгоритм быстрого преобразования Фурье (с примером)
18. Определение чисел Кармайкла. Теорема Кармайкла
19. Определение и свойства оснований Ферма
20. Теорема о бесконечном количестве псевдопростых по любому основанию
21. Теорема о достаточности критерия Эйлера
22. Определение и свойства оснований Эйлера
23. Тест Соловея - Штрассена (с примером)
24. Теорема Селфриджа (о сильно псевдопростых числах)
25. Теорема Рабина
26. Тест Миллера - Рабина (с примером)
27. Пусть $n = 3 \pmod 4$. Доказать: R,, = E,,
28. Связь теста Миллера - Рабина с задачей факторизации
29. Метод Люка проверки числа на простоту (с примером)
30. Теорема Брилхарда — Лемера - Селфриджа (модификация критерия Люка)
31. Теорема Поклингтона, следствие её
32. Теорема Диемитко, следствие её
33. Процедура генерации простого числа в Российском стандарте выработки ЭЦП
34. Пусть $(a, n) = 1$. Доказать: n простое, если и только если $(x - a)^{n} = x^{n} — a \pmod n$
35. Полиномиальный детерминированный тест на простоту (AKS-тест)

7 семестр

1. Факторизация числа: постановка задачи.
2. Метод пробных делений: идея метода; оценка сложности; обосновать заключение, что если $n = d_k \cdot q + r$ и $q < d_k$, то n – простое число.
3. Метод Олвея: идея метода; оценка разностей $\Delta q_{k+1} - \Delta q_k$ и $\Delta r_{k+1} - \Delta r_k$, следствия этих оценок. Продемонстрировать метод на конкретном примере.
4. Метод Ферма: идея метода; продемонстрировать метод на конкретном примере.
5. ρ-метод Полларда: идея метода; продемонстрировать метод на конкретном примере.

6. $p-1$-метод Полларда: идея метода; продемонстрировать метод на конкретном примере.
7. Методы случайных квадратов: идея метода; поиск случайных квадратов
   а) методом Диксона;
   б) методом квадратичного решета;
   в) методом цепных дробей. Получить оценку для $\left|P_i^2 - x^2 Q_i^2\right|$ и ее следствие.

   Продемонстрировать каждый метод на конкретном примере.
8. Дискретное логарифмирование: постановка задачи.
9. Алгоритм Гельфонда: идея, обоснование, продемонстрировать на конкретном примере.
10. ρ-метод Полларда: идея метода, продемонстрировать на конкретном примере.
11. Алгоритм Адлемана: идея метода, когда лучше всего работает, рекомендации по выбору факторной базы; продемонстрировать на конкретном примере.
12. Алгоритм Полига – Хелмана: идея метода, продемонстрировать на конкретном примере.
13. Логарифмирование в подгруппах простого порядка: модификация алгоритма Адлемана; продемонстрировать на конкретном примере.
14. Алгоритм нахождения наибольшего общего делителя: определение НОД, алгоритм Евклида, продемонстрировать на конкретном примере.
15. Неприводимость полиномов: определение неприводимого полинома; критерий 1 неприводимости многочленов и его обоснование; критерий 1 неприводимости многочленов и его обоснование. Продемонстрировать каждый критерий на конкретном примере.
16. Примитивность многочленов: определение примитивного многочлена, тест на примитивность многочлена и его обоснование. Продемонстрировать тест на конкретном примере.
17. Освобождение полинома от квадратов: определение полинома, свободного от квадратов, задача освобождения полинома от квадратов, обоснование алгоритма освобождения полинома от квадратов (без доказательств), продемонстрировать алгоритм на конкретном примере.
18. Алгоритм Берликэмпа: обоснование алгоритма (без доказательств), продемонстрировать на конкретном примере.

б) Примеры задач.

В экзаменационный билет включаются задачи того же типа, что и в контрольные работы.

в) Критерии оценивания.

Результаты экзамена определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Оценка «отлично» выставляется, если:

а) студент дал полный и развернутый ответ на теоретические вопросы;

б) решение практического задания верное.

Оценка «хорошо» выставляется, если:

а) ответ студента на теоретические вопросы в целом полный, но имеются незначительные замечания;

б) решение практического задания верное или содержит арифметические ошибки, не влияющие на используемый алгоритм

Оценка «удовлетворительно» выставляется, если:

а) ответ студента на теоретические вопросы не полный;

б) решение практического задания содержит ошибки, существенно повлиявшие на результат.

Оценка «неудовлетворительно» выставляется, если:

а) ответ студента на теоретические вопросы не полный и содержит серьезные ошибки;

б) решение практического задания не доведено до конца или для его решения выбран неверный алгоритм.

Если в течение семестра студент посетил не менее 75% занятий и выполнил все контрольные и лабораторные работы на положительную оценку, то он освобождается от выполнения практической части билета.

4. Оценочные материалы для проверки остаточных знаний (сформированности компетенций)

Теоретические вопросы (ИОПК-10.1)

1. Дихотомический алгоритм возведения в степень.
2. Алгоритм Барретта приведения чисел по модулю
3. Вычисление наибольшего общего делителя (алгоритм Евклида, бинарный алгоритм)
4. Методы быстрого умножения
5. Проверка простых чисел на простоту: простейшие тесты на простоту
6. Задача факторизации числа. Простейшие методы факторизации чисел
7. Дискретное логарифмирование. Простейшие методы дискретного логарифмирования.
8. Проверка многочленов на неприводимость.

Задачи (ИОПК-3.2, ИОПК-3.3, ИПК-2.2)

1. Методом Карацубы умножить числа 125 и 356.
2. Разложить на множители число n = 1969.
3. Пусть $G = \mathbb{Z}^*_{73} = < g >$, где $g = 5$. Найти $\log_g 36$.
4. Найти НОД($f(x)$, $g(x)$) если $f(x) = x^5 + 4x^4 + x + 4$, $g(x) = x^3 + 4x^2 + 2 \in \mathbb{Z}_5[x]$
5. Проверить на неприводимость многочлен $f(x) = x^5 + 4x^4 + x + 4 \in \mathbb{Z}_5[x]$.

Информация о разработчиках

Пахомова Елена Григорьевна, канд. физ.-мат. наук, доцент, кафедра компьютерной безопасности, доцент.

Останин Сергей Александрович, канд. техн. наук, доцент, кафедра компьютерной безопасности, доцент.