МИНОБРНАУКИ РОССИИ
Ярославский государственный университет им. П.Г. Демидова

Кафедра компьютерной безопасности и математических методов обработки информации

УТВЕРЖДАЮ
Декан математического факультета

Нестеров П.Н.
20 июня 2023 г.

Рабочая программа дисциплины

Криптографические алгоритмы

Направление подготовки (специальности)
10.05.01 Компьютерная безопасность

Направленность (профиль)
«Математические методы защиты информации»

Форма обучения очная

Программа рассмотрена
на заседании кафедры
от 14 апреля 2023 г., протокол № 8

Программа одобрена НМК
математического факультета
протокол № 9 от 3 мая 2023 г.

Ярославль

1. Цели освоения дисциплины

Целью изучения дисциплины «Криптографические алгоритмы» является освоение обучающимися передовых знаний в области теоретической криптографии, а именно вопросов, связанных с возможностью развития классической криптографии после создания квантового компьютера (постквантовой криптографии).

Дисциплина обеспечивает приобретение знаний и умений в области использования криптографических алгоритмов для решения задач защиты информации, способствует освоению принципов корректного применения современных криптографических средств и методов защиты информации.

Задачами освоения дисциплины «Криптографические алгоритмы» являются:

- приобретение навыков анализа сложности и безопасности алгоритмов теории решеток;
- овладение методами теории решеток для решения задач в области современной криптографии.

2. Место дисциплины в структуре образовательной программы

Данная дисциплина относится к обязательной части образовательной программы.

Для освоения данной дисциплины обучающиеся должны владеть математическим аппаратом алгебры, линейной алгебры, теории алгоритмов, знать основные криптографические понятия и методы, основные алгебраические структуры (векторные пространства, кольца многочленов) и их свойства, методы представления алгебраических структур с помощью структур данных, уметь осуществлять программную реализацию известных алгоритмов.

Для успешного освоения дисциплины «Криптографические алгоритмы» ей должны предшествовать следующие дисциплины:

«Алгебра»;
«Линейная алгебра»;
«Теория алгоритмов»;
«Методы программирования»;
«Алгебраическая алгоритмика»;
«Методы и средства криптографической защиты информации».

Полученные в курсе «Криптографические алгоритмы» знания необходимы для изучения дисциплин «Математические методы защиты банковской информации» и «Информационная безопасность электронного бизнеса».

3. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы

Процесс изучения дисциплины направлен на формирование следующих компетенций в соответствии с ФГОС ВО, ООП ВО и приобретения следующих знаний, умений, навыков и (или) опыта деятельности:

Формируемая компетенция (код и формулировка)	Индикатор достижения компетенции (код и формулировка)	Перечень планируемых результатов обучения
Общепрофессиональные компетенции		
ОПК-3. Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности	И-ОПК-3.5. Знает необходимые математические методы для решения задач обеспечения защиты информации.	Знать: - современные математические методы построения криптографических алгоритмов, основанных на теории решеток.
	И-ОПК-3.6. Умеет: применять совокупность необходимых математических методов для решения задач обеспечения защиты информации.	Уметь: - анализировать сложность и безопасность криптографических алгоритмов, основанных на теории решеток.
ОПК-10. Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности	И-ОПК-10.5. Знать современные криптографические алгоритмы на основе теории решеток.	Знать: - алгоритмы построения приведенных базисов решетки; - алгоритмы Бабаи, Хастада, Кооперсмита; - криптосистему NTRU; - криптосистему LWE.
	И-ОПК-10.6. Владеет навыками реализации алгоритмов, в том числе криптографических, в современных программных комплексах.	Владеть навыками: - разработки криптографических алгоритмов на основе теории решеток, с использованием среды Microsoft Visual Studio с применением технологии OpenMP.
ОПК-2.1 Способен разрабатывать алгоритмы, реализующие современные математические методы защиты информации	ОПК-2.1_4 знает способы эффективной реализации алгоритмов.	Знает: - способы эффективной реализации примитивов теории решеток.
	И-ОПК-2.1_2 Способен разрабатывать алгоритмы, используемые в современных математических методах защиты информации	Владеть навыками: - выбора и разработки криптографических алгоритмов на основе теории решеток, с использованием среды Microsoft Visual Studio с применением технологии OpenMP.

4. Объем, структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 6 зачетных единиц, 216 акад. часов.

№ п/п	Темы (разделы) дисциплины, их содержание	Семестр	Виды учебных занятий, включая самостоятельную работу студентов, и их трудоемкость (в академических часах)						Формы текущего контроля успеваемости Форма промежуточной аттестации (по семестрам)
			Контактная работа						
			лекции	практические	лабораторные	консультации	аттестационные испытания	самостоятельная работа	
1	Принципы анализа сложности алгоритмов	9	4					4	Задания для самостоятельной работы
2	NP-полнота некоторых задач	9	4			1		8	Задания для самостоятельной работы
3	Решетки в евклидовом пространстве	9	6	2		1		8	Задания для самостоятельной работы
4	Редуцированный по Минковскому базис решетки. Теорема Минковского о выпуклом теле	9	6	2	2	1		8	Задания для самостоятельной работы
5	LLL-приведенные базисы решеток и их приложения	9	6	2	2	1		8	Задания для самостоятельной работы
6	Атаки на криптографические системы с использованием LLL-приведенных базисов решеток	9	6	2	4	1		8	Задания для самостоятельной работы
							0,3	10,7	Зачет
	Всего за 9 семестр 108 часов		**32**	**8**	**8**	**5**	**0,3**	**54,7**	
7	Постквантовая криптография на основе теории решеток	A	10						

8	Принципы построения параллельных алгоритмов	А	6	2	2			2	Задания для самостоятельной работы
9	Технология параллельного программирования OpenMP	А	8	6	6	2		2	Задания для самостоятельной работы
10	Некоторые методы статистического криптоанализа	А	6	7	7	2		2	Задания для самостоятельной работы
						2	0,5	33,5	Экзамен
	Всего за 10 семестр 108 часов		**30**	**15**	**15**	**6**	**0,5**	**39,5**	
	ИТОГО		**62**	**23**	**23**	**11**	**0,8**	**94,2**	

Содержание дисциплины «Криптографические алгоритмы»:

Тема 1. Принципы анализа сложности алгоритмов.

Сложность алгоритмов и ее практическое значение. Подходы к оценкам сложности алгоритмов и вычислений. Модели вычислений. Меры сложности. Свойства функций сложности. Сложность в среднем и сложность в худшем случае, их значение для криптографии. Полиномиальная иерархия.

Тема 2. NP-полнота некоторых задач.

NP-полнота задач о выполнимости булевой формулы, КНФ-выполнимости, 3-выполнимости. Сведение задачи 3-выполнимости к задаче о рюкзаке.

Тема 3. Решетки в евклидовом пространстве.

Понятие решетки в *n*-мерном евклидовом пространстве, базисы решеток и их свойства, целочисленные решетки и матрицы. Связь теории решеток с теорией упаковки шаров в пространстве.

Тема 4. Редуцированный по Минковскому базис решетки. Теорема Минковского о выпуклом теле.

Редуцированный по Минковскому базис решетки и его основные свойства, редукция решеток размерности 2 и 3. Последовательные минимумы. Теорема Эрмита. Теорема Минковского о выпуклом теле.

Тема 5. LLL-приведенные базисы решеток и их приложения.

LLL-приведенные базисы решеток и их свойства. Алгоритм построения LLL-приведенных базисов, оценка его сложности. Приложения LLL-приведенных базисов решеток.

Тема 6. Атаки на криптографические системы с использованием LLL-приведенных базисов решеток.

Атака Хастада на криптосистему RSA. Атака Лагариаса-Одлыжко на ранцевые криптосистемы.

Тема 7. Постквантовая криптография на основе теории решеток.

Сложность квантовых вычислений. Значение создания квантового компьютера для современной криптографии. Вычислительно сложные задачи для квантового компьютера, их применение в криптографии. Протоколы квантового распределения ключей. Примеры вычислительно сложных задач на решетках. Криптосистема NTRU. Теорема Аджтая.

Тема 8. Принципы построения параллельных алгоритмов.

Параллельные и распределенные вычисления. Развитие параллелизма в компьютерах. Концепция неограниченного параллелизма. Граф алгоритма. Параллельная форма алгоритма. Модели данных. Особенности разработки, компиляции и анализа параллельного кода. Отладка параллельных приложений. Сетевой закон Амдала.

Тема 9. Технология параллельного программирования OpenMP.

Технология OpenMP – назначение, методы программирования: организация параллелизма, распределение (балансировка) вычислительной нагрузки, синхронизация. Директивы, функции и переменные среды.

Тема 10. Некоторые методы статистического криптоанализа.

Конечные разности. Дифференциальный криптоанализ. Анализ с помощью усеченных дифференциалов. Анализ с помощью дифференциалов высших порядков. Криптоанализ на основе списка ключей и связанных ключей. Линейный криптоанализ.

5. Образовательные технологии, в том числе технологии электронного обучения и дистанционные образовательные технологии, используемые при осуществлении образовательного процесса по дисциплине

В процессе обучения используются следующие образовательные технологии:

Академическая лекция (или лекция общего курса) – последовательное изложение материала, осуществляемое преимущественно в виде монолога преподавателя. Требования к академической лекции: современный научный уровень и насыщенная информативность, убедительная аргументация, доступная и понятная речь, четкая структура и логика, наличие ярких примеров, научных доказательств, обоснований, фактов.

Проблемная лекция – изложение материала, предполагающее постановку проблемных и дискуссионных вопросов, освещение различных научных подходов, авторские комментарии, связанные с различными моделями интерпретации изучаемого материала. Проблемная лекция начинается с вопросов, с постановки проблемы, которую в ходе изложения материала необходимо решить. В лекции сочетаются проблемные и информационные начала. При этом процесс познания студентов в сотрудничестве и диалоге с преподавателем приближается к поисковой, исследовательской деятельности. Содержание проблемы раскрывается путем организации поиска ее решения или суммирования и анализа традиционных и современных точек зрения.

Лабораторная работа – организация учебной работы с реальными материальными и информационными объектами.

6. Перечень лицензионного и (или) свободно распространяемого программного обеспечения, используемого при осуществлении образовательного процесса по дисциплине

В процессе осуществления образовательного процесса используются:

для формирования материалов для текущего контроля успеваемости и проведения промежуточной аттестации, для формирования методических материалов по дисциплине:

- программы Microsoft Office;
- издательская система LaTex;
- Adobe Acrobat Reader;

при проведении практических занятий используется программное обеспечение

- OpenMP;
- Microsoft Visual Studio.

7. Перечень современных профессиональных баз данных и информационных справочных систем, используемых при осуществлении образовательного процесса по дисциплине (при необходимости)

Для поиска учебной литературы библиотеки ЯрГУ используется автоматизированная библиотечно-информационная система «БУКИ-NEXT» http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php.

8. Перечень основной и дополнительной учебной литературы, ресурсов информационно-телекоммуникационной сети «Интернет» (при необходимости), рекомендуемых для освоения дисциплины

а) основная литература

1. *Мурин Д. М.* Элементы теории сложности вычислений и теории решеток : учебное пособие / Д.М.Мурин ; Яросл. гос. ун-т им. П.Г. Демидова. — Ярославль : ИНДИГО, 2020. – 112 с.

б) дополнительная литература

1. *Глухов М.М.* Введение в теоретико-числовые методы криптографии : учеб. пособие для вузов / М.М. Глухов, И.А. Круглов, А.Б. Пичкур, А.В. Черемушкин, СПб., Лань, 2011, 394 с.

2. *Василенко, О.Н.* Теоретико-числовые алгоритмы в криптографии / О.Н. Василенко – М.: МЦНМО, 2006. – 336 с.

3. *Кормен, Т.* Алгоритмы: построение и анализ / Т. Кормен, Ч. Лейзерсон, Р. Ривест, К. Штайн. пер. с англ. И. В. Красикова, Н. А. Ореховой, В. Н. Романова. - 2-е изд. - М.: Вильямс, 2001. - 995 с.

4. *Маховенко, Е.Б.* Теоретико-числовые методы в криптографии: учеб. пособие для вузов / Е. Б. Маховенко; УМО вузов по образованию в обл. информ. безопасности. - М.: Гелиос АРВ, 2006. - 319 с.

в) ресурсы сети «Интернет» (при необходимости)

http://parallel.ru – сайт Лаборатории параллельных информационных технологий Научно-исследовательского вычислительного центра Московского государственного университета имени М.В.Ломоносова.

На страницах сайта собраны и систематизированы материалы, которые так или иначе связаны с параллельными вычислениями – бурно развивающейся областью современной науки, активно проникающей во все новые и новые стороны нашей жизни.

http://www.latticechallenge.org/ – сайт, на котором проходят соревнования по следующим направлениям: решение задач поиска кратчайшего ненулевого вектора решетки (или лучшего приближения к нему) на наборе сложных решеток различной размерности, предложенных организаторами соревнования; оценка эффективности различных типов алгоритмов поиска кратчайшего ненулевого вектора решетки (или лучшего приближения к нему) на сложных случаях случайных решеток по Гольдштейну и Майеру, получаемых при помощи предоставленного организаторами генератора решеток;

решение задач поиска кратчайшего ненулевого вектора решетки (или лучшего приближения к нему) в решетках, построенных на идеалах кругового многочлена; решение задачи LWE.

https://msdn.microsoft.com/ru-ru/library/default.aspx – библиотека официальной технической документации для разработчиков под ОС Microsoft Windows. Библиотека MSDN (Microsoft Developer Network) содержит документацию на API продуктов Microsoft, а также код примеров, технические статьи и другую полезную для разработчиков информацию.

9. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине включает в свой состав специальные помещения:

- учебные аудитории для проведения занятий лекционного типа;
- учебные аудитории для проведения лабораторных работ, оснащенные средствами вычислительной техники, с установленным программным обеспечением Microsoft Visual Studio;
- учебные аудитории для проведения групповых и индивидуальных консультаций;
- учебные аудитории для проведения текущего контроля и промежуточной аттестации;
- помещения для самостоятельной работы;
- помещения для хранения и профилактического обслуживания технических средств обучения.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде ЯрГУ.

Автор(ы):

Доцент кафедры КБиММОИ, канд. физ.-мат. наук Д.М. Мурин

Приложение № 1 к рабочей программе дисциплины
«Криптографические алгоритмы»

Фонд оценочных средств
для проведения текущего контроля успеваемости
и промежуточной аттестации студентов
по дисциплине

1. Типовые контрольные задания и иные материалы, используемые в процессе текущего контроля успеваемости

1.1 Контрольные задания и иные материалы, используемые в процессе текущей аттестации

Задания для самостоятельной работы

Возможные задания для самостоятельной работы по теме № 1 «Принципы анализа сложности алгоритмов»

1. Пусть $p_1(x)$ и $p_2(x)$ – полиномы. Покажите, что некоторый полином для каждого x принимает значение, большее $p_1(p_2(x))$.
2. Упростите функцию $O(1000\, n^3 + n \log n + (\log n)^{100})$, где n – параметр.
3. Упростите функцию $O(\sum_{k=1}^{t} k! n^k)$, где n – параметр.
4. Упростите функцию $O(1+3+5+...+(2n-1))$, где n – параметр.
5. Упростите функцию $O(1+2+3+...+n)$, где n – параметр.
6. Упростите функцию $O(1^2 + 2^2 + 3^2 + ... + n^2)$, где n – параметр.
7. Упростите функцию $O(\frac{1}{n}\log n + (\log n)^2 + 1)$, где n – параметр.
8. Докажите, что O(const) = O(1).
9. Оцените битовую сложность операций сложения, вычитания, умножения и деления столбиком.
10. Справедливы ли соотношения $2^{n+1} = O(2^n)$ и $2^{2n} = O(2^n)$?
11. Докажите, что множества $o(g(n))$ и $w(g(n))$ не пересекаются.

Возможные задания для самостоятельной работы по теме № 2 «NP-полнота некоторых задач»

1. Покажите, что класс P, который рассматривается как множество языков, замкнут относительно операций объединения, пересечения, конкатенации, дополнения и замыкания Клини.
2. Покажите, что класс языков NP замкнут относительно операций объединения, пересечения, конкатенации, замыкания Клини. Что можно сказать о замкнутости класса NP относительно дополнения?
3. Докажите, что задача о раскраске остается NP-полной, даже если ограничить k числом 3, а наибольшую степень каждой вершины – числом 4.
4. Докажите NP-полноту задачи о клике, непосредственно представляя вычисления НМТ вместо того, чтобы трансформировать ее из 3-КНФ-выполнимости.

5. Покажите, что NP-полна задача распознавания следующего свойства: регулярное выражение без * не представляет всех цепочек некоторой фиксированной длины.
6. Покажите, что NP-полна задача распознавания следующего свойства: регулярное выражение над алфавитом {0} не представляет 0*.
7. Постройте алгоритм полиномиальной сложности для проверки 2-выполнимости.
8. Докажите, что если NP не равно co-NP, то P не равно NP.
9. Докажите, что язык L полный для класса NP тогда и только тогда, когда дополняющий язык U\L (где U – универсальный язык) полный для класса co-NP.
10. Докажите, что задача определения того, является ли тавтологией данная формула, является полной в классе co-NP.

Возможные задания для самостоятельной работы по теме № 3 «Решетки в евклидовом пространстве»

1. Провести процесс ортогонализации Грамма-Шмидта по отношению к векторам $b_1 = (1, 0, 0, 5)$, $b_2 = (0, 1, 0, 5)$, $b_3 = (0, 0, 1, 5)$.
2. На плоскости расположен квадрат площади 4. Какое наименьшее число точек с целочисленными координатами он содержит?
3. На плоскости расположен квадрат площади 4, содержащий не менее семи точек с целочисленными координатами. Докажите, что он содержит ровно девять точек с целочисленными координатами.
4. Пусть решетка построена на векторах (0, 1), $(0, \sqrt{-2})$. Для каких простых p на окружности радиуса $\sqrt{p}$ с центром в начале координат лежит не менее четырех точек решетки?
5. Пусть решетка построена на векторах (0, 1), $(0, \sqrt{-3})$. Для каких простых p на окружности радиуса $\sqrt{p}$ с центром в начале координат лежит не менее четырех точек решетки?
6. Вычислить определитель решетки, базис которой суть
   а) $b_1 = (1, 2, 3)$, $b_2 = (5, 1, 4)$, $b_3 = (3, 2, 5)$;

   б) $b_1 = (-1, 5, 4)$, $b_2 = (3, -2, 0)$, $b_3 = (-1, 3, 6)$;

   в) $b_1 = (0, 2, 2)$, $b_2 = (2, 0, 2)$, $b_3 = (2, 2, 0)$;

   г) $b_1 = (1, 2, 3)$, $b_2 = (4, 5, 6)$, $b_3 = (7, 8, 9)$.
7. Докажите неравенство Адамара.

Возможные задания для самостоятельной работы по теме № 4 «Редуцированный по Минковскому базис решетки. Теорема Минковского о выпуклом теле»

1. Построить приведенный по Минковскому базис решетки, заданный базис которой $b_1 = (2, 1)$, $b_2 = (3, 2)$.
2. Построить приведенный по Минковскому базис решетки, заданный базис которой $b_1 = (1, 0, 1, 2)$, $b_2 = (1, -1, 2, 0)$, $b_3 = (-1, 2, 0, 1)$.
3. Выполнить лабораторную работу по соответствующей теме.

Возможные задания для самостоятельной работы по теме № 5 «LLL-приведенные базисы решеток и их приложения»

1. Построить LLL-приведенный базис решетки, заданный базис которой $b_1 = (2, 1)$, $b_2 = (3, 2)$.
2. Построить LLL-приведенный базис решетки, заданный базис которой $b_1 = (1, 0, 1, 2)$, $b_2 = (1, -1, 2, 0)$, $b_3 = (-1, 2, 0, 1)$.
3. Выполнить лабораторную работу по соответствующей теме.

Возможные задания для самостоятельной работы по теме № 6 «Атаки на криптографические системы с использованием LLL-приведенных базисов решеток»

1. Решить задачу об укладке ранца:
   а) {17, 24, 11, 12, 3, 21, 15, 18, 1, 5}, S = 100;

   б) {21, 12, 13, 14, 15, 18, 23, 1, 2, 3}, S = 70;

   в) {1, 2, 3, 4, 25, 35, 45, 50, 60, 70}, S = 200.

2. Выполнить лабораторные работы по соответствующей теме.

Возможные задания для самостоятельной работы по теме № 8 «Принципы построения параллельных алгоритмов»

1. Рассмотрите способы обеспечения когерентности кэшей в системах с общей разделяемой памятью.
2. Подготовьте обзор программных библиотек, обеспечивающих выполнение операций передачи данных для систем с распределенной памятью.

Задания для самостоятельной работы по теме № 9 «Технология параллельного программирования OpenMP»

1. Реализовать последовательный алгоритм Гаусса решения систем линейных уравнений, разработать параллельный алгоритм и реализовать его, провести вычислительные эксперименты.
2. Выполнить лабораторные работы по соответствующей теме.

Возможные задания для самостоятельной работы по теме № 10 «Некоторые методы статистического криптоанализа»

1. Проанализируйте S-блоки шифра TwoFly. Вероятность линейного приближения какого из S-блоков имеет наибольшее отклонение от 1/2? Определите лучшее приближение для каждого из S-блоков.
2. Используя приближения S-блоков, найденные в предыдущей задаче, найдите линейные приближения шифра TwoFly. С какой вероятностью они будут выполняться? Какое приближение будет наилучшим, т. е. выполняться с наибольшей вероятностью?
3. Сколько пар «открытый текст – шифротекст» достаточно для того, чтобы с вероятностью близкой к единице (например, 0,977) утверждать, что лучшее линейное приближение шифра TwoFly дает верную информацию о ключе? Выразите биты ключа, насколько это возможно, через биты открытого текста.
4. Постройте таблицы дифференциалов для S-блоков шифра TwoFly. Какой из S-блоков допускает дифференциал с наибольшей вероятностью? Определите лучший дифференциал для каждого из S-блоков.

5. Используя дифференциалы S-блоков, полученные в предыдущей задаче, найдите дифференциалы шифра TwoFly. С какой вероятностью шифр допускает эти дифференциалы? Какой дифференциал будет наилучшим, т. е. допускаться с наибольшей вероятностью?
6. Сколько пар «открытый текст – шифротекст» достаточно для того, чтобы с вероятностью близкой к единице (например, 0,977) утверждать, что лучший дифференциал шифра TwoFly дает верную информацию о ключе? Выразите биты ключа, насколько это возможно, через биты открытого текста.
7. Проведите линейный криптоанализ шифра S-AES. Рассмотрите два случая: когда раундовые ключи одинаковые и когда они разные. Оцените необходимый объем выборки для надежной работы метода.
8. Проведите дифференциальный криптоанализ шифра S-AES. Рассмотрите два случая: когда раундовые ключи одинаковые и когда они разные. Оцените необходимый объем выборки для работы алгоритма с надежностью 0,8; 0,95; 0,99.
9. Докажите лемму Мацуи: Пусть X_i, где $1 \le i \le n$, – независимые случайные величины, принимающие значения из Z_2. Пусть $P\{X_i = 0\} = 1/2 + \varepsilon_i$, где $0 \le \varepsilon_i \le 1/2$. Тогда случайная величина $X_1 \oplus X_2 \oplus \ldots \oplus X_n$ принимает значение 0 с вероятностью $1/2 + \varepsilon$, $\varepsilon = 2^{n-1} \prod_{i=1}^{n} \varepsilon_i$.
10. Выполнить лабораторные работы по соответствующей теме.

Задания лабораторных работ

Лабораторная работа по теме № 4 «Редуцированный по Минковскому базис решетки. Теорема Минковского о выпуклом теле»

Реализовать программу, реализующую алгоритм приведения базиса решетки.

Лабораторная работа по теме № 5 «LLL-приведенные базисы решеток и их приложения»

Реализовать программу, реализующую LLL-алгоритм приведения базиса решетки. Реализовать программу, генерирующую базисы решеток различных размерностей.

Лабораторные работы по теме № 6 «Атаки на криптографические системы с использованием LLL-приведенных базисов решеток»

Лабораторная работа № 1.

Реализовать алгоритм решения задачи о рюкзаке на базе LLL-алгоритма. Проанализировать, при каких входных данных алгоритм с наибольшей вероятностью успешно завершается.

Лабораторная работа № 2.

Реализовать алгоритм, реализующий атаку Хастада на RSA. Проанализировать, при каких параметрах криптосистемы RSA атака является эффективной.

Лабораторные работы по теме № 9 «Технология параллельного программирования OpenMP»

Лабораторная работа № 1.

Параллельные методы умножения матрицы на вектор (реализация последовательного алгоритма, разработка параллельного алгоритма, реализация параллельного алгоритма, проведение вычислительных экспериментов).

Лабораторная работа № 2.

Параллельные методы умножения матриц (реализация последовательного алгоритма, разработка параллельного алгоритма, реализация параллельного алгоритма, проведение вычислительных экспериментов).

Возможные лабораторные работы по теме № 10 «Некоторые методы статистического криптоанализа»

Лабораторная работа № 1.

Реализовать метод дифференциального криптоанализа с использованием технологии OpenMP в среде разработки Microsoft Visual Studio (для произвольного блочного алгоритма шифрования).

Лабораторная работа № 2.

Реализовать метод криптоанализа с помощью усеченных дифференциалов с использованием технологии OpenMP в среде разработки Microsoft Visual Studio (для произвольного блочного алгоритма шифрования).

Лабораторная работа № 3.

Реализовать метод криптоанализа с помощью дифференциалов высших порядков с использованием технологии OpenMP в среде разработки Microsoft Visual Studio (для произвольного блочного алгоритма шифрования).

Лабораторная работа № 4.

Реализовать метод линейного криптоанализа с использованием технологии OpenMP в среде разработки Microsoft Visual Studio (для произвольного блочного алгоритма шифрования).

2. Список вопросов и (или) заданий для проведения промежуточной аттестации

Список вопросов к экзамену:

1. Связь между задачей, языком и машинами Тьюринга. Виды машин Тьюринга. Виды задач: задача оптимизации, задача вычисления, задача распознавания, связи между видами задач.
2. Доказательство NP-полноты задачи выполнимости булевой формулы.

3. Доказательство NP-полноты задачи выполнимости булевой формулы, находящейся в КНФ (NP-полнота задачи выполнимости булевой формулы полагается известной).
4. Доказательство NP-полноты задачи 3-выполнимости (NP-полнота задачи выполнимости булевой формулы полагается известной).
5. Доказательство NP-полноты задачи о рюкзаке.
6. Процесс ортогонализации Грамма-Шмидта. Оценка сложности.
7. Основные сведения о решетках. Определитель решетки, его инвариантность относительно выбора базиса.
8. Теорема о дополнении вектора $x = (x_1, \ldots, x_n)$ из Z^n до базиса целочисленной решетки Z^n.
9. Приведенные по Минковскому базисы решетки и их свойства.
10. Редукция решеток размерности 2. Алгоритм Гаусса, оценка его сложности.
11. Последовательные минимумы решеток и их свойства. Теорема Эрмита.
12. Теорема Минковского о выпуклом теле.
13. LLL-приведенные базисы решетки. Определение, основные свойства (без теорем о длинах векторов LLL-приведенного базиса по сравнению с другими ненулевыми векторами решетки).
14. LLL-приведенные базисы решетки. Определение, теоремы о длинах векторов LLL-приведенного базиса по сравнению с другими ненулевыми векторами решетки.
15. Оценка числа точек целочисленной решетки, попадающих в сферу радиуса R с центром в начале координат в n-мерном пространстве. Случай большого радиуса.
16. Оценка числа точек целочисленной решетки, попадающих в сферу радиуса R с центром в начале координат в n-мерном пространстве. Случай малого радиуса.
17. Атака Винера на криптосистему RSA.
18. Атака Хастада на криптосистему RSA.
19. Криптосистема Меркля-Хеллмана.
20. Оценка числа сверхрастущих и инъективных векторов.
21. Метод Лагариаса-Одлыжко решения задачи о рюкзаке. Случай расположения центра сферы в точке начала координат.
22. Метод Лагариаса-Одлыжко решения задачи о рюкзаке. Случай расположения центра сферы в точке (1/2, …, 1/2).
23. Вычислительно сложные задачи для квантового компьютера, их применение в криптографии. Примеры вычислительно сложных задач на решетках.
24. Протоколы квантового распределения ключей.
25. Криптосистема NTRU.
26. Концепция неограниченного параллелизма. Граф алгоритма.
27. Параллельная форма алгоритма. Модели данных.
28. Сетевой закон Амдала.
29. Технология OpenMP. Параллельные и последовательные области – переменные среды и вспомогательные функции.
30. Технология OpenMP. Параллельные и последовательные области – директива parallel, директива single, директива master.
31. Технология OpenMP. Модель данных.
32. Технология OpenMP. Распределение работы – низкоуровневое распараллеливание, параллельные циклы.
33. Технология OpenMP. Распределение работы – параллельные секции, директива workshare, задача (task).
34. Технология OpenMP. Синхронизация – барьер, директива ordered, критические секции, директива atomic.
35. Технология OpenMP. Синхронизация – замки, директива flush.
36. Дифференциальный криптоанализ.
37. Анализ с помощью усеченных дифференциалов.

38. Анализ с помощью дифференциалов высших порядков.
39. Криптоанализ на основе списка ключей и связанных ключей.
40. Линейный криптоанализ.

Правила выставления оценки на зачете.

В процессе зачета требуется ответить на один из приведенных выше вопросов. На подготовку к ответу дается не менее 1 академического часа.

По итогам зачета выставляется одна из оценок: «зачтено», «не зачтено».

Оценка «Зачтено» выставляется студенту, который демонстрирует владение содержанием материала и понятийным аппаратом теории решеток; умеет связывать теорию с практикой. В ответе могут допускаться отдельные неточности (несущественные ошибки), которые исправляются самим студентом после дополнительных и (или) уточняющих вопросов экзаменатора. На часть дополнительных вопросов студент может не дать ответ или дать неверный ответ.

Оценка «Не зачтено» выставляется студенту, который демонстрирует разрозненные, бессистемные знания; беспорядочно и неуверенно излагает материал; не умеет выделять главное и второстепенное, не умеет соединять теоретические положения с практикой; допускает грубые ошибки при определении понятий, вследствие непонимания их существенных и несущественных признаков и связей; дает неполные ответы, логика и последовательность изложения которых имеют существенные и принципиальные нарушения, в ответах отсутствуют выводы. Дополнительные и уточняющие вопросы экзаменатора не приводят к коррекции ответов студента. На основную часть дополнительных вопросов студент затрудняется дать ответ или дает неверные ответы.

Оценка «Не зачтено» выставляется также студенту, который взял экзаменационный билет, но отказалсядать на него ответ.

Правила выставления оценки на экзамене.

В экзаменационный билет включаются два теоретических вопроса. На подготовку к ответу дается не менее 1 академического часа.

По итогам экзамена выставляется одна из оценок: «отлично», «хорошо», «удовлетворительно» или «неудовлетворительно».

Оценка «Отлично» выставляется студенту, который демонстрирует глубокое и полное владение содержанием материала и понятийным аппаратом теории решеток; умеет связывать теорию с практикой. Студент дает развернутые, полные и четкие ответы на вопросы экзаменационного билета и дополнительные вопросы, соблюдает логическую последовательность при изложении материала. Грамотно использует терминологию.

Оценка «Хорошо» выставляется студенту, ответ которого на экзамене в целом соответствуют указанным выше критериям, но отличается меньшей обстоятельностью,

глубиной, обоснованностью и полнотой. В ответе имеют место отдельные неточности (несущественные ошибки), которые исправляются самим студентом после дополнительных и (или) уточняющих вопросов экзаменатора.

Оценка «Удовлетворительно» выставляется студенту, который дает недостаточно полные и последовательные ответы на вопросы экзаменационного билета и дополнительные вопросы, но при этом демонстрирует умение выделить существенные и несущественные признаки и установить причинно-следственные связи. Ответы излагаются с использованием терминологии теории решеток, но при этом допускаются ошибки в определениях некоторых основных понятий, формулировках положений, которые студент затрудняется исправить самостоятельно. При аргументации ответа студент не обосновывает свои суждения. На часть дополнительных вопросов студент затрудняется дать ответ или дает неверные ответы.

Оценка «Неудовлетворительно» выставляется студенту, который демонстрирует разрозненные, бессистемные знания; беспорядочно и неуверенно излагает материал; не умеет выделять главное и второстепенное, не умеет соединять теоретические положения с практикой; допускает грубые ошибки при определении сущности раскрываемых понятий, вследствие непонимания их существенных и несущественных признаков и связей; дает неполные ответы, логика и последовательность изложения которых имеют существенные и принципиальные нарушения, в ответах отсутствуют выводы. Дополнительные и уточняющие вопросы экзаменатора не приводят к коррекции ответов студента. На основную часть дополнительных вопросов студент затрудняется дать ответ или дает неверные ответы.

Оценка «Неудовлетворительно» выставляется также студенту, который взял экзаменационный билет, но отказался дать на него ответ.

Приложение № 2 к рабочей программе дисциплины
«Криптографические алгоритмы»

Методические указания для студентов по освоению дисциплины

Учебным планом на изучение дисциплины «Криптографические алгоритмы» отводится два семестра. В конце второго семестра в качестве итогового контроля предусмотрен экзамен, в конце первого семестра обучающиеся в целях промежуточного контроля сдают зачет. В процессе изучения дисциплины проводятся лабораторные работы, выполняются девять домашних заданий.

При изучении дисциплины «Криптографические алгоритмы», используется широкий спектр форм изучения учебного материала – лекции, практические занятия, лабораторные работы. Это связано с тем, что дисциплина «Криптографические алгоритмы» является предшествующей для прохождения производственной и преддипломной практики и итоговой государственной аттестации обучающихся и призвана по возможности подготовить их к практической деятельности.

Для успешного освоения дисциплины важно, чтобы обучающийся уделил особенное внимание выполнению лабораторных работ. Теоретические основы, необходимые для выполнения лабораторных работ, подробно разбираются на лекционных и практических занятиях. Основная цель выполнения лабораторных работ – дать обучающимся представление о возможной практической деятельности аналитика криптографических алгоритмов. Для успешного выполнения лабораторных работ необходимо знать и понимать лекционный материал. Поэтому в процессе изучения дисциплины рекомендуется регулярное повторение пройденного лекционного материала, чему способствуют регулярные задания для самостоятельной работы. Материал, законспектированный на лекциях, необходимо дома еще раз прорабатывать и при необходимости дополнять информацией, полученной на консультациях, практических занятиях или из учебной литературы.

В качестве заданий для самостоятельной работы дома обучающимся предлагаются математические или практические упражнения, которые должны позволить обучающемуся лучше изучить понятия и методы, применяемые им для решения типовых задач из соответствующих разделов дисциплины. Решения задач должны быть подготовлены, оформлены и представлены в установленные сроки.

Предполагается, что результаты промежуточного контроля (зачета) определяются по итогам текущей аттестации. В случае, если обучающийся не показал по итогам текущей аттестации достаточный уровень усвоения материалов дисциплины, ему будет предложено сдать зачет по экзаменационным вопросам, обсуждаемым в первом семестре изучения дисциплины.

В конце второго семестра изучения дисциплины студенты сдают экзамен. Экзамен принимается по экзаменационным билетам, каждый из которых включает в себя два теоретических вопроса. На самостоятельную подготовку к экзамену выделяется 4 дня, во время подготовки к экзамену предусмотрена групповая консультация.

Опыт преподавания дисциплины «Криптографические алгоритмы» говорит о сложности ее самостоятельного изучения для обучающегося, несмотря на наличие достаточно качественных учебных пособий. Это связано с насыщенностью изучаемого

материала и большим числом лабораторных работ, необходимых для приобретения навыков практического использования изучаемого материала. Поэтому посещение всех аудиторных занятий является настоятельно рекомендуемым.