МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования

«ИРКУТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

(ФГБОУ ВО «ИГУ»)

Институт математики и информационных технологий

Кафедра алгебраических и информационных систем

«УТВЕРЖДАЮ»
Директор ИМИТ ИГУ
_____ М. В. Фалалеев
«15» мая 2024 г.

Рабочая программа дисциплины (модуля)

Б1.В.09 Криптография

Направление подготовки 02.03.02 Фундаментальная информатика и информационные технологии

Направленность (профиль) подготовки Фундаментальная информатика и информационные технологии

Квалификация выпускника бакалавр

Форма обучения очная

Иркутск 2024 г.

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

Цель

Ознакомление студентов с основами криптографии и основами обеспечения защиты информации, формирование практических умений и навыков при работе с криптографическим примитивами, формирование ключевых профильных компетенций.

Задачи:

- дать специальные знания по дисциплине,
- достичь достаточного уровня знаний по криптографическим методам обеспечения информационной безопасности;
- сформировать у студентов практические навыки работы со средствами обеспечения криптографической безопасности.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

2.1. Учебная дисциплина (модуль) относится к части программы, формируемой участниками образовательных отношений, и изучается на третьем курсе.

2.2. Для изучения данной учебной дисциплины (модуля) необходимы знания, умения и навыки, сформированные дисциплинами: Программирование, Теория вероятностей и математическая статистика, Дискретная математика.

2.3. Перечень последующих учебных дисциплин, для которых необходимы знания, умения и навыки, формируемые данной учебной дисциплиной: Выпускная квалификационная работа.

3. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Процесс освоения дисциплины направлен на формирование компетенций (элементов следующих компетенций) в соответствии с ФГОС ВО по соответствующему направлению подготовки.

Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций

Компетенция	Индикаторы компетенций	Результаты обучения
ПК-3 Способность понимать и применять в научно-исследовательской и прикладной деятельности современный математический аппарат, теоретические основы информатики	ИДК $_{ПК3.1}$ Способен понимать современный математический аппарат и теоретические основы информатики	Знает современные криптографические стандарты симметричных и асимметричных систем Умеет определять возможность применения криптографических стандартов для решения текущей задачи. Владеет навыками выявления угроз безопасности при использовании криптографических стандартов
	ИДК $_{ПК3.2}$ Способен применять в научно-исследовательской и прикладной деятельности современный математиче-	Знает устройство современных криптографических стандартов симметричных и асимметричных систем, прикладных криптографических протоколов.

	ский аппарат	Умеет анализировать современные криптографические стандарты симметричных и асимметричных систем, прикладные криптографические протоколы на наличие уязвимостей с помощью современного математического аппарата.
ПК-4 Способность понимать и применять в научно-исследовательской и прикладной деятельности современные языки программирования и программное обеспечение; операционные системы и сетевые технологии; применять алгоритмы и структуры данных при разработке программных решений	ИДК $_{ПК4.1}$ Способен понимать современные языки программирования и программное обеспечение; операционные системы и сетевые технологии	Знает программные объекты, реализующие криптографические стандарты симметричного и асимметричного шифрования Умеет определять последовательность применения библиотечных методов для реализации прикладных криптографических алгоритмов.
	ИДК $_{ПК4.3}$ Способен применять алгоритмы и структуры данных при разработке программных решений	Знает принципы использования библиотечных методов и криптопровайдеров. Умеет применять программные объекты и криптопровайдеры для реализации приложений Владеет приемами использования криптографических примитивов при разработке программных решений

4. СОДЕРЖАНИЕ И СТРУКТУРА ДИСЦИПЛИНЫ

Объем дисциплины составляет 5 зачетных единиц, 180 часов, в том числе 35 часов на контроль, практическая подготовка 32.
Форма промежуточной аттестации: 6 семестр - экзамен.

4.1. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ, СТРУКТУРИРОВАННОЕ ПО ТЕМАМ, С УКАЗАНИЕМ ВИДОВ УЧЕБНЫХ ЗАНЯТИЙ И ОТВЕДЕННОГО НА НИХ КОЛИЧЕСТВА АКАДЕМИЧЕСКИХ ЧАСОВ

№ п/п	Раздел дисциплины/темы	Семестр	Виды учебной работы, включая самостоятельную работу обучающихся и трудоемкость (в часах)					Формы текущего контроля успеваемости
			Контактная работа преподавателя с обучающимися			Самостоятельная работа + контроль		
			Лекции	Семинарские (практические занятия)	Контроль обучения			
1	Тема 1. Базовые понятия криптографии	6	2	2	0,6	3	2	лаб.
2	Тема 2. Симметричные криптосистемы	6	2	2	0,6	3	2	лаб.
3	Тема 3. Поточные шифры	6	2	2	0,6	4	2	тест
4	Тема 4. Блочное шифрование	6	4	4	1,2	6	4	лаб.
5	Тема 5. Режимы шифрования	6	4	4	1,2	6	4	тест
6	Тема 6. Коды аутентификации сообщений	6	2	2	0,6	4	2	лаб.
7	Тема 7. Хеш-функции	6	2	2	0,6	4	2	тест
8	Тема 8. Стандарты аутентичного шифрования	6	4	4	1,6	8	4	лаб.
9	Тема 9. Алгоритмы обмена ключами	6	2	2	0,6	4	2	лаб.
10	Тема 10. Метод ключевого обмена Диффи-Хелмана	6	2	2	0,6	7	3	лаб.
11	Тема 11. Преобразование RSA	6	2	2	0,6	6	2	лаб.
12	Тема 12. Преобразование Эль-Гамаля	6	2	2	0,6	6	2	лаб.

13	Тема 13. Прикладные алгоритмы криптографии	6	2	2	0,6	10	4	лаб.
Итого часов			32	32	10	71/35		

4.2. ПЛАН ВНЕАУДИТОРНОЙ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

Семестр	Название раздела, темы	Самостоятельная работа обучающихся			Оценочное средство	Учебно-методическое обеспечение самостоятельной работы
		Вид самостоятельной работы	Сроки выполнения	Затраты времени (час.)		
6	Симметричные алгоритмы шифрования	УИЛТИн	1-я половина курса + подготовка к экз	36	Тест	УМО расположено в ИОС Domic на странице курса
6	Обеспечение целостности сообщений	УИЛТИн	1-я половина курса + подготовка к экз	24	Тест	УМО располо-жено в ИОС Domic на стра-нице курса
6	Алгоритмы с открытым ключом	УИЛТИн	2-я половина курса + подготовка к экз	46	Контрольная работа	УМО располо-жено в ИОС Domic на стра-нице курса
Общая трудоемкость самостоятельной работы по дисциплине (час)				106		
Из них объем самостоятельной работы с использованием электронного обучения и дистанционных образовательных технологий (час)				106		

4.3. СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

Раздел 1. Симметричные алгоритмы шифрования

Тема 1. Базовые понятия криптографии

Общие принципы и модели. Защита от несанкционированного доступа. Понятие ключа. Шифрование и кодирование. Криптосистемы. История криптографии. Шифр простой замены. Шифр Цезаря. Шифр вертикальной перестановки. Гаммирование. Основные способы криптоанализа простых шифров. Идеальный шифр.

Тема 2. Симметричные криптосистемы

Шифр Вернама. Лемма о теоретически стойком шифре. Потоковые шифры. Атаки на потоковые шифры. Двухразовый блокнот. Пример уязвимости в протоколе. 802.11b WEP. Возможные улучшения протокола.

Тема 3. Поточные шифры

Примеры потоковых шифров. RC4 и его уязвимости. CSS и его уязвимости. eStream. Безопасность потоковых генераторов. Статистический тест для генератора. Криптографическое определение псевдослучайного генератора. Семантически безопасный потоковый шифр. Примеры таких шифров.

Тема 4. Блочное шифрование

Принцип итерирования. Понятие псевдослучайной функции и псевдослучайной перестановки. Шифр DES. Описание структуры. Теорема о трехраундовой сети Фейстеля. Шифр AES. Описание структуры и принципы работы. Переборные атаки на блочные шифры. Проблема DES. Тройной DES. Атака методом встречи посередине. Переборные атаки на блочные шифры. Проблема DES. Атаки на блочные шифры через утечки по побочным каналам. Атаки на основе отказов. Линейный криптонанализ DES (основные идеи). Шифр ГОСТ 28147-89 и его инфраструктура.

Тема 5. Режимы шифрования

Построение блочных шифров на основе псевдослучайных генераторов. Шифрование нескольких сообщений на одном ключе. Атака на основе выборочного открытого текста. Пример шифра нестойкого к атаке на основе выборочного открытого текста. Случайное шифрование. Одноразовое шифрование. Режим CBC. Шифрование с предсказанным значением вектора инициализации. CBC для одноразового шифрования. Набивка блоков. Режим CTR. Сравнение режимов CBC и CTR. Режим OFB.

Раздел 2. Обеспечение целостности сообщений

Тема 6. Коды аутентификации сообщений

Коды аутентификации сообщений. Построение кодов аутентификации больших сообщений. Конструкции CBC-MAC и NMAC. Их эффективность. Схема атаки с использованием коллизий. Конструкция HMAC. Построение кодов аутентификации больших сообщений. Механизмы набивки сообщений. Конструкции CMAC, PMAC, одноразовый MAC.

Тема 7. Хеш-функции

Построение кодов аутентификации сообщений из стойких к коллизиям функций. Атака на основе парадокса дней рождений. Конструкция Меркла-Дамгарда для построения хеш-функций. Построение безопасных сжимающих функций. Хеш-функции на основе блочных шифров.

Тема 8. Стандарты аутентичного шифрования

Необходимость применения аутентичного шифрования. Понятие целостности шифр-текста. Атака на основе выборочного шифр-текста. Аутентичное шифрования на примере протокола TLS. Построение схем аутентичного шифрования из блочных шифров и кодов аутентификации сообщений. Стандарты аутентичного шифрования. Атаки на схемы аутентичного шифрования. Атака на основе анализа набивки сообщения.

Раздел 3. Алгоритмы с открытым ключом

Тема 9. Алгоритмы обмена ключами

Распределение ключей шифрования. Процедуры обмена ключами. Общее введение в теорию асимметричных криптосистем. Эффективные алгоритмы возведения в степень. Алгоритмы факторизации больших чисел. Понятие функции с лазейкой.

Тема 10. Метод ключевого обмена Диффи-Хелмана

Протокол ключевого обмена для нескольких участников. Некоторые модификации метода. Односторонняя генерация ключа. Задача дискретного логарифмирования.
Тема 11. Преобразование RSA
Устройство RSA. Эффективность реализации. Криптостойкость RSA. Варианты стандартов PKCS1. Атаки на криптосистему RSA. Атака на основе общего RSA модуля. Атака на основе малого значения закрытого ключа.
Тема 12. Преобразование Эль-Гамаля
Вычисление и проверка подписи. Шифрование и дешифрование. Эффективность реализации. Особенности использования сеансового ключа. Практическое применение преобразования Эль-Гамаля для задачи доказательства знания.
Тема 13. Прикладные алгоритмы криптографии
Пороговые схемы разделения секрета. Схема Шамира разделения секрета. Доказательство с нулевым разглашением. Алгоритм на основе изоморфизма графов. Протокол Шнорра.

4.3.1. Перечень семинарских, практических занятий и лабораторных работ

№ п/н	№ раздела и темы	Наименование семинаров, практических и лабораторных работ	Трудоемкость (час.)		Оценочные средства	Формируемые компетенции (индикаторы)*
			Всего часов	Из них практическая подготовка		
1	2	3	4	5	6	7
1	1	Тема 1. Базовые понятия криптографии	2	2	Лабораторная работа	ПК-3.1, ПК-3.2, ПК-4.1, ПК-4.3
2	1	Тема 2. Симметричные криптосистемы	2	2	Лабораторная работа	ПК-3.1, ПК-3.2, ПК-4.1, ПК-4.3
3	1	Тема 3. Поточные шифры	2	2	Лабораторная работа	ПК-3.1, ПК-3.2, ПК-4.1, ПК-4.3
4	1	Тема 4. Блочное шифрование	4	4	Лабораторная работа	ПК-3.1, ПК-3.2, ПК-4.1, ПК-4.3
5	1	Тема 5. Режимы шифрования	4	4	Лабораторная работа	ПК-3.1, ПК-3.2, ПК-4.1, ПК-4.3
6	2	Тема 6. Коды аутентификации сообщений	2	2	Лабораторная работа	ПК-3.1, ПК-3.2, ПК-4.1, ПК-4.3
7	2	Тема 7. Хеш-функции	2	2	Лабораторная работа	ПК-3.1, ПК-3.2,

						ПК-4.1, ПК-4.3
8	2	Тема 8. Стандарты аутентичного шифрования	4	4	Лабораторная работа	ПК-3.1, ПК-3.2, ПК-4.1, ПК-4.3
9	3	Тема 9. Алгоритмы обмена ключами	2	2	Лабораторная работа	ПК-3.1, ПК-3.2, ПК-4.1, ПК-4.3
10	3	Тема 10. Метод ключевого обмена Диффи-Хелмана	2	2	Лабораторная работа	ПК-3.1, ПК-3.2, ПК-4.1, ПК-4.3
11	3	Тема 11. Преобразование RSA	2	2	Лабораторная работа	ПК-3.1, ПК-3.2, ПК-4.1, ПК-4.3
12	3	Тема 12. Преобразование Эль-Гамаля	2	2	Лабораторная работа	ПК-3.1, ПК-3.2, ПК-4.1, ПК-4.3
13	3	Тема 13. Прикладные алгоритмы криптографии	2	2	Лабораторная работа	ПК-3.1, ПК-3.2, ПК-4.1, ПК-4.3
		Всего	32	32		

4.3.2. Перечень тем (вопросов), выносимых на самостоятельное изучение студентами в рамках самостоятельной работы (СР)

«Не предусмотрено».

4.4. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОРГАНИЗАЦИИ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

Самостоятельная работа студентов всех форм и видов обучения является одним из обязательных видов образовательной деятельности, обеспечивающей реализацию требований Федеральных государственных стандартов высшего образования. Согласно требованиям нормативных документов самостоятельная работа студентов является обязательным компонентом образовательного процесса, так как она обеспечивает закрепление получаемых на лекционных занятиях знаний путем приобретения навыков осмысления и расширения их содержания, навыков решения актуальных проблем формирования общекультурных и профессиональных компетенций, научно-исследовательской деятельности, подготовки к семинарам, лабораторным работам, сдаче зачетов и экзаменов. Самостоятельная работа студентов представляет собой совокупность аудиторных и внеаудиторных занятий и работ. Самостоятельная работа в рамках образовательного процесса в вузе решает следующие задачи:

– закрепление и расширение знаний, умений, полученных студентами во время аудиторных и внеаудиторных занятий, превращение их в стереотипы умственной и физической деятельности;

– приобретение дополнительных знаний и навыков по дисциплинам учебного плана;

– формирование и развитие знаний и навыков, связанных с научно-исследовательской деятельностью;

– развитие ориентации и установки на качественное освоение образовательной программы;

– развитие навыков самоорганизации;

– формирование самостоятельности мышления, способности к саморазвитию, самосовершенствованию и самореализации;

– выработка навыков эффективной самостоятельной профессиональной теоретической, практической и учебно-исследовательской деятельности.

Подготовка к лекции. Качество освоения содержания конкретной дисциплины прямо зависит от того, насколько студент сам, без внешнего принуждения формирует у себя установку на получение на лекциях новых знаний, дополняющих уже имеющиеся по данной дисциплине. Время на подготовку студентов к двухчасовой лекции по нормативам составляет не менее 0,2 часа.

Подготовка к практическому занятию. Подготовка к практическому занятию включает следующие элементы самостоятельной деятельности: четкое представление цели и задач его проведения; выделение навыков умственной, аналитической, научной деятельности, которые станут результатом предстоящей работы. Выработка навыков осуществляется с помощью получения новой информации об изучаемых процессах и с помощью знания о том, в какой степени в данное время студент владеет методами исследовательской деятельности, которыми он станет пользоваться на практическом занятии. Подготовка к практическому занятию нередко требует подбора материала, данных и специальных источников, с которыми предстоит учебная работа. Студенты должны дома подготовить к занятию 3–4 примера формулировки темы исследования, представленного в монографиях, научных статьях, отчетах. Затем они самостоятельно осуществляют поиск соответствующих источников, определяют актуальность конкретного исследования процессов и явлений, выделяют основные способы доказательства авторами научных работ ценности того, чем они занимаются. В ходе самого практического занятия студенты сначала представляют найденные ими варианты формулировки актуальности исследования, обсуждают их и обосновывают свое мнение о наилучшем варианте. Время на подготовку к практическому занятию по нормативам составляет не менее 0,2 часа.

Подготовка к контрольной работе. Контрольная работа назначается после изучения определенного раздела (разделов) дисциплины и представляет собой совокупность развернутых письменных ответов студентов на вопросы, которые они заранее получают от преподавателя. Самостоятельная подготовка к контрольной работе включает в себя: — изучение конспектов лекций, раскрывающих материал, знание которого проверяется контрольной работой; повторение учебного материала, полученного при подготовке к семинарским, практическим занятиям и во время их проведения; изучение дополнительной литературы, в которой конкретизируется содержание проверяемых знаний; составление в мысленной форме ответов на поставленные в контрольной работе вопросы; формирование психологической установки на успешное выполнение всех заданий. Время на подготовку к контрольной работе по нормативам составляет 2 часа.

Подготовка к экзамену. Самостоятельная подготовка к экзамену схожа с подготовкой к зачету, особенно если он дифференцированный. Но объем учебного материала, который нужно восстановить в памяти к экзамену, вновь осмыслить и понять, значительно больше, поэтому требуется больше времени и умственных усилий. Важно сформировать целостное представление о содержании ответа на каждый вопрос, что предполагает знание разных научных трактовок сущности того или иного явления, процесса, умение раскрывать факторы, определяющие их противоречивость, знание имен ученых, изучавших обсуждаемую проблему. Необходимо также привести информацию о материалах эмпирических исследований, что указывает на всестороннюю подготовку студента к экзамену. Время на подготовку к экзамену по нормативам составляет 36 часов для бакалавров.

В ФБГОУ ВО «ИГУ» организация самостоятельной работы студентов регламентируется Положением о самостоятельной работе студентов, принятым Ученым советом ИГУ 22 июня 2012 г.

4.5. ПРИМЕРНАЯ ТЕМАТИКА КУРСОВЫХ РАБОТ (ПРОЕКТОВ)

«Не предусмотрено».

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

а) перечень литературы

1. Лось, А. Б. Криптографические методы защиты информации для изучающих компьютерную безопасность : учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — Москва : Издательство Юрайт, 2022. — 473 с. —ISBN 978-5-534-12474-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/489242.
2. Введение в криптографию [Текст] : научное издание / ред. В. В. Ященко. - 4-е изд., доп. - М. : Изд-во МЦНМО, 2012. - 347 с. ; 22 см. - Алф. указ.: с. 341-347. - ISBN 978-5-4439-0026-1
3. Рябец Л.В. Задачник-практикум по криптографии: учеб. пособие / Л.В. Рябец. – Иркутск : Изд-во Вост-Сиб. гос. акад. образ., 2013. – 76 с. – ISBN: 978-5-85827-864-1 (30 экз.)
4. Основы криптографии : учеб. пособие для студ. вузов / А. П. Алферов [и др.]. - 3-е изд., испр. и доп. - М. : Гелиос АРВ, 2005. - 480 с. - ISBN 5-85438-137-0 (38 экз.)
5. Чмора А. Л. Основы криптографии: учеб.пособие / А.Л. Чмора – М.: Гелиос АРВ, 2001. – 244 с. – ISBN 5854380374 (51экз.)+
6. Каширская, Е. Н. Криптографические системы : учебное пособие / Е. Н. Каширская, А. П. Кушнир. — Москва : РТУ МИРЭА, 2021. — 66 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/182424.— Режим доступа: для авториз. пользователей.
7. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства / В.Ф. Шаньгин. – М.: ДМК-Пресс. – 2010. – 542 с. – ISBN: 978-5-94074-518-1 (25 экз.)

б) периодические издания

в) список авторских методических разработок:

лекции по криптографии, видео-лекции, расположенные в ИОС Domic и на сайте http://cloud.isu.ru/

г) базы данных, информационно-справочные и поисковые системы

Java Cryptography Architecture (JCA) Reference Guide. URL: https://docs.oracle.com/en/java/javase/11/security/java-cryptography-architecture-jca-reference-guide.html.

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1. УЧЕБНО-ЛАБОРАТОРНОЕ ОБОРУДОВАНИЕ:

Для проведения лекционных занятий необходима аудитория с презентационным оборудованием, для проведения практических занятий необходим компьютерный класс на 25-30 рабочих мест (в зависимости от численности учебной группы), оборудованная доской, презентационной техникой.

6.2. ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ:

1. Комплект разработчика приложений Java Platform (JDK) 11, Standard Edition (распространяется бесплатно);
2. Интегрированная среда разработки NetBeans IDE 12 (распространяется бесплатно, LGPLv2.1, GPLv2 with Classpatch exception);
3. LibreOffice Impress (распространяется бесплатно, GNU LGPL v3+, MPL 2.0);

6.3. ТЕХНИЧЕСКИЕ И ЭЛЕКТРОННЫЕ СРЕДСТВА:

ИОС EDUCA, DOMIC, презентационное оборудование, персональный компьютер с возможностью демонстрации презентаций в формате pdf.

7. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

При реализации данного курса используются следующие образовательные технологии: технологии традиционного обучения, игровые технологии, технологии проблемного обучения, технологии обучения в сотрудничестве, технологии контекстного обучения, интерактивные технологии, технологии дистанционного обучения, активные педагогические технологии.

8. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

8.1. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ВХОДНОГО КОНТРОЛЯ

Не предусмотрено

8.2. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ТЕКУЩЕГО КОНТРОЛЯ

Тесты на странице курса в ИОС Domic в соответствии с п. 4.1.

Примеры оценочных средств текущего контроля

Демонстрационный тест к разделу Обеспечение целостности сообщений

Вопрос 1 Предположим, что система MAC (S,V) используется для защиты файлов в файловой системе компьютера. К каждому файлу добавляется специальный tag. Алгоритм S в своей работе использует только содержимое файла. Для каких атак подобная система MAC является уязвимой?

Варианты ответов

Выполнить конкатенацию двух файлов в системе и создать третий.

Удалить последний байт в файле.

Изменить время модификации файла.

Поменять местами два файла в файловой системе.

Добавить новые данные в файл.

Вопрос 2 Пусть система MAC (S,V) является безопасной. Система определена над пространством (K,M,T), где M={0,1}n и T={0,1}128. Какие из предложенных ниже конструкций являются безопасными MAC?

Варианты ответов

S′(k,m)=S(k,m) и V′(k,m,t)={V(k,m,t),1,m≠0n;otherwise

S′(k,m)=S(k,m ∥ m) и V′(k,m,t)=V(k,m ∥ m,t)

S′(k,m)=S(k,m)[0,...,126] и V′(k,m,t)=[V(k,m,t ∥ 0)orV(k,m,t ∥ 1)]

S′(k,m)={S(k,1n),S(k,m),m=0n;otherwise и V′(k,m,t)={V(k,1n,t),V(k,m,t),m=0n;otherwise

S′(k,m)=[S(k,m),S(k,0n)] и V′(k,m,(t1,t2))=[V(k,m,t1)andV(k,m,t2)]

S′(k,m)=[t=S(k,m),output(t,t)] и V′(k,m,(t1,t2))={V(k,m,t1),0,t1=t2;otherwise

Вопрос 3 Схема вычисления кодов аутентификации сообщений ECBC-MAC использует фиксированный вектор инициализации (в лекции использовался нулевой вектор). Предположим, что вместо фиксированного, для каждого сообщения используется случайный вектор IV и этот вектор добавляется к tag. Другими словами, S(k,m)=(r,ECBCr(k,m)), где r это случайный IV. Алгоритм проверки по ключу k, сообщению m и тегу (r,t) выдает 1 ("yes"), если t=ECBCr(k,m).

Такая схема построения MAC является небезопасной. Атакующий может получить тег (r,t) для сообщения m, состоящего из одного блока. Теперь он способен сконструировать новый тег для нового сообщения. Укажите пару тег, сообщение, которую может сконструировать атакующий.

Варианты ответов

Тег (m⊕t,t) является правильным для сообщения m⊕1n.

Тег (r⊕t,r) является правильным для сообщения m.

Тег (r⊕t,m) является правильным для сообщения 0n.

Тег (r⊕1n,t) является правильным для сообщения m⊕1n.

Вопрос 4 Алиса намеревается организовать широковещательную отправку сообщений для 6 получателей B1,…,B6. Секретность сообщений не важна, важна целостность и аутентичность. Каждый из получателей должен быть уверен, что сообщение получено от Алисы.

Для своей задачи Алиса решила использовать MAC. Предположим, что Алиса и 6 пользователей работают с одним общим ключом k. Тогда каждый из B1,…,B6 при получении сообщения может проверить правильность тега. Но эта схема небезопасна, т.к., например, пользователь B1 может создать сообщение, прикрепить к нему тег, полученный на ключе k и отправить в сеть. При этом, пользователи B2,…,B6 будут уверены, что сообщение получено от Алисы.

Вместо этого, Алиса сгенерировала 4 секретных ключа S={k1,…,k4}. Каждому пользователю Bi она передала подмножество ключей Si⊆S. Теперь Алиса при передаче сообщения прикладывает к нему четыре тега, каждый из которых получен на одном из четырех ключей. Когда пользователь Bi получает сообщение он проверяет только те теги сообщения, для которых у него есть ключи.

Выберите правильный способ, которым Алиса может распределить случайные ключи так, чтобы никто из пользователей не смог бы создавать сообщения для других пользователей правильные сообщения от имени Алисы

Варианты ответов

S1={k1,k2}, S2={k1}, S3={k1,k4}, S4={k2,k3}, S5={k2,k4}, S6={k3,k4}

S1={k2}, S2={k2,k3}, S3={k3,k4}, S4={k1,k3}, S5={k1,k2}, S6={k1,k4}

S1={k1,k2}, S2={k2,k3}, S3={k3,k4}, S4={k1,k3}, S5={k1,k2}, S6={k1,k4}

S1={k1k2}, S2={k1,k3}, S3={k1,k4}, S4={k2,k3}, S5={k2,k4}, S6={k3,k4}

Вопрос 5 Пусть H:M→T стойкая к коллизиям хеш функция. Какая из следующий функций также будет стойкой к коллизиям.

Варианты ответов

H′(m)=H(m[0,…,|m|−2])

H′(m)=H(m) ∥ H(m)

H′(m)=H(H(m))

H′(m)=H(m)⊕H(m⊕1|m|)

H′(m)=H(m)[0,…,31]

H′(m)=H(|m|), где |m| есть длина сообщения m

H′(m)=H(m ∥ m)

H′(m)=H(m ∥ 0)

H′(m)=H(m)⊕H(m)

Лабораторная работа к разделу Симметричное шифрование. Шифрование AES

Для работы с алгоритмами и протоколами шифрования будем использовать стандартный API JCA, содержащийся в JDK 1.6. Приведенные ниже классы и примеры будут работать как со стандартным криптопровайдером JCE, так и с любым другим криптопровайдером, поддерживающим реализованный в Java API (например, Bouncy Castle).

При шифровании данных управление ключами может происходить двумя способами: шифрование на случайном ключе, шифрование на известном ключе.

Рассмотрим процедуру симметричного шифрования на случайном ключе. Ключ создается объектом класса KeyGenerator из пакета javax.crypto. Для создания генератора нужно воспользоваться специальным методом

KeyGenerator kg = KeyGenerator.getInstance("DES");

где аргументом метода выступает имя алгоритма, для которого происходит генерация ключа (в данном случае DES). Список доступных алгоритмов здесь. После создания генератора

необходимо использовать метод init() для его инициализации и метод generateKey() — для создания ключа.
Например, следующий код создает ключ шифрования на основании безопасного генератора случайных чисел для алгоритма AES:

```
KeyGenerator kg = KeyGenerator.getInstance("AES");
kg.init(new SecureRandom());
SecretKey key = kg.generateKey();
```

При использовании в качестве ключа готовой последовательности байт нужно воспользоваться классом SecretKeySpec из пакета javax.crypto.spec. Ключ создается через параметры конструктора, в которых указывается массив байт, содержащих ключ, и алгоритм шифрования. Например, следующий код генерирует ключ для алгоритма AES на основе строки из шестнадцати символов "1234567890123456":

```
byte[] newKey = "1234567890123456".getBytes();
SecretKey key = new SecretKeySpec(newKey, "AES");
```

Класс Cipher является основным для работы с алгоритмами шифрования и расположен в пакете javax.crypto. Этот класс предоставляет возможность работы как с алгоритмами шифрования, так и с режимами работы шифров, схемами дополнения сообщений. В зависимости от параметров инициализации, объект класса Cipher может работать как в режиме шифрования, так и в режиме расшифрования, с симметричными и асимметричными алгоритмами.
Для создания нового объекта класса следует воспользоваться специальным методом:

```
Cipher c = Cipher.getInstance(algorithm)
```

где algorithm представляет собой строку вида: алгоритм шифрования\режим работы\алгоритм дополнения
Имена доступных алгоритмов шифрования и их настройки прописаны в стандарте Java, и, обычно, они совпадают с общепринятыми обозначениями. Для дополнения сообщений, в основном, используются два стандарта: NoPadding — для шифрования без дополнения сообщения (например, для режима шифрования CTR) и PKCS5Padding — для дополнения сообщения до размера, кратного размеру блока используемого алгоритма (например, для режима CBC).
Для реализации процедуры шифрования тексты должны быть представлены в виде массива байт. Опишем шифрование сообщения по шагам:
Создание объекта Cipher с использованием метода getInstance.
Инициализация объекта Cipher с помощью метода init() для шифрования или расшифрования. Этот метод принимает на вход два обязательных параметра и один необязательный параметр. Первый параметр указывает режим работы алгоритма: Cipher.ENCRYPT_MODE или Cipher.DECRYPT_MODE. Второй параметр — ключ шифрования. Тип ключа зависит от используемого алгоритма шифрования. Третьим параметром указывается вектор инициализации алгоритма: объект класса IvParameterSpec.
Шифрование или расшифрование производится методами update() для работы с сообщением в режиме потока (обработка сообщения по частям) и doFinal() для обработки сообщения полностью.
Ниже приведен пример шифрования сообщения OpenText шифром AES в режиме CBC на случайном ключе и случайном векторе инициализации:

```
KeyGenerator kg = KeyGenerator.getInstance("AES");
kg.init(new SecureRandom());
SecretKey key = kg.generateKey();
SecureRandom sr = new SecureRandom();
byte[] IV = new byte[16];
sr.nextBytes(IV);
Cipher c = Cipher.getInstance("AES/CBC/PKCS5Padding");
c.init(Cipher.ENCRYPT_MODE, key, new
IvParameterSpec(IV));
```

byte[] encryptedData = c.doFinal(OpenText.getBytes());
Так как массив байт невозможно вывести в текстовый файл, то результат шифрования нужно закодировать либо в шестнадцатеричном формате, либо в формате Base64.
Работа с форматом Base64 в Java обеспечивается двумя классами BASE64Encoder и BASE64Decoder из пакета sun.misc. Для выполнения преобразований используются методы encode и decodeBuffer соответствующих классов.
По полученным параметрам выполнить расшифрование заданного шифр-текста. Исходный открытый текст зашифрован алгоритмом AES в режиме CBC. В варианте содержится шифр-текст, вектор инициализации, ключ шифрования. Все данные представлены в формате BASE64. Требуется расшифровать шифр-текст.

1. Расшифрование нужно проводить по следующей схеме:
2. Раскодировать ключ, вектор инициализации и шифр-текст из формата BASE64 в последовательности байт.
3. С использованием объекта класса SecretKeySpec по последовательности байт ключа создать объект класса SecretKey.
4. Создать объект класса Cipher с параметром "AES/CBC/ISO10126Padding".
5. При инициализации шифра требуется подключить вектор инициализации с помощью объекта класса IvParameterSpec.
6. Выполнить расшифрование шифр-текста.

В результате расшифрования должен получиться массив байт, который в кодировке ASCII можно интерпретировать как осмысленный текст. Для преобразования массива байт в строку можно воспользоваться конструктором класса String.

Лабораторная работа к разделу Алгоритмы с открытым ключом. Атака на RSA при использовании закрытого ключа

Даны числа N и e, формирующие открытый ключ преобразования RSA. Известно, что значение закрытого ключа d мало (это можно предположить исходя из значения ключа e). С использованием подходящих дробей требуется получить значение ключа d, и затем на основе его значения решить задачу факторизации для числа N.
Вычисление закрытого ключа
Известно, что при $d<\frac{\sqrt[4]{N}}{3}$ выполняется соотношение $$ \left|\frac{e}{N}-\frac{k}{d}\right|<\frac{1}{2d^2}. $$
Таким образом, для нахождения закрытого ключа можно воспользоваться подходящими дробями согласно алгоритму:
Представить дробь $\frac{e}{N}$ в виде цепной дроби.
Для найденной цепной дроби построить последовательность подходящих дробей.
Начиная с некоторого номера знаменатель подходящей дроби можно рассматривать в качестве кандидата на закрытый ключ d.
Для каждого кандидата проверить условие корректности закрытого ключа. Согдасно определению открытого и закрытого ключей для любого сообщения m должно выполняться соотношение $$m^{ed} \equiv m (N)$$.
Знаменатель подходящей дроби, удовлетворяющий условию корректности можно рассматривать в качестве закрытого ключа преобразования RSA.
Факторизация модуля при известном закрытом ключе
Пусть известны модуль N, открытый ключ e и закрытый ключ d, полученный на предыдущем шаге.
Возьмем произвольное число x. Обозначим за $y_1 = x^{\frac{ed-1}{2}}$ (это возможно, поскольку ed это нечетное число). Тогда $$y_1^2\equiv 1 (N).$$ Иначе $$(y_1-1)(y_1+1)\equiv0(N).$$ Возможны следующие варианты:
Если $y_1=1$. Если $\frac{ed-1}{2}$ — число четное, то введем $y_2 = x^{\frac{ed-1}{4}}$ и проанализируем значение y_2 (все рассуждения справедливы для y_2). Иначе потребуется выбрать другое основание x.

Если $y_1=-1$. То потребуется выбрать другое основание x.
Если y_1 есть число отличное от 1 и -1, то тогда делитель числа N вычисляется по формуле:$$p=НОД(y_1-1,N).$$

Лабораторная работа к разделу Алгоритмы с открытым ключом. Шифрование с использованием библиотеки OpenSSL

Механизм шифрования сообщений

Цель данного задания заключается в ознакомлении с основными возможностями криптографической библиотеки OpenSSL. Библиотека, в основном, предназначена для организации взаимодействия на основе инфраструктуры открытых ключей. Но в последних версиях библиотеки реализована функциональность по симметричному шифрованию сообщений. Библиотека работает из командной строки в пакетном режиме.

Версии библиотек: openssl-1.0.2-i386-win32.zip, openssl-1.0.2-x64_86-win64.zip

Требуется сгенерировать случайный ключ шифрования, зашифровать алгоритмом AES некоторый открытый текст и передать ключ шифрования через преобразование RSA с помощью алгоритма шифрования сеансового ключа и зашифрованное сообщение на проверку преподавателю.

Часть 1. Шифрование сообщения

С помощью OpenSSL зашифруйте сообщение. Шифрование нужно проводить по следующей схеме:

Выберите некоторое сообщение (содержащее в том числе номер зачетной книжки) и поместите его в файл. Сообщение может быть любого разумного размера и должно читаться без использования специальных программ.

Сгенерируйте с помощью команды openssl rand (doc) случайный ключ необходимой для алгоритма AES-128-CBC длины и сохраните его в файл в шестнадцатеричном формате .

Сгенерируйте с помощью команды openssl rand вектор инициализации необходимой для алгоритма AES-128-CBC длины и сохраните его в файл в шестнадцатеричном формате.

С помощью команды openssl enc (doc) зашифруйте алгоритмом AES-128-CBC файл с открытым текстом на сгенерированных ранее ключе и векторе инициализации. NB! При шифровании следует использовать именно ключ шифрования, а не пароль.

Сохраните ключ шифрования и вектор инициализации в одном файле в двух разных строках без дополнительных комментариев.

Часть 2. Самостоятельное шифрование ключа симметричного шифрования

В этой части лабораторной потребуется создать собственную пару RSA-ключей и пройти обе фазы алгоритма шифрования симметричного ключа. Работать можно по следующей схеме:

С помощью команды openssl genrsa (doc) сгенерируйте закрытый RSA-ключ. Длина ключа должна составлять 2048 бит. Для большей надежности ключ можно зашифровать паролем.

С помощью команды openssl rsa (doc) сгенерируйте открытый RSA-ключ.

На открытом RSA-ключе с помощью openssl rsautl (doc) зашифруйте файл с ключом и вектором инициализации.

Проведите проверку своих действий и расшифруйте на закрытом RSA-ключе полученный на предыдущем шаге файл.

Проверьте, что расшифрование прошло успешно и в итоге получился тот же самый ключ симметричного шифрования.

Расшифруйте сообщение.

Часть 3. Отправка результатов на проверку

Для отправки результатов шифрования на проверку необходимо выполнить следующие действия:

Загрузите открытый RSA-ключ преподавателя.

На загруженном открытом ключе с помощью openssl rsautl зашифруйте файл с ключом симметричного шифрования и вектором инициализации.

Отправьте на проверку файл с зашифрованным текстом и файл с зашифрованным симметричным ключом. Свои RSA-ключи в ИОС Домик загружать не требуется.
Проверка результата шифрования будет проводиться следующими командами:
openssl rsautl -decrypt -inkey private.pem -in key.hex.enc -out key.hex
openssl enc -aes-128-cbc -d -in ct.txt -out ot.txt -K 000000 -iv 000000 -p

8.3. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПРОМЕЖУТОЧНОГО КОНТРОЛЯ

Материалы для проведения текущего и промежуточного контроля знаний студентов:

№	Вид контроля	Контролируемые темы (разделы)	Контролируемые компетенции/ индикаторы
1	**2**	**3**	**4**
1	Контроль в виде тестов Разноуровневые задания к лабораторному практикуму	Раздел 1	ПК-3, ПК-4
2	Контроль в виде тестов Разноуровневые задания к лабораторному практикуму	Раздел 2	ПК-3, ПК-4
3	Контрольные работы Разноуровневые задания к лабораторному практикуму	Раздел 3	ПК-3, ПК-4
4	Экзамен	Промежуточная аттестация	ПК-3, ПК-4

Оценочные средства промежуточного контроля формируются в соответствии с Положением о балльно-рейтинговой системе:

Выполнение лабораторных, домашних заданий в информационно-образовательной среде, а также контрольных работ и тестов дает 60 баллов в семестре. Распределение весов учебных единиц представлено в ИОС Domic. В оценке экзамен составляет 30 баллов. Дополнительные 10 баллов выставляется за посещаемость.

Процедура сдачи экзамена

Для успешной сдачи экзамена требуется осветить два теоретических вопроса, каждый из которых дает 15 баллов. После процедуры выбора, экзаменуемому предоставляется 60 минут для подготовки ответа на выбранные вопросы. После ответа на основные вопросы экзаменуемому может быть задан дополнительный вопрос, оценивающийся в 10 баллов.

Критерии оценивания теоретических вопросов:

15 баллов: экзаменуемый самостоятельно и без наводящих вопросов осветил все основные разделы вопроса, ввел необходимые определения, описал необходимые алгоритмы; привел примеры.

10 баллов: экзаменуемый, после задания уточняющих и наводящих вопросов, в достаточно полной степени осветил содержание вопроса, ввел определения, возможно не осветил некоторые шаги алгоритмов, привел примеры.

5 баллов: экзаменуемый не осветил вопрос, но ответил на наводящие, уточняющие и дополнительные вопросы, привел основные определения, но не привел необходимые примеры.

0 баллов: не ответил на выбранные им вопросы экзамена и уточняющие вопросы экзаменатора.

Список вопросов для промежуточной аттестации:

1. Общие принципы криптографии. Защита от несанкционированного доступа. Основные способы криптоанализа простых шифров. Идеальный шифр.
2. Шифр Вернама. Лемма о теоретически стойком шифре. Потоковые шифры. Атаки на потоковые шифры. Двухразовый блокнот.
3. Примеры потоковых шифров. RC4 и его уязвимости.
4. Безопасность потоковых генераторов. Статистический тест для генератора. Криптографическое определение псевдослучайного генератора.
5. Принцип итерирования. Понятие псевдослучайной функции и псевдослучайной перестановки. Шифр DES. Описание структуры. Теорема о трехраундовой сети Фейстеля.
6. Шифр AES. Описание структуры и принципы работы. Переборные атаки на блочные шифры.
7. Построение блочных шифров на основе псевдослучайных генераторов. Шифрование нескольких сообщений на одном ключе. Атака на основе выборочного открытого текста. Пример шифра нестойкого к атаке на основе выборочного открытого текста.
8. Случайное шифрование. Одноразовое шифрование. Режим CBC. Шифрование с предсказанным значением вектора инициализации. CBC для одноразового шифрования. Набивка блоков. Режим CTR. Сравнение режимов CBC и CTR. Режим OFB.
9. Коды аутентификации сообщений. Построение кодов аутентификации больших сообщений. Конструкции CBC-MAC и NMAC. Их эффективность. Схема атаки с использованием коллизий.
10. Конструкция HMAC. Построение кодов аутентификации больших сообщений. Механизмы набивки сообщений.
11. Построение кодов аутентификации сообщений из стойких к коллизиям функций. Атака на основе парадокса дней рождений.
12. Конструкция Меркла-Дамгарда для построения хеш-функций. Построение безопасных сжимающих функций. Хеш-функции на основе блочных шифров.
13. Необходимость применения аутентичного шифрования. Понятие целостности шифр-текста. Атака на основе выборочного шифр-текста. Аутентичное шифрования на примере протокола TLS.
14. Стандарт PKCS1. Атаки на RSA. Атака при малом значении закрытого ключа.
15. Задача дискретного логарифмирования. Метод ключевого обмена Диффи-Хеллмана.
16. Преобразование Эль-Гамаля. Шифрование и создание подписи сообщений.
17. Схема Шамира разделения секрета.
18. Алгоритм Шнорра доказательства знания.

Разработчик:

_____

доцент кафедры алгебраических и информационных систем Рябец Л.В.

Программа составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 02.03.02 «Фундаментальная информатика и информационные технологии» (уровень бакалавриата), утвержденный приказом Министерства образования и науки Российской Федерации от 23 августа 2017 г. N 808, зарегистрированный в Минюсте России «14» сентября 2017 г. № 48185 с изменениями и дополнениями с изменениями и дополнениями от: 26 ноября 2020 г., 8 февраля 2021 г.

Программа рассмотрена на заседании кафедры Алгебраических и информационных систем ИМИТ ИГУ «04» апреля 2023 г.

Протокол № 9 Зав. кафедрой_____ Пантелеев В.И.