Федеральное государственное бюджетное образовательное учреждение
высшего образования

САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ
АРХИТЕКТУРНО-СТРОИТЕЛЬНЫЙ УНИВЕРСИТЕТ

Кафедра Информационных технологий

УТВЕРЖДАЮ
Начальник учебно-методического управления

Михайлова
Анна Олеговна

Подписано цифровой
подписью: Михайлова
Анна Олеговна

«29» июня 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Криптография

направление подготовки/специальность 01.03.02 Прикладная математика и информатика

направленность (профиль)/специализация образовательной программы Прикладная математика и информатика

Форма обучения очная

Санкт-Петербург, 2023

1. Цели и задачи освоения дисциплины (модуля)

Целью дисциплины является освоение студентами методов, способов и средств программной и аппаратной реализации криптографических алгоритмов

Задачами освоения дисциплины являются:

− изучение математических основ криптографии;

− получение студентами знаний о компьютерной криптографии, включая программную реализацию криптографических алгоритмов, проверку их качества, генерацию и распределение ключей;

− приобретение навыков использования алгоритмов шифрования, электронной цифровой подписи, хэш-функций, генерации псевдослучайных последовательностей чисел и протоколов аутентификации, используемых в широко распространенных программных продуктах.

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

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, обеспечивающие достижение планируемых результатов освоения ОПОП
ОПК-4 Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	ОПК-4.2 Предлагает способ и средство решения задачи профессиональной деятельности с учетом возможностей информационных технологий	**знает** − математические основы криптографической защиты информации; **умеет** − определять возможности применения теоретических положений и методов высшей математики для постановки и решения конкретных задач криптографии; **владеет** − стандартными математическими методами и их применением к решению задач защиты данных;
ОПК-4 Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	ОПК-4.3 Составляет алгоритм решения сформулированной задачи	**знает** − алгоритмы шифрования и особенности их реализации; **умеет** − решать прикладные задачи криптографической защиты; − оценивать эффективность применения различных методов криптографии; **владеет** − навыками работы с современными пакетами прикладных программ в области криптографии и информационной безопасности.

3. Указание места дисциплины (модуля) в структуре образовательной программы

Данная дисциплина (модуль) включена в Блок «Дисциплины, модули» Б1.О.15 основной профессиональной образовательной программы 01.03.02 Прикладная математика и информатика и относится к обязательной части учебного плана.

Для изучения дисциплины, обучающиеся должны:

знать:

− основные положения высшей алгебры и теории чисел;

− основные положения теории вероятностей и математической статистики;

− базовые понятия и основные приёмы матричной алгебры;

уметь:

− определять возможности применения теоретических положений и методов высшей математики для постановки и решения конкретных задач;

владеть:

− стандартными математическими методами и их применением к решению задач защиты данных;

− навыками работы с наиболее распространенными пакетами прикладных программ в области информационной безопасности.

№ п/п	Последующие дисциплины	Код и наименование индикатора достижения компетенции
1	Вероятностное и имитационное моделирование	ПК-4.1, ПК-4.4
2	Выполнение и защита выпускной квалификационной работы	УК-1.1, УК-1.2, УК-1.3, УК-1.4, УК-1.5, УК-1.6, УК-2.1, УК-2.2, УК-2.3, УК-2.4, УК-3.1, УК-3.2, УК-3.3, УК-3.4, УК-3.5, УК-3.6, УК-4.1, УК-4.2, УК-4.3, УК-4.4, УК-5.1, УК-5.2, УК-5.3, УК-6.1, УК-6.2, УК-6.3, УК-6.4, УК-6.5, УК-7.1, УК-7.2, УК-7.3, УК-7.4, УК-8.1, УК-8.2, УК-8.3, УК-8.4, УК-9.1, УК-9.2, УК-9.3, УК-9.4, УК-9.5, УК-10.1, УК-10.2, УК-10.3, ОПК-1.1, ОПК-1.2, ОПК-1.3, ОПК-2.1, ОПК-2.2, ОПК-2.3, ОПК-3.1, ОПК-3.2, ОПК-4.1, ОПК-4.2, ОПК-4.3, ОПК-5.1, ОПК-5.2, ОПК-5.3, ПК-1.1, ПК-1.2, ПК-1.3, ПК-1.4, ПК-2.1, ПК-2.2, ПК-2.3, ПК-3.1, ПК-3.2, ПК-3.3, ПК-4.1, ПК-4.2, ПК-4.3, ПК-4.4, ПК(Ц)-1.1, ПК(Ц)-1.2, ПК(Ц)-1.3, ПК(Ц)-1.4, ПК(Ц)-1.5

4. Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Вид учебной работы	Всего часов	Из них часы на практическую подготовку	Семестр
			2
Контактная работа	32		32
Практические занятия (Пр)	32	0	32
Иная контактная работа, в том числе:	0,8		0,8
консультации по курсовой работе (проекту), контрольным работам (РГР)	0,4		0,4
контактная работа на аттестацию (сдача зачета, зачета с оценкой; защита курсовой работы (проекта); сдача контрольных работ (РГР))	0,4		0,4
контактная работа на аттестацию в сессию (консультация перед экзаменом и сдача			
Часы на контроль	4		4
Самостоятельная работа (СР)	35,2		35,2
Общая трудоемкость дисциплины (модуля)			
часы:	72		72
зачетные единицы:	2		2

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

5.1. Тематический план дисциплины (модуля)

№	Разделы дисциплины	Семестр	Контактная работа (по учебным занятиям), час.						СР	Всего, час.	Код индикатора достижения компетенции
			лекции		ПЗ		ЛР				
			всего	из них на практическую подготовку	всего	из них на практическую подготовку	всего	из них на практическую подготовку			
1.	1 раздел. 1. Криптографическая защита информации										
1.1.	Математические основы криптографии и криптоанализа	2			3				8	11	ОПК-4.2, ОПК-4.3
1.2.	1.2. Симметричные и асимметричные криптосистемы	2			5				2	7	ОПК-4.2, ОПК-4.3
1.3.	1.3. Функции хеширования: назначение и использование	2			4				2	6	ОПК-4.2, ОПК-4.3
2.	2 раздел. 2. Электронная цифровая подпись										
2.1.	2.1. ЭЦП: назначение и области применения	2			2				3,2	5,2	ОПК-4.2, ОПК-4.3
2.2.	2.2. Основные алгоритмы ЭЦП	2			5				1	6	ОПК-4.2, ОПК-4.3
2.3.	2.3. Проблемы генерации ключей	2			5				2	7	ОПК-4.2, ОПК-4.3
3.	3 раздел. 3. Методы криптоанализа										
3.1.	3.1. Частотный анализ.	2			2				7	9	ОПК-4.2, ОПК-4.3

3.2.	3.2. Криптоанализ симметричных и асимметричных шифров	2			3				6	9	ОПК-4.2, ОПК-4.3
3.3.	3.3. Сравнение методов криптоанализа	2			3				4	7	ОПК-4.3, ОПК-4.2
4.	4 раздел. Иная контактная работа										
4.1.	Иная контактная работа	2								0,8	ОПК-4.2, ОПК-4.3
5.	5 раздел. Контроль										
5.1.	Зачет	2								4	ОПК-4.2, ОПК-4.3

5.1. Практические занятия

№ разд	Наименование раздела и темы практических занятий	Наименование и содержание практических занятий
1	Математические основы криптографии и криптоанализа	Математические основы криптографии и криптоанализа Концепция информационной безопасности. Нормативно-руководящие документы. Математические основы криптографии. Теория делимости, алгоритм Евклида, функция Эйлера. Сравнение и система вычетов. Модульная арифметика и дискретный логарифм. Асимметричные криптосистемы. Криптосистема RSA. Криптосистема Эль-Гамаля. Криптосистемы без передачи ключей.
1	Математические основы криптографии и криптоанализа	Криптосистема RSA Модульная арифметика и дискретный логарифм. Асимметричные криптосистемы. Криптосистема RSA.
1	Математические основы криптографии и криптоанализа	Криптосистема Эль-Гамаля Модульная арифметика и дискретный логарифм. Асимметричные криптосистемы. Криптосистема Эль-Гамаля.
2	1.2. Симметричные и асимметричные криптосистемы	Симметричные и асимметричные криптосистемы Современные практические приложения криптографических методов. Принципы и методы построения симметричных криптосистем.
2	1.2. Симметричные и асимметричные криптосистемы	Построение шифров подстановки и перестановки. Построение шифров подстановки. Шифры одноалфавитной замены. Шифры многоалфавитной замены. Построение шифров перестановки.
2	1.2. Симметричные и асимметричные криптосистемы	Основной шаг и базовые циклы криптопреобразований по ГОСТ 28147-89. Основной шаг и базовые циклы криптопреобразований по ГОСТ 28147-89. Режимы и схемы работы алгоритмов шифрования по ГОСТ 28147–89.
2	1.2. Симметричные и асимметричные криптосистемы	Аппаратно-программный комплекс криптографической защиты данных и ограничения доступа к ним КРИПТОН. Аппаратно-программный комплекс криптографической защиты данных и ограничения доступа к ним КРИПТОН. Несимметричные системы шифрования и их построение.
2	1.2. Симметричные и асимметричные криптосистемы	Алгоритм Диффи-Хеллмана. Алгоритм Диффи-Хеллмана.

3	1.3. Функции хеширования: назначение и использование	Хэш-функции: назначение и практическое использование. ГОСТ Р34.11–94 «Крипто-графическая защита информации. Функция хэширования». Функции хеширования: назначение и использование Хэш-функции: назначение и практическое использование. ГОСТ Р34.11–94 «Крипто-графическая защита информации. Функция хэширования». Важнейшие практически используемые стойкие хэш-функции.
3	1.3. Функции хеширования: назначение и использование	Важнейшие практически используемые стойкие хэш-функции Важнейшие практически используемые стойкие хэш-функции
4	2.1. ЭЦП: назначение и области применения	ЭЦП: назначение и области применения устный опрос, решение задачи, тесты
4	2.1. ЭЦП: назначение и области применения	Процедуры выработки и проверки подписи. Электронная цифровая подпись: сущность и варианты реализации. Процедуры выработки и проверки подписи.
5	2.2. Основные алгоритмы ЭЦП	2.2. Основные алгоритмы ЭЦП Наиболее известные алгоритмы электронной подписи. 2.2. Основные алгоритмы ЭЦП Наиболее известные алгоритмы электронной подписи: схема RSA, схема Эль-Гамаля, ГОСТ Р 34.10-2001/34.10-2012. Математические модели и программная реализация алгоритмов ЭЦП.
5	2.2. Основные алгоритмы ЭЦП	Основные алгоритмы ЭЦП. Схема RSA. Наиболее известные алгоритмы электронной подписи: схема RSA, схема Эль-Гамаля, ГОСТ Р 34.10-2001/34.10-2012. Математические модели и программная реализация алгоритмов ЭЦП.
5	2.2. Основные алгоритмы ЭЦП	ГОСТ Р 34.10-2001/34.10-2012. Наиболее известные алгоритмы электронной подписи: схема RSA, схема Эль-Гамаля, ГОСТ Р 34.10-2001/34.10-2012. Математические модели и программная реализация алгоритмов ЭЦП.
5	2.2. Основные алгоритмы ЭЦП	Математические модели и программная реализация алгоритмов ЭЦП. Наиболее известные алгоритмы электронной подписи: схема RSA, схема Эль-Гамаля, ГОСТ Р 34.10-2001/34.10-2012. Математические модели и программная реализация алгоритмов ЭЦП.
5	2.2. Основные алгоритмы ЭЦП	Наиболее известные алгоритмы электронной подписи: схема Эль-Гамаля Наиболее известные алгоритмы электронной подписи: схема RSA, схема Эль-Гамаля, ГОСТ Р 34.10-2001/34.10-2012. Математические модели и программная реализация алгоритмов ЭЦП.
6	2.3. Проблемы генерации ключей	Проблемы генерации ключей Проблемы генерации ключей Защита открытых ключей шифрования от подмены. Сертификация ключей шифрования. Центры сертификации. Формат электронных сертификатов. Расширения сертификатов. Отзыв сертификатов.
6	2.3. Проблемы генерации ключей	Сертификация ключей шифрования. Защита открытых ключей шифрования от подмены. Сертификация ключей шифрования. Центры сертификации. Формат электронных сертификатов. Расширения сертификатов. Отзыв сертификатов.

6	2.3. Проблемы генерации ключей	Формат электронных сертификатов Защита открытых ключей шифрования от подмены. Сертификация ключей шифрования. Центры сертификации. Формат электронных сертификатов. Расширения сертификатов. Отзыв сертификатов.
7	3.1. Частотный анализ.	Частотный анализ Частотный анализ. Полный перебор ключей Частотный и дифференциальный криптоанализ текста. Раскрытие простых подстановочных шифров. Характеристики метода.
7	3.1. Частотный анализ.	Полный перебор ключей. Характеристики метода. Частотный анализ. Полный перебор ключей Характеристики метода.
8	3.2. Криптоанализ симметричных и асимметричных шифров	Криптоанализ симметричных и асимметричных шифров Криптоанализ симметричных и асимметричных шифров Криптоанализ симметричных шифров. Криптоанализ асимметричных шифров. Атака по ключам. Метод «встречи посередине». Криптоанализ по побочным каналам. Крипто-анализ хэш-функций.
8	3.2. Криптоанализ симметричных и асимметричных шифров	Криптоанализ симметричных и симметричных шифров. Криптоанализ симметричных шифров. Криптоанализ асимметричных шифров. Атака по ключам. Метод «встречи посередине». Криптоанализ по побочным каналам. Крипто-анализ хэш-функций.
9	3.3. Сравнение методов криптоанализа	Сравнение методов криптоанализа 3.3. Сравнение методов криптоанализа Обзор и оценка методов криптоанализа. Нанотехнологии в криптоанализе.
9	3.3. Сравнение методов криптоанализа	Обзор и оценка методов криптоанализа. Сравнение методов криптоанализа Обзор и оценка методов криптоанализа.

5.2. Самостоятельная работа обучающихся

№ разд	Наименование раздела дисциплины и темы	Содержание самостоятельной работы
1	Математические основы криптографии и криптоанализа	Математические основы криптографии и криптоанализа изучение материала, подготовка к тестированию
2	1.2. Симметричные и асимметричные криптосистемы	Симметричные и асимметричные криптосистемы изучение материала, подготовка к тестированию
3	1.3. Функции хеширования: назначение и использование	Функции хеширования: назначение и использование изучение материала, подготовка к тестированию
4	2.1. ЭЦП: назначение и области применения	ЭЦП: назначение и области приме-нения изучение материала, подготовка к тестированию

5	2.2. Основные алгоритмы ЭЦП	Основные алгоритмы ЭЦП изучение материала, подготовка к тестированию
6	2.3. Проблемы генерации ключей	Проблемы генерации ключей изучение материала, подготовка к тестированию
7	3.1. Частотный анализ.	Частотный анализ. Полный перебор ключей изучение материала, подготовка к тестированию
8	3.2. Криптоанализ симметричных и асимметричных шифров	Криптоанализ симметричных и асимметричных шифров изучение материала, подготовка к тестированию
9	3.3. Сравнение методов криптоанализа	Сравнение методов криптоанализа изучение материала, подготовка к тестированию

6. Методические материалы для самостоятельной работы обучающихся по дисциплине (модулю)

Методические рекомендации по работе с конспектом лекций

Просмотрите конспект сразу после занятий. Пометьте материал конспекта лекций, который вызывает затруднения для понимания. Попытайтесь найти ответы на затруднительные вопросы, используя предлагаемую литературу. Если самостоятельно не удалось разобраться в материале, сформулируйте вопросы и обратитесь на текущей консультации или на ближайшей лекции за помощью к преподавателю.

Каждую неделю рекомендуется отводить время для повторения пройденного материала, проверяя свои знания, умения и навыки по контрольным вопросам.

Слушание и запись лекций – сложный вид вузовской аудиторной работы. Внимательное слушание и конспектирование лекций предполагает интенсивную умственную деятельность студента. Краткие записи лекций, их конспектирование помогает усвоить учебный материал. Конспект является полезным тогда, когда записано самое существенное, основное и сделано это самим студентом.

Не надо стремиться записать дословно всю лекцию. Такое «конспектирование» приносит больше вреда, чем пользы. Запись лекций рекомендуется вести по возможности собственными формулировками. Желательно запись осуществлять на одной странице, а следующую оставлять для проработки учебного материала самостоятельно в домашних условиях.

Конспект лекции лучше подразделять на пункты, параграфы, соблюдая красную строку. Этому в большой степени будут способствовать пункты плана лекции, предложенные преподавателям. Принципиальные места, определения, формулы и другое следует сопровождать замечаниями «важно», «особо важно», «хорошо запомнить» и т.п. Можно делать это и с помощью разноцветных маркеров или ручек.

Работая над конспектом лекций, всегда необходимо использовать не только учебник, но и ту литературу, которую дополнительно рекомендовал лектор. Именно такая серьезная, кропотливая работа с лекционным материалом позволит глубоко овладеть знаниями.

Методические рекомендации по подготовке к лабораторным работам

Лабораторные работы представляют одну из форм освоения теоретического материала с одновременным формированием практических навыков в изучаемой дисциплине. Их назначение – углубление проработки теоретического материала, формирование практических навыков путем регулярной и планомерной самостоятельной работы студентов на протяжении всего курса. Процесс подготовки к лабораторным работам включает изучение нормативных документов, обязательной и дополнительной литературы по рассматриваемому вопросу. Непосредственное проведение лабораторной работы предполагает:

- изучение теоретического материала по теме лабораторной работы (по вопросам изучаемой темы);
- выполнение необходимых расчетов и экспериментов;

оформление отчета с заполнением необходимых таблиц, построением графиков, подготовкой выводов по проделанным экспериментам и теоретическим расчетам;

- по каждой лабораторной работе проводится контроль: проверяется содержание отчета, проверяется усвоение теоретического материала. Контроль усвоения теоретического материала является индивидуальным.

Методические рекомендации по подготовке к зачету с оценкой

Студенты сдают зачеты в конце теоретического обучения. К зачету допускается студент, выполнивший в полном объеме задания, предусмотренные в рабочей программе. В случае пропуска каких-либо видов учебных занятий по уважительным или неуважительным причинам студент самостоятельно выполняет и сдает на проверку в письменном виде общие или индивидуальные задания, определяемые преподавателем.

Зачет по теоретическому курсу проходит в устной или письменной форме (определяется преподавателем) на основе перечня вопросов, которые отражают содержание действующей рабочей программы учебной дисциплины.

Студентам рекомендуется:

- внимательно прочитать вопросы к зачету;
- составить план ответа на каждый вопрос

7. Оценочные материалы для проведения текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине (модулю)

7.1. Перечень компетенций с указанием этапов их формирования в процессе освоения дисциплины

№ п/п	Контролируемые разделы дисциплины (модуля)	Код и наименование индикатора контролируемой компетенции	Вид оценочного средства
1	Математические основы криптографии и криптоанализа	ОПК-4.2, ОПК-4.3	устный опрос, решение задач
2	1.2. Симметричные и асимметричные криптосистемы	ОПК-4.2, ОПК-4.3	устный опрос, решение задачи
3	1.3. Функции хеширования: назначение и использование	ОПК-4.2, ОПК-4.3	устный опрос, решение задачи, тесты
4	2.1. ЭЦП: назначение и области применения	ОПК-4.2, ОПК-4.3	устный опрос, решение задачи, тесты
5	2.2. Основные алгоритмы ЭЦП	ОПК-4.2, ОПК-4.3	устный опрос, решение задачи, тесты
6	2.3. Проблемы генерации ключей	ОПК-4.2, ОПК-4.3	устный опрос, решение задачи, тесты
7	3.1. Частотный анализ.	ОПК-4.2, ОПК-4.3	устный опрос, решение задачи, тесты
8	3.2. Криптоанализ симметричных и асимметричных шифров	ОПК-4.2, ОПК-4.3	устный опрос, решение задачи, тесты
9	3.3. Сравнение методов криптоанализа	ОПК-4.3, ОПК-4.2	устный опрос, решение задачи, тесты
10	Иная контактная работа	ОПК-4.2, ОПК-4.3	
11	Зачет	ОПК-4.2, ОПК-4.3	

7.2. Типовые контрольные задания или иные материалы текущего контроля успеваемости, необходимые для оценки знаний, умений и навыков и (или) опыта профессиональной деятельности, характеризующих этапы формирования компетенций в процессе освоения дисциплины

Примерные задания для проверки сформированности индикаторов достижения компетенций ОПК-4.2, ОПК-4.3

Алгоритм шифрования на основе задачи об укладке ранца

В 1978 г. Меркль и Хеллман предложили использовать задачу об укладке ранца (рюкзака) для асимметричного шифрования. Она относится к классу NP-полных задач и формулируется следующим образом. Дано множество предметов различного веса. Спрашивается, можно ли положить некоторые из этих предметов в ранец так, чтобы его вес стал равен определенному значению? Более формально задача формулируется так: дан набор значений M1, M2, ..., Mn и суммарное значение S; требуется вычислить значения bi такие что

$S = b1M1 + b2M2 + ... + bnMn$,

где n – количество предметов;

bi - бинарный множитель. Значение bi = 1 означает, что предмет i кладут в рюкзак, bi = 0 - не кладут.

Например, веса предметов имеют значения 1, 5, 6, 11, 14, 20, 32 и 43. При этом можно упаковать рюкзак так, чтобы его вес стал равен 22, использовав предметы весом 5, 6 и 11. Невозможно упаковать рюкзак так, чтобы его вес стал равен 24.

В основе алгоритма, предложенного Мерклом и Хеллманом, лежит идея шифрования сообщения на основе решения серии задач укладки ранца. Предметы из кучи выбираются с помощью блока открытого текста, длина которого (в битах) равна количеству предметов в куче. При этом биты открытого текста соответствуют значениям b, а текст является полученным суммарным

весом. Пример шифрограммы, полученной с помощью задачи об укладке ранца, показан в следующей таблице.

Суть использования данного подхода для шифрования состоит в том, что на самом деле существуют две различные задачи укладки ранца - одна из них решается легко и характеризуется линейным ростом трудоемкости, а другая, как принято считать, нет. Легкий для укладки ранец можно превратить в трудный. Раз так, то можно применить в качестве открытого ключа трудный для укладки ранец, который легко использовать для шифрования, но невозможно - для дешифрования. А в качестве закрытого ключа применить легкий для укладки ранец, который предоставляет простой способ дешифрования сообщения.

В качестве закрытого ключа (легкого для укладки ранца) используется сверхвозрастающая последовательность. Сверхвозрастающей называется последовательность, в которой каждый последующий член больше суммы всех предыдущих. Например, последовательность {2, 3, 6, 13, 27, 52, 105, 210} является сверхвозрастающей, а {1, 3, 4, 9, 15, 25, 48, 76} - нет.

Решение для сверхвозрастающего ранца найти легко. В качестве текущего выбирается полный вес, который надо получить, и сравнивается с весом самого тяжелого предмета в ранце. Если текущий вес меньше веса данного предмета, то его в рюкзак не кладут, в противном случае его укладывают в рюкзак. Уменьшают текущий вес на вес положенного предмета и переходят к следующему по весу предмету в последовательности. Шаги повторяются до тех пор, пока процесс не закончится. Если текущий вес уменьшится до нуля, то решение найдено. В противном случае, нет.

Например, пусть полный вес рюкзака равен 270, а последовательность весов предметов равна {2, 3, 6, 13, 27, 52, 105, 210}. Самый большой вес – 210. Он меньше 270, поэтому предмет весом 210 кладут в рюкзак. Вычитают 210 из 270 и получают 60. Следующий наибольший вес последовательности равен 105. Он больше 60, поэтому предмет весом 105 в рюкзак не кладут. Следующий самый тяжелый предмет имеет вес 52. Он меньше 60, поэтому предмет весом 52 также кладут в рюкзак. Аналогично проходят процедуру укладки в рюкзак предметы весом 6 и 2. В результате полный вес уменьшится до 0. Если бы этот рюкзак был бы использован для дешифрования, то открытый текст, полученный из значения шифртекста 270, был бы равен 10100101.

Открытый ключ представляет собой не сверхвозрастающую (нормальную) последовательность. Он формируется на основе закрытого ключа и, как принято считать, не позволяет легко решить задачу об укладке ранца. Для его получения все значения закрытого ключа умножаются на число n по модулю m. Значение модуля m должно быть больше суммы всех чисел последовательности, например, 420 (2+3+6+13+27+52+105+210=418). Множитель n должен быть взаимно простым числом с модулем m, например, 31. Результат построения нормальной последовательности (открытого ключа) представлен в следующей таблице.

Таблица 2. Пример получения открытого ключа

Для шифрования сообщение сначала разбивается на блоки, по размерам равные числу элементов последовательности в рюкзаке. Затем, считая, что единица указывает на присутствие элемента последовательности в рюкзаке, а ноль — на его отсутствие, вычисляются полные веса рюкзаков – по одному рюкзаку для каждого блока сообщения.

В качестве примера возьмем открытое сообщение «АБРАМОВ», символы которого представим в бинарном виде в соответствии с таблицей кодов символов Windows 1251. Результат шифрования с помощью открытого ключа {62, 93, 186, 403, 417, 352, 315, 210} представлен в следующей таблице.

Таблица 3. Пример шифрования

Для расшифрования сообщения получатель должен сначала определить обратное число n-1, такое что (n * n-1) mod m = 1. В математике обратное число n-1 (обратное значение, обратная величина) - число, на которое надо умножить данное число n, чтобы получить единицу (n * n-1 = 1). Пара чисел, произведение которых равно единице, называются взаимно обратными. Например: 5 и 1/5, -6/7 и -7/6. Обратными числами по модулю m называются такие числа n и n-1, для которых справедливо выражение (n * n-1) mod m = 1. Для вычисления обратных чисел по модулю обычно используется расширенный алгоритм Евклида. После определения обратного числа каждое значение шифрограммы умножается на n-1 по модулю m и с помощью закрытого ключа определяются биты открытого текста.

В нашем примере сверхвозрастающая последовательность равна {2, 3, 6, 13, 27, 52, 105,

210}, m = 420, n = 31. Значение n-1 равно 271 (31*271 mod 420 = 1).

Таблица 4. Пример расшифрования

В своей работе авторы рекомендовали брать длину ключа, равную 100 (количество элементов последовательности).

Алгоритм Диффи-Хеллмана

Это способ шифрования, при котором два человека могут обмениваться зашифрованными сообщениями без всякого обмена секретными ключами.

Важным является то обстоятельство, что данная функция необратима. То есть, даже зная саму функцию и результат ее применения к переменной x, невозможно (или, по крайней мере очень сложно) найти исходное значение x.

В современных системах p >300 и a >100, что делает взлом ключа практически невозможным (за реальное время).

Основным недостатком асимметричных методов является их низкое быстродействие: данные алгоритмы в несколько тысяч раз медленнее симметричных. Поэтому на практике часто используют сочетание симметричных и асимметричных методов. В частности, текст шифруется быстродействующим симметричным алгоритмом; а секретный ключ, его сопровождающий, асимметричным алгоритмом.

Шифр Хилла

Это шифр замены (подстановки), но с использованием модульной арифметики и линейной алгебры.

Для шифрования используется матрица A с определителем, равным единице, т.е. ad-bc=1; для расшифровки – обратная матрица A-1.

Для большей надежности можно группировать буквы по 3 или по 4. И использовать матрицы размерности 3*3 или 4*4.

Алгоритм Диффи-Хеллмана

Это способ шифрования, при котором два человека могут обмениваться зашифрованными сообщениями без всякого обмена секретными ключами.

Важным является то обстоятельство, что данная функция необратима. То есть, даже зная саму функцию и результат ее применения к переменной x, невозможно (или, по крайней мере очень сложно) найти исходное значение x.

В современных системах p >300 и a >100, что делает взлом ключа практически невозможным (за реальное время).

Основным недостатком асимметричных методов является их низкое быстродействие: данные алгоритмы в несколько тысяч раз медленнее симметричных. Поэтому на практике часто используют сочетание симметричных и асимметричных методов. В частности, текст шифруется быстродействующим симметричным алгоритмом; а секретный ключ, его сопровождающий, асимметричным алгоритмом.

Шифр Хилла

Это шифр замены (подстановки), но с использованием модульной арифметики и линейной алгебры.

Для шифрования используется матрица A с определителем, равным единице, т.е. ad-bc=1; для расшифровки – обратная матрица A-1.

Для большей надежности можно группировать буквы по 3 или по 4. И использовать матрицы размерности 3*3 или 4*4

7.3. Система оценивания результатов обучения по дисциплине (модулю) при проведении текущего контроля успеваемости

Оценка «отлично» (зачтено)	знания: - систематизированные, глубокие и полные знания по всем разделам дисциплины, а также по основным вопросам, выходящим за пределы учебной программы; - точное использование научной терминологии, систематически грамотное и логически правильное изложение ответа на вопросы; - полное и глубокое усвоение основной и дополнительной литературы, рекомендованной рабочей программой по дисциплине (модулю) умения: - умеет ориентироваться в теориях, концепциях и направлениях дисциплины и давать им критическую оценку, используя научные достижения других дисциплин навыки: - высокий уровень сформированности заявленных в рабочей программе компетенций; - владеет навыками самостоятельно и творчески решать сложные проблемы и нестандартные ситуации; - применяет теоретические знания для выбора методики выполнения заданий; - грамотно обосновывает ход решения задач; - безупречно владеет инструментарием учебной дисциплины, умение его эффективно использовать в постановке научных и практических задач; - творческая самостоятельная работа на практических/семинарских/лабораторных занятиях, активно участвует в групповых обсуждениях, высокий уровень культуры исполнения заданий
Оценка «хорошо» (зачтено)	знания: - достаточно полные и систематизированные знания по дисциплине; - усвоение основной и дополнительной литературы, рекомендованной рабочей программой по дисциплине (модулю) умения: - умеет ориентироваться в основных теориях, концепциях и направлениях дисциплины и давать им критическую оценку; - использует научную терминологию, лингвистически и логически правильно излагает ответы на вопросы, умеет делать обоснованные выводы; - владеет инструментарием по дисциплине, умение его использовать в постановке и решении научных и профессиональных задач навыки: - самостоятельная работа на практических занятиях, участие в групповых обсуждениях, высокий уровень культуры исполнения заданий; - средний уровень сформированности заявленных в рабочей программе компетенций; - без затруднений выбирает стандартную методику выполнения заданий; - обосновывает ход решения задач без затруднений

Оценка «удовлетворительно» (зачтено)	знания: - достаточный минимальный объем знаний по дисциплине; - усвоение основной литературы, рекомендованной рабочей программой; - использование научной терминологии, стилистическое и логическое изложение ответа на вопросы, умение делать выводы без существенных ошибок умения: - умеет ориентироваться в основных теориях, концепциях и направлениях по дисциплине и давать им оценку; - владеет инструментарием учебной дисциплины, умение его использовать в решении типовых задач; - умеет под руководством преподавателя решать стандартные задачи навыки: - работа под руководством преподавателя на практических занятиях, допустимый уровень культуры исполнения заданий; - достаточный минимальный уровень сформированности заявленных в рабочей программе компетенций; - испытывает затруднения при обосновании алгоритма выполнения заданий
Оценка «неудовлетворительно» (не зачтено)	знания: - фрагментарные знания по дисциплине; - отказ от ответа (выполнения письменной работы); - знание отдельных источников, рекомендованных рабочей программой по дисциплине; умения: - не умеет использовать научную терминологию; - наличие грубых ошибок навыки: - низкий уровень культуры исполнения заданий; - низкий уровень сформированности заявленных в рабочей программе компетенций; - отсутствие навыков самостоятельной работы; - не может обосновать алгоритм выполнения заданий

7.4. Теоретические вопросы и практические задания для проведения промежуточной аттестации обучающихся, необходимые для оценки знаний, умений и навыков и (или) опыта профессиональной деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

7.4.1. Теоретические вопросы для проведения промежуточной аттестации обучающихся

Примерные теоретические вопросы для проведения промежуточной аттестации обучающихся

1. Криптография и криптоанализ: основные понятия и этапы развития
2. Математические основы криптографии
3. Теорема Ферма
4. Функция Эйлера
5. Расширенный алгоритм Евклида
6. Китайская теорема об остатках
7. Генерация простых чисел
8. Алгоритм быстрого возведения в степень по модулю
9. Элементарные шифры.
10. Потоковые шифры.
11. Блочные шифры.
12. Симметричные криптосистемы.
13. Алгоритмы шифрования DES и 3-DES.
14. Стандарт шифрования ГОСТ 28147-89.
15. Стандарт шифрования AES.

16. Основные режимы работы блочного симметричного алгоритма.
17. Особенности применения алгоритмов симметричного шифрования.
18. Асимметричные криптосистемы.
19. Алгоритм шифрования RSA.
20. Асимметричные криптосистемы на базе эллиптических кривых.
21. Алгоритм асимметричного шифрования ECES.
22. Функции хеширования: назначение и использование.
23. Отечественный стандарт хеширования ГОСТ Р 3411-94.
24. Нанотехнологии в криптоанализе.
25. Основные процедуры цифровой подписи.
26. Задача аутентификации и цифровая подпись.
27. Электронная подпись RSA.
28. Электронная подпись на базе шифра Эль-Гамаля.
29. Алгоритм цифровой подписи DSA.
30. Алгоритм цифровой подписи ECDSA.
31. Алгоритм цифровой подписи ГОСТ Р 34.10-94.
32. Отечественный стандарт цифровой подписи ГОСТ Р 34.10-2001.
33. Управление криптоключами.
34. Использование комбинированной криптосистемы.
35. Метод распределения ключей Диффи-Хеллмана.
36. Протокол вычисления ключа парной связи ECKEP.
37. Инфраструктура управления открытыми ключами PKI.
38. Принципы функционирования PKI.
39. Основные положения теории информации.
40. Хранение, измерение, обработка и передача информации.
41. Вероятностный подход к измерению информации.
42. Математические основы кодирования и декодирования.
43. Коды с исправлением и обнаружением ошибок.
44. Линейные коды.
45. Циклические коды.
46. Применение стеганографии в современных системах.
47. Основные методы встраивания скрытых данных.

7.4.2. Практические задания для проведения промежуточной аттестации обучающихся

2-й модуль: Электронная цифровая подпись

Вариант 1 (ОПК-2)

1. Построить подпись RSA для сообщения m при следующих параметрах:
P=3; Q=11; c=7; m=9.

Вариант 2 (ОПК-2)

2. Для указанного открытого ключа пользователя RSA проверить подлинность подписанных сообщений:

N=33; d=3; (10,14); (24,18); (10,18)

Вариант 3 (ОПК-3)

Сформировать и проверить ЭЦП Эль Гамаля при следующих начальных условиях (выдается преподавателем) :

P=11, G=2, секретный ключ X=8.

Вычисляем значение открытого ключа:

Y = GX mod P = Y = 28 mod 11 = 3.

Предположим, что исходному сообщению M соответствует хэш-значение m = 5.

Для того, чтобы вычислить цифровую подпись под сообщением M, имеющем хэш-значение m = 5, сначала выберем случайное целое число K = 9.

Далее вычисляем элементы a и b подписи:

a = GK mod P = 29 mod 11 = 6,

элемент b определяем, используя расширенный алгоритм Евклида:

m = (X * a + K * b) (mod (P – 1)).

При m = 5, a = 6, X = 8, K = 9, P = 11 получаем

5 = (6 * 8 + 9 * b)(mod 10)

или

9 * b º – 43 (mod 10).

Решая сравнение, получаем b = 3. Цифровая подпись представляет собой пару: a = 6, b = 3.

Далее отправитель передает подписанное сообщение. Приняв подписанное сообщение и открытый ключ Y = 3, получатель вычисляет хэш-значение для сообщения M : m = 5, а затем вычисляет два числа:

1) Yaab (mod P) = 36 * 63 (mod 11) =10 ;

2) Gm (mod P) = 25 (mod 11) =10.

Так как эти два целых числа равны, принятое получателем сообщение признается подлинным.

7.4.3. Примерные темы курсовой работы (проекта) (при наличии)

Курсовые работы (проекты) учебным планом не предусмотрены.

7.5. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта профессиональной деятельности, характеризующие этапы формирования компетенций

Процедура проведения промежуточной аттестации и текущего контроля успеваемости регламентируется локальным нормативным актом, определяющим порядок организации и проведения текущего контроля успеваемости и промежуточной аттестации обучающихся.

Процедура оценивания формирования компетенций при проведении текущего контроля приведена в п. 7.2.

Типовые контрольные задания или иные материалы текущего контроля приведены в п. 7.3.

Промежуточная аттестация по дисциплине проводится в форме зачета. Зачет проводится в форме компьютерного тестирования.

7.6. Критерии оценивания сформированности компетенций при проведении промежуточной аттестации

<table>
<tr><td rowspan="3">Критерии оценивания</td><td colspan="4">Уровень освоения и оценка</td></tr>
<tr><td>Оценка «неудовлетворительно»</td><td>Оценка «удовлетворительно»</td><td>Оценка «хорошо»</td><td>Оценка «отлично»</td></tr>
<tr><td>«не зачтено»</td><td colspan="3">«зачтено»</td></tr>
</table>

	Уровень освоения компетенции «недостаточный». Компетенции не сформированы. Знания отсутствуют, умения и навыки не сформированы	Уровень освоения компетенции «пороговый». Компетенции сформированы. Сформированы базовые структуры знаний. Умения фрагментарны и носят репродуктивный характер. Демонстрируется низкий уровень самостоятельности практического навыка.	Уровень освоения компетенции «продвинутый». Компетенции сформированы. Знания обширные, системные. Умения носят репродуктивный характер, применяются к решению типовых заданий. Демонстрируется достаточный уровень самостоятельности устойчивого практического навыка.	Уровень освоения компетенции «высокий». Компетенции сформированы. Знания аргументированные, всесторонние. Умения успешно применяются к решению как типовых, так и нестандартных творческих заданий. Демонстрируется высокий уровень самостоятельности, высокая адаптивность практического навыка
знания	Обучающийся демонстрирует: -существенные пробелы в знаниях учебного материала; -допускаются принципиальные ошибки при ответе на основные вопросы билета, отсутствует знание и понимание основных понятий и категорий; -непонимание сущности дополнительных вопросов в рамках заданий билета.	Обучающийся демонстрирует: -знания теоретического материала; -неполные ответы на основные вопросы, ошибки в ответе, недостаточное понимание сущности излагаемых вопросов; -неуверенные и неточные ответы на дополнительные вопросы.	Обучающийся демонстрирует: -знание и понимание основных вопросов контролируемого объема программного материала; - знания теоретического материала -способность устанавливать и объяснять связь практики и теории, выявлять противоречия, проблемы и тенденции развития; -правильные и конкретные, без грубых ошибок, ответы на поставленные вопросы.	Обучающийся демонстрирует: -глубокие, всесторонние и аргументированные знания программного материала; -полное понимание сущности и взаимосвязи рассматриваемых процессов и явлений, точное знание основных понятий, в рамках обсуждаемых заданий; -способность устанавливать и объяснять связь практики и теории, -логически последовательные, содержательные, конкретные и исчерпывающие ответы на все задания билета, а также дополнительные вопросы экзаменатора.

умения	При выполнении практического задания билета обучающийся продемонстрировал недостаточный уровень умений. Практические задания не выполнены Обучающийся не отвечает на вопросы билета при дополнительных наводящих вопросах преподавателя.	Обучающийся выполнил практическое задание билета с существенными неточностями. Допускаются ошибки в содержании ответа и решении практических заданий. При ответах на дополнительные вопросы было допущено много неточностей.	Обучающийся выполнил практическое задание билета с небольшими неточностями. Показал хорошие умения в рамках освоенного учебного материала. Предложенные практические задания решены с небольшими неточностями. Ответил на большинство дополнительных вопросов.	Обучающийся правильно выполнил практическое задание билета. Показал отличные умения в рамках освоенного учебного материала. Решает предложенные практические задания без ошибок Ответил на все дополнительные вопросы.
владение навыками	Не может выбрать методику выполнения заданий. Допускает грубые ошибки при выполнении заданий, нарушающие логику решения задач. Делает некорректные выводы. Не может обосновать алгоритм выполнения заданий.	Испытывает затруднения по выбору методики выполнения заданий. Допускает ошибки при выполнении заданий, нарушения логики решения задач. Испытывает затруднения с формулированием корректных выводов. Испытывает затруднения при обосновании алгоритма выполнения заданий.	Без затруднений выбирает стандартную методику выполнения заданий. Допускает ошибки при выполнении заданий, не нарушающие логику решения задач Делает корректные выводы по результатам решения задачи. Обосновывает ход решения задач без затруднений.	Применяет теоретические знания для выбора методики выполнения заданий. Не допускает ошибок при выполнении заданий. Самостоятельно анализирует результаты выполнения заданий. Грамотно обосновывает ход решения задач.

Оценка по дисциплине зависит от уровня сформированности компетенций, закрепленных за дисциплиной, и представляет собой среднее арифметическое от выставленных оценок по отдельным результатам обучения (знания, умения, владение навыками).

Оценка «отлично»/«зачтено» выставляется, если среднее арифметическое находится в интервале от 4,5 до 5,0.

Оценка «хорошо»/«зачтено» выставляется, если среднее арифметическое находится в интервале от 3,5 до 4,4.

Оценка «удовлетворительно»/«зачтено» выставляется, если среднее арифметическое находится в интервале от 2,5 до 3,4.

Оценка «неудовлетворительно»/«не зачтено» выставляется, если среднее арифметическое находится в интервале от 0 до 2,4.

8. Учебно-методическое и материально-техническое обеспечение дисциплины (модуля)

8.1. Перечень основной и дополнительной литературы, необходимой для освоения дисциплины (модуля)

№ п/п	Автор, название, место издания, издательство, год издания учебной и учебно-методической литературы	Количество экземпляров/электронный адрес ЭБС
	Основная литература	
1	Грибунин В. Г., Мартынов А. П., Николаев Д. Б., Фомченко В. Н., Астайкин А. И., Криптография и безопасность цифровых систем, Саров: Российский федеральный ядерный центр – ВНИИЭФ, 2011	http://www.iprbookshop.ru/60851.html
2	Романьков В. А., Алгебраическая криптография, Омск: Омский государственный университет им. Ф.М. Достоевского, 2013	http://www.iprbookshop.ru/24868.html
3	Гатченко Н. А., Исаев А. С., Яковлев А. Д., Криптографическая защита информации, Санкт-Петербург: Университет ИТМО, 2012	http://www.iprbookshop.ru/68658.html
4	Грибунин В. Г., Мартынов А. П., Николаев Д. Б., Фомченко В. Н., Астайкин А. И., Криптография и безопасность цифровых систем, Саров: Российский федеральный ядерный центр – ВНИИЭФ, 2011	https://www.iprbookshop.ru/60851.html
	Дополнительная литература	
1	Горюхина Е. Ю., Литвинова Л. И., Ткачева Н. В., Информационная безопасность, Воронеж: Воронежский Государственный Аграрный Университет им. Императора Петра Первого, 2015	http://www.iprbookshop.ru/72672.html
2	Романьков В. А., Алгебраическая криптография, Омск: Омский государственный университет им. Ф.М. Достоевского, 2013	http://www.iprbookshop.ru/24868.html
3	Фороузан Бехроуз, Берлин А. Н., Криптография и безопасность сетей, Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Вузовское образование, 2017	http://www.iprbookshop.ru/72337.html

Обучающиеся из числа инвалидов и лиц с ОВЗ обеспечиваются печатными и (или) электронными образовательными ресурсами в формах, адаптированных к ограничениям их здоровья.

8.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

Наименование ресурса сети «Интернет»	Электронный адрес ресурса
Основные понятия криптографии	https://intuit.ru/studies/courses/691/547/lecture/12371
История криптографии: от стеганографии до сложных алгоритмов	https://pikabu.ru/story/istoriya_kriptografii_ot_steganografii_do_slozhnyikh_algoritmov_chast_1_6108987
Эволюция криптографии: от математики до физики	https://tproger.ru/translations/understanding-cryptography/
Электронная цифровая подпись	https://www.e-notary.ru/vse-ob-elektronnoj-cifrovoj-podpisi/
Классический криптоанализ	https://habr.com/ru/post/271257/

8.3. Перечень современных профессиональных баз данных и информационных справочных систем

Наименование	Электронный адрес ресурса
Электронно-библиотечная система издательства "ЮРАЙТ"	https://www.biblio-online.ru/
Электронно-библиотечная система издательства "Лань"	https://e.lanbook.com/
Информационно-правовая система Консультант	\\law.lan.spbgasu.ru\ConsultantPlus ADM
Система дистанционного обучения СПбГАСУ Moodle	https://moodle.spbgasu.ru/

8.4. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного и свободно распространяемого программного обеспечения

Наименование	Способ распространения (лицензионное или свободно распространяемое)
Microsoft Windows 10 Pro	Договор № Д32009689201 от 18.12.2020г

8.5. Материально-техническое обеспечение дисциплины
Сведения об оснащенности учебных аудиторий и помещений для самостоятельной работы

Наименование учебных аудиторий и помещений для самостоятельной работы	Оснащенность оборудованием и техническими средствами обучения
47. Компьютерный класс	Рабочие места с ПК (стол компьютерный, системный блок, монитор, клавиатура, мышь), стол рабочий, подключение к компьютерной сети СПбГАСУ, выход в Internet.
47. Помещения для самостоятельной работы	Помещение для самостоятельной работы (читальный зал библиотеки, ауд. 217): ПК-23 шт., в т.ч. 1 шт.- ПК для лиц с ОВЗ (системный блок, монитор, клавиатура, мышь) с подключением к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду СПбГАСУ. ПО Microsoft Windows 10
47. Учебные аудитории для проведения лекционных занятий	Учебная аудитория для проведения занятий лекционного типа, комплект мультимедийного оборудования (персональный компьютер, мультимедийный проектор, экран, аудиосистема), доска маркерная белая эмалевая, экран, комплект учебной мебели, подключение к компьютерной сети СПбГАСУ, выход в Интернет.
47. Учебные аудитории для проведения практических занятий, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	Учебная аудитория для проведения практических занятий, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации – комплект мультимедийного оборудования (персональный компьютер, мультимедийный проектор, экран, аудиосистема), доска маркерная белая эмалевая, комплект учебной мебели, подключение к компьютерной сети СПбГАСУ, выход в Интернет.

Для инвалидов и лиц с ОВЗ обеспечиваются специальные условия для получения образования в соответствии с требованиями нормативно-правовых документов.