МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Ярославский государственный университет им. П.Г. Демидова

Кафедра компьютерных сетей

УТВЕРЖДАЮ
Декан факультета ИВТ
_____ Д.Ю. Чалый
«_24_» ___мая_____ 2022 г.

Рабочая программа дисциплины
«Математические методы защиты информации»

Направление подготовки
01.03.02 Прикладная математика и информатика

Направленность (профиль)
«Программирование и технологии искусственного интеллекта»

Квалификация выпускника
Бакалавр

Форма обучения
очная

Программа рассмотрена
на заседании кафедры
от 22 марта 2022 г.,
протокол № 7

Программа одобрена НМК
факультета ИВТ
протокол № 6 от
18 апреля 2022 г.

Ярославль

1. Цели освоения дисциплины

Целями дисциплины «Математические методы защиты информации» являются освоение теоретических основ современных методов защиты информации от несанкционированного доступа. Данный курс вырабатывает у студентов алгоритмическое мышление, умение применять основные концепции в области защиты информации.

2. Место дисциплины в структуре ОП бакалавриата

Дисциплина «Математические методы защиты информации» относится к вариативной части (дисциплина по выбору)ОП бакалавриата.

Для освоения данной дисциплиной студенты должны обладать знаниями по математике и информатике в объеме школьной программы, проявлять настойчивость, целеустремленность и инициативу в процессе обучения. Для выполнения программной реализации алгоритмов студенты должны иметь понятие хотя бы об одном из языков программирования.

Полученные в рамках дисциплины знания необходимыдля развития алгоритмического мышления, развития навыков решения сложных задач.

3. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения ОП бакалавриата

Процесс изучения дисциплины направлен на формирование следующих элементов компетенций в соответствии с ФГОС ВО, ОП 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**
Профессиональные компетенции		
ПК-1 Способен понимать, анализировать и совершенствовать данные современных научных исследований	ПК – 1.1 Обладает базовыми знаниями, полученными в области математических и/ или естественных наук, программирования и информационных технологий; ПК – 1.3 Владеет основными методами математического и алгоритмического моделирования	Знать: – методы защиты информации; – некоторые криптографические алгоритмы Уметь: – реализовывать некоторые криптографические алгоритмы – уметь выполнять передачу или генерацию ключей. Владеть навыками: – вычислять хэш значение; – создавать ЭЦП

4. Объем, структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 3 зач.ед., 108 акад.час.

№ 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.	Определение безопасности.	5	2	5				2	
2.	Шифрование. Симметричные шифры.	5	4	5		1		2	задания для самостоятельной работы
3.	Криптоанализ.	5	2	5		1		2	
4.	Асимметричные шифры. Электронные цифровые подписи	5	3	5		1		2	задания для самостоятельной работы Контрольная работа 1
5.	Поточные шифры	5	3	5		1		2	задания для самостоятельной работы
6.	Аутентикация, авторизация, пароли.	5	2	5				2	задания для самостоятельной работы
7.	Хэш-функции	5	2	6				2	задания для самостоятельной работы Контрольная работа 2
	Всего за 5 семестр		**0**	**36**		**4**		**14**	**Экзамен**
	Всего		**18**	**36**		**4**		**14**	

Содержание разделов дисциплины:

Раздел 1. Определение безопасности.

1.1. Определение информации, данных, знаний. Определение безопасности. Несанкционированный доступ. Информационные системы. Доступность, целостность, конфиденциальность.

1.2. Основные понятия об угрозах

Раздел 2. Шифрование. Симметричные шифры.

2.1. Шифрование. Терминология шифрования. Трудоемкость дешифрования. Симметричные шифры. Схема Фейстеля, SP-сеть. Режимы шифрования, гаммирование. Рюкзачная криптосистема

2.2. Алгоритмы AES, RC6, Гост 28147-89, DES, Serpent, Mars

Раздел 3. Криптоанализ.

3.1. Полный перебор. Частотный криптоанализ.

3.2. Дифференциальный и линейный криптоанализ.

Раздел 4. Асимметричные шифры. Электронные цифровые подписи

4.1. Асимметричные шифры, шифры с открытым ключом. Электронные цифровые подписи. Трудоемкость дешифрования.

4.2. Алгоритм RSA. Задача дискретного логарифмирования, задача разложения на множители. Малая теорема Ферма. Расширенный алгоритм Евклида. Алгоритм Рабина.
4.3. Алгоритм Эль-Гамаля. Подсознательный канал.

Раздел 5. Поточные шифры

5.1. Генераторы случайных и псевдослучайных чисел, их использование при аутентификации.
5.2. Криптографические ГПСЧ, их свойства. Виды поточных шифров. Трудоемкость дешифрования.
5.3. Генератор LFSR, и его модификации. Алгоритмы A5, RC4

Раздел 6. Аутентикация, авторизация, пароли.

Аутентикация, авторизация, пароли, токены, "рукопожатие". Протоколы аутентификации без передачи секретной информации, одноразовые ключи. Схема разделения секрета. Доказательство с нулевым зганием.

Раздел 7. Хэш-функции

7.1. Свойства криптографических хэш-функций. Их использование в протоколах аутентификации и для контроля изменения чувствительной информации.
7.2. Хэш-функции MD5, SHA1.

5. Образовательные технологии, используемые при осуществлении образовательного процесса по дисциплине

В процессе обучения используются следующие образовательные технологии:

Вводная лекция – дает первое целостное представление о дисциплине и ориентирует студента в системе изучения данной дисциплины. Студенты знакомятся с назначением и задачами курса, его ролью и местом в системе учебных дисциплин и в системе подготовки в целом. Дается краткий обзор курса, история развития науки и практики, достижения в этой сфере, имена известных ученых, излагаются перспективные направления исследований. На этой лекции высказываются методические и организационные особенности работы в рамках данной дисциплины, а также дается анализ рекомендуемой учебно-методической литературы.

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.

Практическое занятие – занятие, посвященное освоению конкретных умений и навыков и закреплению полученных на лекции знаний.

6. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного программного обеспечения и информационных справочных систем (при необходимости)

В процессе осуществления образовательного процесса используются:

– для формирования текстов материалов для промежуточной и текущей аттестации, для разработки документов, презентаций, для работы с электронными таблицами - программы OfficeStd 2013 RUS OLP NL Acdmc 021-10232, LibreOffice (свободное), издательская система LaTeX;

- компиляторы с высокоуровневых языков программирования;

– для поиска учебной литературы библиотеки ЯрГУ– Автоматизированная библиотечная информационная система "БУКИ-NEXT" (АБИС "Буки-Next").

7. Перечень основной и дополнительной учебной литературы, ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

а) основная:

1. Романьков, В. А., Введение в криптографию : курс лекций / В. А. Романьков, М., ФОРУМ, 2012, 239с

2. Мельников, В. П., Информационная безопасность и защита информации : учеб. пособие для вузов / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; под ред. С. А. Клейменова. - 4-е изд., стереотип., М., Академия, 2009, 331с

3. Запечников, С. В., Криптографические методы защиты информации : учеб. пособие для академического бакалавриата / С. В. Запечников, О. В. Казарин, А. А. Тарасов, М., Юрайт, 2016, 309с

4. Лось, А. Б., Криптографические методы защиты информации : учебник для академического бакалавриата / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков, М., Юрайт, 2016, 473с

5. Запечников, С. В., Криптографические методы защиты информации [Электронный ресурс] : учебник для академического бакалавриата / С. В. Запечников, О. В. Казарин, А. А. Тарасов, М., Юрайт, 2017, 309с https://biblio-online.ru/viewer/B27D8A2B-F86C-4F18-9F21-3E0695C0A4C0/kriptograficheskie-metody-zaschity-informacii#page/1

6. Математические методы защиты информации / Яросл. гос. ун-т. Ч. 2 [Электронный ресурс] : метод. указания (сост. М. В. Краснов), Ярославль, ЯрГУ, 2011, 44с http://www.lib.uniyar.ac.ru/edocs/iuni/20110407.pdf

7. Математические методы защиты информации / Яросл. гос. ун-т. Ч. 2 : метод. указания (сост. М. В. Краснов), Ярославль, ЯрГУ, 2011, 44с

8. Математические методы защиты информации / Яросл. гос. ун-т. Ч. 3 [Электронный ресурс] : метод. указания для студентов, обучающихся по направлению Прикладная математика и информатика (сост. М. В. Краснов), Ярославль, ЯрГУ, 2013, 47с http://www.lib.uniyar.ac.ru/edocs/iuni/20130406.pdf

9. Математические методы защиты информации / Яросл. гос. ун-т. Ч. 3 : метод. указания для студентов, обучающихся по направлению Прикладная математика и информатика (сост. М. В. Краснов), Ярославль, ЯрГУ, 2013, 47с

б) дополнительная:

1. Смарт, Н., Криптография / Н. Смарт ; пер. с англ., М., Техносфера, 2006, 528с

2. Краснов, М. В., Математические методы защиты информации : метод. указания / М. В. Краснов ; Яросл. гос. ун-т, Ярославль, ЯрГУ, 2004, 26с

в) ресурсы сети «Интернет»

- Ш.Т. Ишмухаметов, Р.Г. Рубцова Математические основы защиты информации, Из-во: КФУ, Казань 2012 132с (см. ресурс http://window.edu.ru/resource/128/78128)

Электронно-библиотечная система «Юрайт»(https://urait.ru/).

Электронно-библиотечная система «Лань»(https://e.lanbook.com/).

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

- специальные помещения:

-учебные аудитории для проведения занятий лекционного типа и практических занятий (семинаров);

- 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 в электронную информационно-образовательную среду организации.

Число посадочных мест в лекционной аудитории больше либо равно списочному составу потока, а в аудитории для практических занятий (семинаров)– списочному составу группы обучающихся.

- фонд библиотеки.

- компьютерная техника.

Автор(ы) :

Доцент кафедры компьютерных сетей, к.ф.-м.н. _____ М.В.Краснов

Приложение №1 к рабочей программе дисциплины
«Математические методы защиты информации»

Фонд оценочных средств
для проведения текущей и промежуточной аттестации студентов
по дисциплине

1. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

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

Все контрольные и самостоятельные работы формируют ПК-2

Задания для самостоятельной работы

Пример заданий для самостоятельной работы к разделу 2

Задания	Ответы:
1.Постройте аффинную криптосистему $f(x)=(ax+b)\bmod m$, для русского алфавита. Закодируйте слово «кокос»	Числовые значения могут отличаться от тех, которые приведены в данном решении Напомним, что аффинная криптосистема определяется тремя натуральными числами $a,b,m.$ Шифрование происходит заменой символа с порядковым номером x на символ порядковый номер которого вычисляется по формуле $f(x)=(ax+b)\bmod m.$ Заметим, что на пару чисел a и m наложено условие взаимной простоты. Закодируйте слово «кокос». Будем рассматривать $f(x)=(5x+2)\bmod 33.$ Нам надо закодировать $(11,15,11,15,18).$ В результате получим $(24,11,24,11,26).$
2. Взломайте аффинную криптосистему $f(x)=(ax+b)\bmod m$, для русского алфавита. Известно, что в исходном тексте чаще всего встречаются символы с порядковыми номерами 10 и 15, а в шифрованном тексте с порядковыми номерами 7 и 12.	Нам надо решить систему $\begin{cases}10a+b=7\bmod 33\\15a+b=12\bmod 33\end{cases}$ или $\begin{cases}10a+b=12\bmod 33\\15a+b=7\bmod 33\end{cases}$ Ответ $a=1¿b=30¿$ или $a=32¿b=22¿$
3. Выполните операцию умножения байтов в поле $GF(2^8)$, которая используется в алгоритме AES. x^7+x+1 и $x^6+x^4+x^2+x+1$	Алгоритм оперирует байтами, которые рассматриваются как элементы конечного поля $GF(2^8).$ Поскольку байты оперируют в поле $GF(2^8)$, то заданы операции сложения и умножения: • сложение - суть операция поразрядного XOR . • умножение - это операция умножения многочленов со взятием результата по модулю некоторого неприводимого многочлена $\phi(x)$ и использованием операции XOR при приведении подобных членов. В качестве неприводимого многочлена $\phi(x)=x^8+x^4+x^3+x+1$. Выполняем умножение $((x^7+x+1)*(x^6+x^4+x^2+x+1))¿\bmod(x^8+x^4+x^3+x+1)=¿=x^7+x^6+1.$
4. Примените процедуру MixColunms алгоритма AES к век-	Процедура MixColunms, одна из процедур используемых в раунде алгоритма AES.

тору $(e0, b4, 52, ae)$, результат запишите в виде четырехбайтового слова	Алгоритм оперирует байтами, которые рассматриваются как элементы конечного поля $GF(2^8)$. Поскольку байты оперируют в поле $GF(2^8)$, то заданы операции сложения и умножения: • сложение $\oplus$ - суть операция поразрядного XOR. • умножение- это операция умножения многочленов со взятием результата по модулю некоторого неприводимого многочлена $\phi(x)$ и использованием операции XOR при приведении подобных членов. В качестве неприводимого многочлена $\phi(x)=x^8+x^4+x^3+x+1$. Раундовые преобразования работают с четырехбайтовыми словами. Этому слову можно поставить в соответствие многочлен $a(x)=a_3x^3+a_2x^2+a_1x+a_0$, где $a_i \in GF(2^8)$. Рассмотрим как будет происходить сложение и умножение четырехбайтовых слов $a(x)$ и $b(x)$, где $a(x)=a_3x^3+a_2x^2+a_1x+a_0$, $b(x)=b_3x^3+b_2x^2+b_1x+b_0$: • сложение $a(x)+b(x)=(a_3 \oplus b_3)x^3+(a_2 \oplus b_2)x^2+(a_1 \oplus b_1)x+(a_0 \oplus b_0)$ • умножение $c(x)=a(x) \otimes b(x)=c_6x^6+c_5x^5+c_4x^4+c_3x^3+c_2x^2+c_1x+c_0$, Для того, чтобы результат умножения был снова представлен в виде четырехбайтового слова, его надо взять по модулю многочлена x^4+1. Следовательно, в результате получим вектор $d(x)=d_3x^3+d_2x^2+d_1x+d_0$ Процедура MixColunms алгоритма AES состоит из трех операций: • вектор записывается как многочлен вида $a(x)=a_3x^3+a_2x^2+a_1x+a_0$ • мы должны вычислить $d(x)=a(x) \otimes g(x)$, где $g(x)=\{03\}x^3+\{01\}x^2+\{01\}x+\{02\}$. • записать многочлен виде вектора Решение • вектор $(e0, b4, 52, ae)$, записываем как многочлен $a(x)=\{ae\}x^3+\{52\}x^2+\{b4\}x+\{e0\}$. • вычисляем $d(x)=a(x) \otimes g(x)$ • записываем ответ $(e0, cb, 19, 9a)$

Критерии оценивания

Номер задачи	Критерии	Шкала оценивания
1	*Уметь*: реализовывать некоторые криптографические алгоритмы	0 баллов – студент полностью неверно решил задачу 1 балл – студент верно решил задачу, но не привел пояснений к ходу решения или допустил одну вычислительную ошибку. 2 балла – студент полностью разобрался в решении задачи
2	*Уметь*: реализовывать некоторые криптографические алгоритмы	0 баллов – студент полностью неверно решил задачу

		2 балла – студент полностью разобрался в решении задачи
3	*Уметь*: реализовывать некоторые криптографические алгоритмы	0 баллов – студент полностью неверно решил задачу 1 балл – студент верно решил задачу, но не привел пояснений к ходу решения или допустил вычислительную ошибку. 2 балла – студент полностью разобрался в решении задачи
4	*Уметь*: реализовывать некоторые криптографические алгоритмы	0 баллов – студент полностью неверно решил задачу 1 балл – студент верно решил задачу, но не привел пояснений к ходу решения или допустил вычислительную ошибку. 2 балла – студент полностью разобрался в решении задачи

Набранное количество баллов соответствует оценке за выполнение работы:
- менее 4 баллов — оценка «неудовлетворительно» компетенция не сформирована;
- от 4 до 5 баллов — оценка «удовлетворительно», пороговый уровень формирования компетенции;
- от 6 до 7 баллов — оценка «хорошо», продвинутый уровень формирования компетенции;
- 8 баллов — оценка «отлично», высокий уровень формирования компетенции.

Пример заданий для самостоятельной работы к разделу 4

Задания	Ответы:
1. Вычислить $\begin{cases} x \equiv 1 \mod 3 \\ x \equiv 2 \mod 5 \\ x \equiv 3 \mod 7 \\ x \equiv 3 \mod 11 \\ x \equiv 7 \mod 13 \end{cases}$	Напомним процесс вычисления. Пусть задано: множество натуральных чисел $(m_1, m_2, \ldots, m_k)$ не равных единице, которые являются попарно взаимно простыми множество натуральных чисел $(b_1, b_2, \ldots, b_k)$. Система сравнений $\begin{cases} x \equiv b_1 \mod m_1 \\ \ldots \\ x \equiv b_k \mod m_k \end{cases}$ имеет решение $x = x_0 ¿ \mod(m_1 m_2 \ldots m_k); ¿$ где $x_0 = M_1 M_1' b_1 + \ldots + M_k M_k' b_k;$ числа M_s и M_s определяется из условий $m_1 m_2 \ldots m_k = M_s m_s,$ $M_s M_s' = 1 ¿ \mod m_s ¿$ Рассмотрим наше уравнение $M_1 = 5005, M_2 = 3003, M_3 = 2145, M_4 = 1365, M_5 = 1155.$ $M_1' = 1, M_2' = 2, M_3' = 5, M_4' = 1, M_5' = 6.$ $m_1 m_2 \ldots m_5 = 15015$ $x_0 = 5005*1*1 + 3003*2*2 + 2145*5*3 +$ $+1365*3*1 + 1155*6*7 = 101797$ $x = 11707$
2.Построить криптосистему Эль-Гамаля и закодируйте число 7	Числовые значения могут отличаться от тех, которые приведены в данном решении Криптосистема Эль-Гамаля строится следующим образом: • сначала выбирается большое простое число p • выбирается число g которое является примитивным

	для Z_p • выбирается случайное натуральное число x, причем $x<p$ • вычисляем $y=g^x \bmod p$ Для того чтобы зашифровать сообщение M надо выполнить следующие действия: • выбрать случайное натуральное число k,¿$1<k<p-1$,¿ такое что числа k и $p-1$ взаимно простые. • вычислить $a=g^k \bmod p$ и $b=(y^k M) \bmod p$. Пара чисел (a,b) и есть шифрованный текст Для того чтобы расшифровать сообщение, надо вычислить $M=\frac{b}{a^x} \bmod p$. Построим криптосистему Эль-Гамаля и закодируем число 7 Строим криптосистему • выбираем $p=13$; $g=2$; выбираем секретный ключ $x=8$. • вычисляем $y=2^8 \bmod 13=9$ Для того чтобы зашифровать сообщение $M=7$ надо выполнить следующие действия: • выбрать случайное натуральное число $k=7$ заметим, что числа 7 и 12 взаимно простые. • вычислить $a=2^7 \bmod 13=11$ и $b=(9^7*7) \bmod 13=11$. Шифрованный текст – пара чисел $(11,11)$
3. Сформулировать алгоритм установки ЭЦП DSA. Дан текст с хэш значением равным 7. Выполните установку ЭЦП DSA	Числовые значения могут отличаться от тех, которые приведены в данном решении Схема DSA строится следующим образом: • сначала выбирается большое простое число p • выбирается простое число q которое является делителем $p-1$ • выбирается натуральное число t, которое $0<t<p$. . Если число $t^{\frac{p-1}{q}}=1 \bmod p$, то выбираем другое число t. В противном случае $g=t^{\frac{p-1}{q}} \bmod p$. • выбирается натуральное число x, которое является секретным ключом причем $1<x<q$ • вычисляем $y=g^x \bmod p$ Установка подписи: • проверяем выполняется ли условие для хэш значение m текста M, что $0<m<q$ • выбирается натуральное число k,¿$(0<k<q)$.¿ • вычисляем k^{-1}, для которого выполняется условие $k*k^{-1}=1 \bmod q$

	• вычисляем два числа r и s по следующим правилам: $r=(g^k \bmod p) \bmod q$ и $s=k^{-1}(xr+m) \bmod q$ Если не выполняются условия $0<r<q, 0<s<q$ поменяйте входные параметры. Подписью является пара чисел (r,s) Проверка подписи Предположим, что к нам пришло сообщение M' с хэш значением m' и подписью (r',s') • если хотя бы одно из условий $0<r'<q, 0<s'<q$ не выполняется, то подпись считается недействительной • вычисляем $v=(s')^{-1} \bmod q$ • вычисляем: $z_1=(m'v) \bmod q$ $z_2=(r'v) \bmod q$ $u=((g^{z_1} y^{z_2}) \bmod p) \bmod q$ • проверяем условие $r'=u$. Если оно выполняется то подпись считается подлинной а сообщение –неизмененным. Дан текст с хэш значением равным 7. Выполните установку ЭЦП DSA. Строим схему DSA • выбираем $p=23, q=11, t=3$ • вычисляем $g=3^2 \bmod 23=9$ • выбираем $x=2$ • вычисляем $y=9^2 \bmod 23=12$ Установка подписи: • выбираем $k=4$ • вычисляем: $k^{-1}=3$, $r=(9^4 \bmod 23) \bmod 11=6$, $s=(3*(2*6+7)) \bmod 11=2$ Подписью является пара чисел $(6,2)$
4. Применяя расширенный алгоритм Евклида: а) найти d,x,y для которых выполняется $d=НОД(a,b)=ax+by$, где a=342; b=612 b) найти q для которого выполняется $8q \bmod 101=1$	а) 18=342*9+612*(-5), следовательно $d=18, x=9, y=-5$ b) После применении расширенного алгоритма Евклида $d=НОД(a,b)=ax+by$, где $a=101, b=8$. Мы получим: $1=НОД(101,8)=101*(-3)+8*38$, возьмем указанное выражение по модулю 101. В результате $(101*(-3)+8*38) \bmod 101 \Rightarrow (8*38) \bmod 101 \Rightarrow q=38$

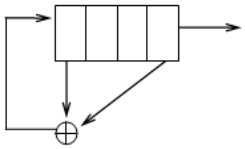
Критерии оценивания

Номер задачи	Критерии	Шкала оценивания
1	*Уметь:* реализовывать некоторые криптографические алгоритмы.	0 баллов – студент полностью неверно решил задачу

	Владеть навыками: создавать ЭЦП.	1 балл – студент верно решил задачу, но не привел пояснений к ходу решения или допустил вычислительную ошибку. 2 балла – студент полностью разобрался в решении задачи
2	*Уметь:* реализовывать некоторые криптографические алгоритмы. *Владеть навыками:* создавать ЭЦП.	0 баллов – студент полностью неверно решил задачу 1 балл – студент верно решил задачу, но не привел пояснений к ходу решения или допустил вычислительную ошибку. 2 балла – студент полностью разобрался в решении задачи
3	*Уметь:* реализовывать некоторые криптографические алгоритмы. *Владеть навыками:* создавать ЭЦП.	0 баллов – студент полностью неверно решил задачу 1 балл – студент верно решил задачу, но не привел пояснений к ходу решения или допустил вычислительную ошибку. 2 балла – студент полностью разобрался в решении задачи
4	*Уметь:* реализовывать некоторые криптографические алгоритмы. *Владеть навыками:* создавать ЭЦП.	0 баллов – студент полностью неверно решил задачу 1 балл – студент верно решил только одну подзадачу. 2 балла – студент полностью разобрался в решении задачи

Набранное количество баллов соответствует оценке за выполнение работы:
- менее 4 баллов — оценка «неудовлетворительно» компетенция несформирована;
- от 4 до 5 баллов — оценка «удовлетворительно», пороговый уровень формирования компетенции;
- от 6 до 7 баллов — оценка «хорошо», продвинутый уровень формирования компетенции;
- 8 баллов — оценка «отлично», высокий уровень формирования компетенции.

Пример заданий для самостоятельной работы к разделу 5

<table>
<tr><th>Задания</th><th>Ответы:</th></tr>
<tr><td>1. Постройте регистр сдвига с линейной обратной связью с ассоциированным многочленом x^4+x+1 и выпишем состояние регистра, если он был инициализирован вектором $(1,1,1,1)$.</td><td>

<table>
<tr><th colspan="2">Состояние регистра</th><th>выход</th><th colspan="2">Состояние регистра</th><th>выход</th></tr>
<tr><th>итерация</th><th>состояние рег. стало</th><th></th><th>итерация</th><th>состояние рег. стало</th><th></th></tr>
<tr><td>0</td><td>1111</td><td></td><td>9</td><td>0100</td><td>1</td></tr>
<tr><td>1</td><td>0111</td><td>1</td><td>10</td><td>0010</td><td>0</td></tr>
<tr><td>2</td><td>1011</td><td>1</td><td>11</td><td>0001</td><td>0</td></tr>
<tr><td>3</td><td>0101</td><td>1</td><td>12</td><td>1000</td><td>1</td></tr>
<tr><td>4</td><td>1010</td><td>1</td><td>13</td><td>1100</td><td>0</td></tr>
<tr><td>5</td><td>1101</td><td>0</td><td>14</td><td>1110</td><td>0</td></tr>
<tr><td>6</td><td>0110</td><td>1</td><td>15</td><td>1111</td><td>0</td></tr>
<tr><td>7</td><td>0011</td><td>0</td><td></td><td></td><td></td></tr>
<tr><td>8</td><td>1001</td><td>1</td><td></td><td></td><td></td></tr>
</table>
</td></tr>
<tr><td>2. Постройте 10 битную псевдослучайную</td><td>Числовые значения могут отличаться от тех, которые</td></tr>
</table>

последовательность с помощью BBS-генератора.

приведены в данном решении

Напомним, что BBS-генератор строится следующим образом:

- вначале выбираются p и q - два больших простых числа примерно одинакового размера, причем $p \equiv 3 \bmod 4$ и $q \equiv 3 \bmod 4$.
- вычисляем число $n = pq$;
- выбираем случайное целое число x, что числа x и n являются взаимно простыми;
- вычисляем число $x_0 = x^2 \bmod n$, которое называется стартовым числом генератора;
- искомой последовательностью бит длиной m будет являться последовательность

$$BBS_{n,m}(x_0) = b_0 b_1 b_2 \ldots b_i \ldots b_{m-1}, \quad i = 0, \ldots, m-1,$$

где b_i - младший бит числа x_i, $x_{i+1} = x_i^2 \bmod n$.

Постройте 10 битную псевдослучайную последовательность

- Пусть $p = 11$, $q = 19$, тогда $n = 209$. Пусть $x = 2$.
- Стартовое число генератора $x_0 = x^2 \bmod n \Rightarrow$ $x_0 = 2^2 \bmod 209 \Rightarrow$ $x_0 = 4$.
- В качестве элементов псевдослучайной последовательности будем брать младший бит в двоичной записи чисел $x_{i+1} = x_i^2 \bmod n$

  В результате получим последовательность $BBS_{209,10}(4) = 0011010001$

3. Создайте комбинирующий генератор, состоящий из двух регистров сдвига с линейной обратной связью.

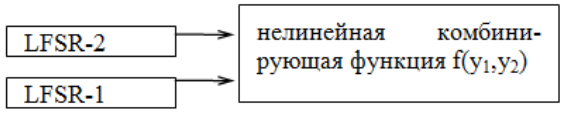
Первый регистр с ассоциированным многочленом $x^6 + x + 1$, он был инициализирован вектором $(1,1,1,1,1,1)$. Выход регистра y_1.

Второй регистр с ассоциированным многочленом $x^4 + x + 1$ он был инициализирован вектором $(1,1,1,1)$. Выход регистра y_2.

В качестве комбинирующей функции возьмем $f(y_1, y_2) = y_1 \oplus y_2$

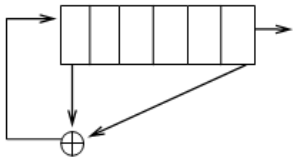
Постройте 7 битную псевдослучайную последовательность

Напомним, что комбинирующий генератор проиллюстрировать следующей схемой



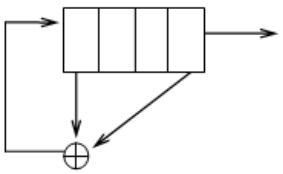
Решение

- Первый регистр



Состояние регистра		выход	Состояние регистра		выход
итерация	состояние рег. стало	y_1.	итерация	состояние рег. стало	y_1.
0	111111		4	101011	1
1	011111	1	5	010101	1
2	101111	1	6	101010	1
3	010111	1	7	110101	0

- Второй регистр



Состояние регистра		выход	Состояние регистра		выход
итерация	состояние рег. стало	y_2.	итерация	состояние рег. стало	y_2.
0	1111		4	1010	1
1	0111	1	5	1101	0
2	1011	1	6	0110	1
3	0101	1	7	0011	0

В результате получим последовательность 0000100

4. Создайте сжимающий генератор, состоящий из двух регистров сдвига с линейной обратной связью.

Первый регистр с ассоциированным многочленом x^6+x+1, он был инициализирован вектором $(1,1,1,1,1,1)$. Выход регистра b_i.

Второй регистр с ассоциированным многочленом x^4+x+1 он был инициализирован вектором $(1,1,1,1)$. Выход регистра c_i.

Постройте 7 битную псевдослучайную последовательность

Напомним, что сжимающий генератор описывается следующей образом:

Используется 2 регистра с линейной обратной связью. Тактовые импульсы поступают на оба LFSR. Предположим, что

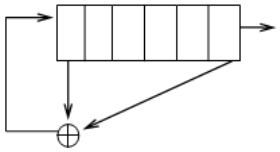
$b=b_0 b_1 b_2 \ldots$ последовательность с выхода LFSR1.

$c=c_0 c_1 c_2 \ldots$ - последовательность с выхода LFSR2,

Тогда результирующая последовательность $z=z_0 z_1 z_2 \ldots$ включает в себя те биты b_i, для которых соответствующие биты $c_i=1$. Остальные биты последовательности b игнорируются.

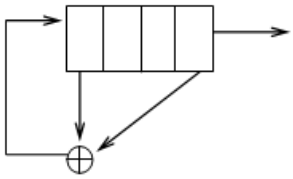
Решение

• Первый регистр



Состояние регистра		выход	Состояние регистра		выход
итерация	состояние рег. стало	b_i	итерация	состояние рег. стало	b_i
0	111111		5	010101	1
1	011111	1	6	101010	1
2	101111	1	7	110101	0
3	010111	1	8	011010	1
4	101011	1	9	001101	0

• Второй регистр



Состояние регистра		выход	Состояние регистра		выход
итерация	Состояние рег. стало	c_i	итерация	состояние рег. стало	c_i
0	1111		5	1101	0
1	0111	1	6	0110	1

2	1011	1	7	0011	0
3	0101	1	8	1001	1
4	1010	1	9	0100	1

В результате получим последовательность 1111110

Критерии оценивания

Номер задачи	Критерии	Шкала оценивания
1	*Уметь*: реализовывать некоторые криптографические алгоритмы.	0 баллов – студент полностью неверно решил задачу 1 балл – студент верно решил задачу, но не привел пояснений к ходу решения. 2 балла – студент полностью разобрался в решении задачи
2	*Уметь*: реализовывать некоторые криптографические алгоритмы.	0 баллов – студент полностью неверно решил задачу 1 балл – студент верно решил задачу, но не привел пояснений к ходу решения. 2 балла – студент полностью разобрался в решении задачи
3	*Уметь*: реализовывать некоторые криптографические алгоритмы.	0 баллов – студент полностью неверно решил задачу 1 балл – студент верно решил задачу, но не привел пояснений к ходу решения. 2 балла – студент полностью разобрался в решении задачи
4	*Уметь*: реализовывать некоторые криптографические алгоритмы.	0 баллов – студент полностью неверно решил задачу 1 балл – студент верно решил задачу, но не привел пояснений к ходу решения. 2 балла – студент полностью разобрался в решении задачи

Набранное количество баллов соответствует оценке за выполнение работы:
- менее 4 баллов — оценка «неудовлетворительно» компетенция не сформирована;
- от 4 до 5 баллов — оценка «удовлетворительно», пороговый уровень формирования компетенции;
- от 6 до 7 баллов — оценка «хорошо», продвинутый уровень формирования компетенции;
- 8 баллов — оценка «отлично», высокий уровень формирования компетенции

Пример заданий для самостоятельной работы к разделу 6

Задания	Ответы:
1.Приведите пример работы протокола типа «точка-точка» Предположим, что пользователи A и обладают общей секретной информацией (секретным ключом k_{AB}).	Два варианта ответа: 1. передачу сеансового ключа можно описать следующей символьной записью: $A \rightarrow B: \quad E_{k_{AB}}(k, T, b),$ которая означает, что пользователь A создал сеансовый ключ k и отправил пользователю B сообщение $E_{k_{AB}}(k, T, b),$

	где $E_{k_{AB}}$ - алгоритм шифрования с ключом k_{AB}, - сеансовый ключ, $T-$ временная метка, b -идентификатор пользователя B. Зная секретный ключ k_{AB} пользователь B легко может найти ключ k. 2. Если дополнительно требуется аутентификация сеанса, то можно использовать протокол, состоящий из следующих действий: a) $B \rightarrow A: \quad r_B$ b) $A \rightarrow B: \quad E_{k_{AB}}(k, r_B, T, b)$ где запись $B \rightarrow A: \quad r_B$ означает, что пользователь B сгенерировал случайное число r_B и отправил его пользователю A; запись $A \rightarrow B: \quad E_{k_{AB}}(k, r_B, T, b)$ означает, что пользователь A создал сеансовый ключ k и отправил пользователю B сообщение $E_{k_{AB}}(k, r_B, T, b)$ где $E_{k_{AB}}$ - алгоритм шифрования с ключом k_{AB}, - сеансовый ключ, $T-$ временная метка, b -идентификатор пользователя B. Зная секретный ключ k_{AB} пользователь B легко может найти ключ k, а по числу r_B убедиться, что его послал пользовать A.
2. Есть два пользователя A и B используя протокол DIFFIE-HELLMAN сгенерируйте общий секретный ключ	Числовые значения могут отличаться от тех, которые приведены в данном решении 1.Пользователи A и B выбирают в открытом доступе большое простое число n и g, где g образующий элемент мультипликативной группы $Z_n^{¿}$. Пусть $n=13$ и $g=2$ 2. Пользователь A выбирает случайное большое натуральное число x и отправляет пользователю B величину $X=g^x \bmod ¿ n ¿$; Пусть $x=5$ и $X=6$ 3. Пользователь B выбирает случайное большое натуральное число y и отправляет пользователю A величину $Y=g^y \bmod ¿ n ¿$; Пусть $y=7$ и $Y=11$ 4. Пользователь A вычисляет величину $k=Y^x \bmod ¿ n ¿$; Вычисляем $k=11^5 \bmod ¿ 13=7 ¿$ 5. Пользователь B вычисляет величину $\tilde{k}=X^y \bmod ¿ n ¿$. Вычисляем $\tilde{k}=6^7 \bmod ¿ 13=7 ¿$ Получили $\tilde{k}=k=7$
3. Есть два пользователя A и B используя протокол MTI сгенерируйте общий секретный ключ	Числовые значения могут отличаться от тех, которые приведены в данном решении 1.Пользователи A и B выбирают в открытом доступе большое простое число n и g, где g образующий элемент мультипликативной группы $Z_n^{¿}$. Пусть $n=13$ и $g=2$ 2. Пользователи A и B должны сгенерировать секретные

	ключи a, $1 \le a \le n-2$, и b, $1 \le b \le n-2$, соответственно, и публикуют свои открытые ключи $z_A = g^a \bmod n$ и $z_B = g^b \bmod n$; Пусть Пользователь A генерирует число $a=5$ и публикует $z_A = 2^5 \bmod 13 = 6$, соответственно пользователь B генерирует число $b=3$ и публикует $z_B = 2^3 \bmod 13 = 8$; 3. Пользователь A выбирает случайное натуральное число x , $1 \le x \le n-2$ и отправляет пользователю B величину $X = g^x \bmod ¿ n ¿$; Пусть пользователь A генерирует число $x=2$ и отправляет пользователю B величину $X = 2^2 \bmod ¿ 13 = 4 ¿$; 4. Пользователь B выбирает случайное большое натуральное число y , $1 \le y \le n-2$ и отправляет пользователю A величину $Y = g^y \bmod ¿ n ¿$; Пусть пользователь B генерирует число $y=4$ и отправляет пользователю величину $Y = 2^4 \bmod ¿ 13 = 3 ¿$; 5. Пользователь A вычисляет величину $k = Y^a z_B^x \bmod n$; Пусть пользователь A на настоящий момент знает величины: $n, g, a, z_A, z_B, x, X, Y$. Пользователь A вычисляет величину $k = \left(Y^a z_B^x\right) \bmod ¿ n = ¿$ $\left(3^5 8^2\right) \bmod 13 =$ $(9*12) \bmod 13 = 4$ 6. Пользователь B вычисляет величину $\tilde{k} = X^b z_A^y \bmod n.$ Пусть пользователь B на настоящий момент знает величины: $n, g, b, z_A, z_B, y, X, Y$. Пользователь B вычисляет величину $\tilde{k} = \left(X^b z_A^y\right) \bmod ¿ n = ¿$ $\left(4^3 6^4\right) \bmod ¿ 13 = ¿$ $12*9 \bmod ¿ 13 = 4 ¿$ Получили $\tilde{k} = k = 4$
4. Постройте схему разделения секрета на примере пороговой схемы Шамира (n,t); где $n=5, t=3$. В качестве конечного поля возьмем Z_{13} , секретной информацией будем считать число 11	Числовые значения могут отличаться от тех, которые приведены в данном решении Схема разделения секрета включает два протокола: • протокол формирования частичных секретов и распределения их между пользователями; • протокол восстановления секрета группой пользователей. В качестве примера рассмотрим пороговую схему Шамира. Для построения пороговой схемы (n,t) Шамир воспользовался многочленами вида $f(x) = b_{t-1} x^{t-1} + b_{t-2} x^{t-2} + \ldots + b_1 x + b_0$ в конечном поле. Секретным считается свободный член b_0 . В качестве конечного поля возьмем Z_{13} , а в качестве многочлена, на котором основана схема Шамира $(5,3)$; возьмем $f(x) = \left(7x^2 + 8x + 11\right) ¿ ¿$. • протокол формирования частичных секретов состоит в вычислении $f(x)$ $a_1 = f(1) = (7+8+11) \bmod ¿ 13 = 0 ¿$; $a_2 = f(2) = (28+16+11) \bmod ¿ 13 = 3 ¿$; $a_3 = f(3) = (63+24+11) \bmod ¿ 13 = 7 ¿$; $a_4 = f(4) = (112+32+11) \bmod ¿ 13 = 12 ¿$;

	$a_5=f(5)=(175+40+11)\bmod ¿13=5¿$. • протокол восстановления секрета группой пользователей из t человек. Чтобы восстановить $f(x)$ из трех частичных секретов. Будем считать, что нам дано a_2, a_3, a_5 тогда решается система линейных уравнений: ¿ ¿ Решением будет $b_2=7, b_1=8, b_0=11$.

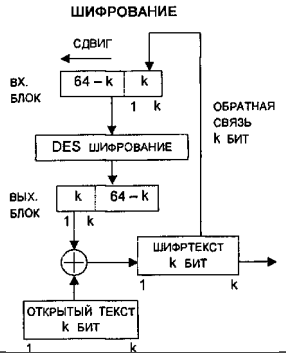
Критерии оценивания

Номер задачи	Критерии	Шкала оценивания
1	*Уметь:* выполнять передачу или генерацию ключей.	0 баллов – студент полностью не верно решил задачу 1 балл – студент верно решил задачу, но не привел пояснений к ходу решения. 2 балла – студент полностью разобрался в решении задачи
2	*Уметь:* выполнять передачу или генерацию ключей.	0 баллов – студент полностью неверно решил задачу 1 балл – студент верно решил задачу, но не привел пояснений к ходу решения или была допущена вычислительная ошибка. 2 балла – студент полностью разобрался в решении задачи
3	*Уметь:* выполнять передачу или генерацию ключей.	0 баллов – студент полностью неверно решил задачу 1 балл – студент верно решил задачу, но не привел пояснений к ходу решения или была допущена вычислительная ошибка. . 2 балла – студент полностью разобрался в решении задачи
4	*Уметь:* выполнять передачу или генерацию ключей.	0 баллов – студент полностью не верно решил задачу 1 балл – студент верно решил задачу, но не привел пояснений к ходу решения или была допущена вычислительная ошибка. . 2 балла – студент полностью разобрался в решении задачи

Набранное количество баллов соответствует оценке за выполнение работы:
- менее 4 баллов — оценка «неудовлетворительно»;
- от 4 до 5 баллов — оценка «удовлетворительно», пороговый уровень формирования компетенции;
- от 6 до 7 баллов — оценка «хорошо», продвинутый уровень формирования компетенции;
- 8 баллов — оценка «отлично», высокий уровень формирования компетенции.

Пример заданий для самостоятельной работы к разделу 7

Задания	Ответы:
1.Дайте определение хэш-функции	Хэш-функция h — это функция, определенная на битовых строках произвольной длины со значениями в строках битов фиксированной длины.. Хэш-функция h() принимает в качестве аргумента сообщение (документ) M произвольной длины и возвращает хэш-значение h(M) = H фиксированной длины. Предполагается, что алгоритм вычисления хэш-значения является эффективным и общедоступным.
2.Укажите, каким условиям должна удовлетворять хэш-функция	Хэш-функция должна удовлетворять целому ряду условий: • хэш-функция должна быть чувствительна к всевозможным изменениям в тексте M, таким как вставки, выбросы, перестановки • хэш-функция должна обладать свойством необратимости, то есть задача подбора документа M', который обладал бы требуемым значением хэш-функции, должна быть вычислительно трудная; • вероятность того, что значения хэш-функций двух различных документов (вне зависимости от их длин) совпадут, должна быть ничтожно мала Проиллюстрируем, что условия накладываемые на хеш функцию очень важны Предположим, что есть два пользователя A и B **условие 1** хэш-функция должна быть чувствительна к всевозможным изменениям в тексте M, таким как вставки, выбросы, перестановки, предположим противное. Тогда фразы «Казнить, нельзя помиловать» и «Казнить нельзя, помиловать» будут иметь одно хэш-значение и текст можно подменить. Для иллюстрации оставшихся условий рассмотрим ЭЦП RSA. Дано текст M и его хэш-значение $h(M)$. Все параметры, которые используются в криптосистеме RSA. Установка подписи вычисляем: $S = h(M)^d \bmod n$ Проверка подписи: • вычисляем $H' = S^e \bmod n$ • вычисляем $h(M)$ • проверяем равенство $H' = h(M)$. Если оно верно, то подпись законна. **условие 2** это условие препятствует криптоаналитику фабриковать сообщение с данной подписью, предположим условие не выполняется. Тогда возможна следующая атака. - B вычисляет $H' = R^e \bmod n$ с некоторым выбранным наугад целым числом R. - Кроме того, B находит прообраз значения H' при отображении $h()$, т.е. B определяет $M = h^{-1}(m')$. Теперь B обладает Вашей подписью R для сообщения M. **условие 3** вероятность того, что значения хэш-функций двух различных документов совпадут, должна быть ничтожно мала, предположим противное. Тогда возможна следующая атака - A выбирает два сообщения M и M', удовлетво-

	ряющие соотношению $H'=h(M)=h(M')$ - А подписывает M и получает (M,S) - Потом А отказывается от своего сообщения, утверждая, что посылал сообщение M'.
3. Основной принцип проектирования хэш-функции.	Основной принцип проектирования хэш-функции заключается в том, что ее значения должны производить лавинный эффект. Другими словами, небольшое изменение в аргументе хэш-функции должно очень сильно повлиять на ее значение.
4.Постройте однонаправленную хэш-функцию используя симметричный блочный алгоритм DES, хэш-значение состоит из k бит.	Однонаправленную хэш-функцию можно построить, используя симметричный блочный алгоритм DES, например используя режим «обратная связь по шифру». Последний блок шифротекста можно рассматривать в качестве хэш-значения для текста M. 

Критерии оценивания

Номер задачи	Критерии	Шкала оценивания
1	*Владеть навыками:* вычислять хэш значение	0 баллов – студент полностью неверно решил задачу 2 балла – студент полностью верно дал определение.
2	*Владеть навыками:* вычислять хэш значение	0 баллов – студент полностью неверно решил задачу 1 балл – студент верно решил задачу, но не привел пояснений к ходу решения. 2 балла – студент полностью разобрался в решении задачи
3	*Владеть навыками:* вычислять хэш значение	0 баллов – студент полностью неверно решил задачу 2 балла – студент полностью верно дал определение.
4	*Владеть навыками:* вычислять хэш значение	0 баллов – студент полностью неверно решил задачу 1 балл – студент верно решил задачу, но не привел пояснений к ходу решения (без схемы шифрования). 2 балла – студент полностью разобрался в решении задачи

Набранное количество баллов соответствует оценке за выполнение работы:
- менее 4 баллов — оценка «неудовлетворительно» компетенция не сформирована;
- от 4 до 5 баллов — оценка «удовлетворительно», пороговый уровень формирования компетенции;

- от 6 до 7 баллов — оценка «хорошо», продвинутый уровень формирования компетенции;
- 8 баллов — оценка «отлично», высокий уровень формирования компетенции

Типовой вариант контрольной работы

На контрольных работах студентам предлагается следующие типовые задания:

Контрольная работа 1

Задания	Ответы:
1.Применяя расширенный алгоритм Евклида: a) найти d,x,y для которых выполняется $d=НОД(a,b)=ax+by$, где a=512; b=724 b) найти x для которого выполняется $8x \bmod 107$	a) $4=НОД(512,724)=512*(-41)+724*29$, следовательно $d=4, x=-41, y=29$ b) После применении расширенного алгоритма Евклида $d=НОД(a,b)=ax+by$, где $a=107, b=8.$ Мы получим: $1=НОД(107,8)=107*3+8*(-40)$, возьмем указанное выражение по модулю 107. В результате $(107*3+8*(-40)) \bmod 107 \Rightarrow (8*(-40)) \bmod 107 \Rightarrow q=-40=67$
2.Построить криптосистему RSA и закодируйте число 7	Числовые значения могут отличаться от тех, которые приведены в данном решении Криптосистема RSA строится следующим образом: • сначала выбираются два больших простых числа p и q • вычисляем $n=pq$ и $\varphi(n)=(p-1)(q-1)$ • выбирается открытый ключ натуральное число e такой, что $1 \le e \le n-1$ и который является взаимно простым с $\varphi(n)=(p-1)(q-1)$ • вычисляем секретный ключ d такой, что $1 \le d \le n-1$ и $ed \equiv 1 \bmod \varphi(n)$ Для того чтобы зашифровать блок сообщения $M¿(0<M<n)¿$ надо выполнить следующие действия: $C=M^e \bmod n$ Для того чтобы расшифровать блок сообщения $C¿(0<C<n)¿$ надо выполнить следующие действия: $M=C^d \bmod n$ Построим криптосистему RSA и закодируем число 7 Строим криптосистему • выбираем $p=3$ и $q=11;$ • вычисляем $n=33$ и $\varphi(n)=20$ • выбираем $e=3$ • вычисляем $d=7$ Для того чтобы зашифровать сообщение $M=7$ надо выполнить следующие действия: $C=M^e \bmod n=7^3 \bmod 33=13$
3. Вычислить $\begin{cases} x \equiv 1 \mod 4 \\ x \equiv 3 \mod 5 \\ x \equiv 2 \mod 7 \end{cases}$	Напомним процесс вычисления. Пусть задано: множество натуральных чисел $(m_1, m_2, \ldots, m_k)$ не равных единице, которые являются попарно взаимно простыми множество натуральных чисел $(b_1, b_2, \ldots, b_k)$. Система сравнений $\begin{cases} x \equiv b_1 \mod m_1 \\ \ldots \\ x \equiv b_k \mod m_k \end{cases}$ имеет решение $x=x_0¿ \bmod (m_1 m_2 \ldots m_k);¿$ где $x_0=M_1 M_1' b_1+\ldots+M_k M_k' b_k;$ числа M_s и M_s определяется из условий

	$m_1 m_2 \ldots m_k = M_s m_s, \quad M_s M_s' = 1 ¿ \bmod m_s ¿$ Рассмотрим наше уравнение $M_1=35, M_2=28, M_3=20; \quad M_1'=3, M_2'=2, M_3'=6.$ $m_1 m_2 m_3 = 140;$ $x_0 = 35*3*1+28*2*3+20*6*2=513$ $x=93$
4. Сформулировать алгоритм установки ЭЦП DSA. Дан текст с хэш значением равным 5. Выполните установку ЭЦП DSA. К полученным результатам примените протокол проверки подписи	Числовые значения могут отличаться от тех, которые приведены в данном решении Схема DSA строится следующим образом: сначала выбирается большое простое число p выбирается простое число q которое является делителем $p-1$ выбирается натуральное число t, которое $0<t<p.$. Если число $t^{\frac{p-1}{q}}=1 \bmod p,$ то выбираем другое число $t.$ В противном случае $g=t^{\frac{p-1}{q}} \bmod p.$ выбирается натуральное число x, которое является секретным ключом причем $1<x<q$ вычисляем $y=g^x \bmod p$ Установка подписи: проверяем выполняется ли условие для хэш значение m текста M, что $0<m<q$ выбирается натуральное число $k, ¿(0<k<q).¿$ вычисляем k^{-1}, для которого выполняется условие $k*k^{-1}=1 \bmod q$ вычисляем два числа r и s по следующим правилам: $r=(g^k \bmod p) \bmod q$ и $s=k^{-1}(xr+m) \bmod q$ Если не выполняются условия $0<r<q, 0<s<q$ поменяйте входные параметры. Подписью является пара чисел (r,s) Проверка подписи Предположим, что к нам пришло сообщение M' с хэш значением m' и подписью (r',s') если хотя бы одно из условий $0<r'<q, 0<s'<q$ не выполняется, то подпись считается недействительной вычисляем $v=(s')^{-1} \bmod q$ вычисляем: $z_1=(m'v) \bmod q$ $z_2=(r'v) \bmod q$ $u=((g^{z_1} y^{z_2}) \bmod p) \bmod q$ проверяем условие $r'=u.$ Если оно выполняется то подпись считается подлинной а сообщение –неизмененным. Дан текст с хэш значением равным 7. Выполните установку ЭЦП DSA. Строим схему DSA выбираем $p=23, q=11, t=3$ вычисляем $g=3^2 \bmod 23=9$ выбираем $x=2$

	вычисляем $y=9^2 \bmod 23=12$ Установка подписи: выбираем $k=4$ вычисляем: $k^{-1}=3$, $r=(9^4 \bmod 23) \bmod 11=6$, $s=(3*(2*6+5)) \bmod 11=7$ Подписью является пара чисел $(6,7)$ Проверка подписи Дано $m'=5$; ¿ ¿ условие $0<6<11$, ¿ $0<7<11$ ¿ выполняется вычисляем: $v=(s')^{-1} \bmod q=7^{-1} \bmod 11=8$ $z_1=(m'v) \bmod q=(5*8) \bmod 11=7$ $z_2=(r'v) \bmod q=(6*8) \bmod 11=4$ $u=((g^{z_1} y^{z_2}) \bmod p) \bmod q=((9^7 ¿ 12^4) \bmod 23) \bmod 11=6$ Условие $r'=u$ выполнено, подпись подлинная.
5. Построить рюкзачную криптосистему и закодировать элементы множества, которые состоят из двоичных векторов (000,010,011,111)	Числовые значения могут отличаться от тех, которые приведены в данном решении Напомним описание рюкзачной криптосистемы. Создание криптосистемы: выбираем сверхрастущий вектор $A=(a_1,\ldots,a_n)$ - это секретная информация выбираем m и t, такие что $m>\sum_{i=1}^{n} a_i$ и $НОД(m,t)=1$ - это секретная информация вычисляем t^{-1}, такое что $t*t^{-1}=1 \bmod m$ - это секретная информация строим вектор $B=(b_1,\ldots,b_n)$, где $b_i=ta_i \bmod m$. . Вектор B - это открытая информация и используется, как ключ зашифрования. Шифрование Дано: вектор $B=(b_1,\ldots,b_n)$, двоичный вектор $X=(x_1,\ldots,x_n)$. шифр вычисляем $C=B*X$ Дешифрование Дано: вектор $A=(a_1,\ldots,a_n)$, числа C,t^{-1},m. вычисляем $\alpha=(C*t^{-1}) \bmod m$ решаем задачу о рюкзаке (A,α) Рассмотрим предложенное задание Создание криптосистемы: выберем $A=(1,3,5), m=11, t=5, t^{-1}=9$ - это секретный ключ вычислим $B=(5,4,3)$. Шифрование Дано: вектор $B=(5,4,3)$, двоичные вектора $x_1=(0,0,0); x_2=(0,1,0)$; $x_3=(0,1,1); x_4=(1,1,1)$. получили шифр $c_1=0; c_2=4; c_3=7; c_4=12$
6. Взломайте аффинную	Нам надо решить систему

криптосистему $f(x)=(ax+b)\bmod m$, для русского алфавита. Известно, что в исходном тексте чаще всего встречаются символы с порядковыми номерами 10 и 14, а в шифрованном тексте с порядковыми номерами 8 и 17.	$\begin{cases}10a+b=8 \bmod 33\\14a+b=17 \bmod 33\end{cases}$ или $\begin{cases}10a+b=17 \bmod 33\\14a+b=8 \bmod 33\end{cases}$ Ответ $a=27¿b=2¿$ или $a=6¿b=23¿$
7. Выполните операцию умножения байтов в поле $GF(2^8)$, которая используется в алгоритме AES. x^4+x+1 и x^4+x^2+1	Алгоритм оперирует байтами, которые рассматриваются как элементы конечного поля $GF(2^8)$. Поскольку байты оперируют в поле $GF(2^8)$, то заданы операции сложения и умножения: • сложение - суть операция поразрядного XOR. • умножение - это операция умножения многочленов со взятием результата по модулю некоторого неприводимого многочлена $\phi(x)$ и использованием операции XOR при приведении подобных членов. В качестве неприводимого многочлена $\phi(x)=x^8+x^4+x^3+x+1$. 1. Решение 2. $((x^4+x+1)*(x^4+x^2+1))¿\bmod(x^8+x^4+x^3+x+1)=x^6+x^5+x^4+x^2.$

Критерии оценивания

Номер задачи	Критерии	Шкала оценивания
1	*Знать*: методы защиты информации, некоторые криптографические алгоритмы *Уметь:* реализовывать некоторые криптографические алгоритмы, уметь выполнять передачу или генерацию ключей. *Владеть навыками*: вычислять хэш значение, создавать ЭЦП	0 баллов – студент полностью неверно решил задачу 1 балл – студент верно решил одну подзадачу. 2 балла – студент полностью разобрался в решении задачи
2	*Знать*: методы защиты информации, некоторые криптографические алгоритмы *Уметь:* реализовывать некоторые криптографические алгоритмы, уметь выполнять передачу или генерацию ключей. *Владеть навыками*: вычислять хэш значение, создавать ЭЦП	0 баллов – студент полностью неверно решил задачу 1 балл – студент верно решил задачу, но не привел пояснений к ходу решения или допустил вычислительную ошибку. 2 балла – студент полностью разобрался в решении задачи
3	*Знать*: методы защиты информации, некоторые криптографические алгоритмы *Уметь:* реализовывать некоторые криптографические алгоритмы, уметь выполнять передачу или генерацию ключей. *Владеть навыками*: вычислять хэш значение, создавать ЭЦП	0 баллов – студент полностью неверно решил задачу 1 балл – студент верно решил задачу, но не привел пояснений к ходу решения или допустил вычислительную ошибку. 2 балла – студент полностью разобрался в решении задачи
4	*Знать*: методы защиты информации, некоторые криптографические алгоритмы *Уметь:* реализовывать некоторые криптографические алгоритмы, уметь выполнять передачу или генерацию ключей. *Владеть навыками*: вычислять хэш значение, создавать ЭЦП	0 баллов – студент полностью неверно решил задачу 1 балл – студент верно решил задачу, но не привел пояснений к ходу решения или допустил вычислительную ошибку. 2 балла – студент полностью разобрался в решении задачи
5	*Знать*: методы защиты информации, некоторые крип-	0 баллов – студент полностью невер-

	тографические алгоритмы *Уметь:* реализовывать некоторые криптографические алгоритмы, уметь выполнять передачу или генерацию ключей. *Владеть навыками*: вычислять хэш значение, создавать ЭЦП	но решил задачу 1 балл – студент верно решил задачу, но не привел пояснений к ходу решения. 2 балла – студент полностью разобрался в решении задачи
6	*Знать*: методы защиты информации, некоторые криптографические алгоритмы *Уметь:* реализовывать некоторые криптографические алгоритмы, уметь выполнять передачу или генерацию ключей. *Владеть навыками*: вычислять хэш значение, создавать ЭЦП	0 баллов – студент полностью неверно решил задачу 2 балла – студент полностью разобрался в решении задачи
7	*Знать*: методы защиты информации, некоторые криптографические алгоритмы *Уметь:* реализовывать некоторые криптографические алгоритмы, уметь выполнять передачу или генерацию ключей. *Владеть навыками*: вычислять хэш значение, создавать ЭЦП	0 баллов – студент полностью неверно решил задачу 1 балл – студент верно решил задачу, но не привел пояснений к ходу решения или допустил вычислительную ошибку. 2 балла – студент полностью разобрался в решении задачи

Максимальное количество баллов -14 баллов

Набранное количество баллов соответствует оценки за контрольную работу:

Рассмотрим формирование компетенции и оценки:

-менее 6 баллов компетенция не сформирована – оценка «неудовлетворительно»;

-от 6 до 10 баллов — пороговый уровень формирования компетенции - оценка «удовлетворительно»;

- от 11 до 12 баллов — продвинутый уровень формирования компетенции - оценка «хорошо» ;

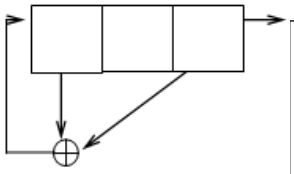
- от 13 до 14 баллов — высокий уровень формирования компетенции - оценка «отлично».

Контрольная работа 2

Задания	Ответы:
1. Есть три пользователя A,B и C используя протокол DIFFIE-HELLMAN сгенерируйте общий секретный ключ	Числовые значения могут отличаться от тех, которые приведены в данном решении 1.Пользователи A,B и C выбирают в открытом доступе большое простое число n и g . Пусть $n=13$ и $g=2$ 2. Пользователь A выбирает случайное большое натуральное число x и отправляет пользователю B величину $X=g^x \bmod ¿n¿$; Пусть $x=5$ и $X=6$ 3. Пользователь B выбирает случайное большое натуральное число y и отправляет пользователю C величину $Y=g^y \bmod ¿n¿$; Пусть $y=7$ и $Y=11$ 4. Пользователь C выбирает случайное большое натуральное число z и отправляет пользователю A величину $Z=g^z \bmod ¿n¿$; Пусть $z=3$ и $Z=8$ 5. Пользователь A отправляет пользователю B следующую величину $Z'=Z^x \bmod ¿n¿$; Вычисляем $Z'=8^5 \bmod ¿13=8¿$

	6. Пользователь B отправляет пользователю C следующую величину $X' = X^y \bmod ¿ n ¿$; Вычисляем $X' = 6^7 \bmod ¿ 13 = 7 ¿$ 7. Пользователь C отправляет пользователю A следующую величину $Y' = Y^z \bmod ¿ n ¿$; Вычисляем $Y' = 11^3 \bmod ¿ 13 = 5 ¿$ 8. Пользователь A вычисляет величину $k = Y^{¿} \bmod ¿ n ¿$; Вычисляем $k = 5^5 \bmod ¿ 13 = 5 ¿$ 9. Пользователь B вычисляет величину $\tilde{k} = Z^{¿} \bmod ¿ n ¿$. Вычисляем $\tilde{k} = 8^7 \bmod ¿ 13 = 5 ¿$ 10. Пользователь C вычисляет величину $\tilde{\tilde{k}} = X^{¿} \bmod ¿ n ¿$. Вычисляем $\tilde{\tilde{k}} = 7^3 \bmod ¿ 13 = 5 ¿$ Получили $\tilde{k} = k = \tilde{\tilde{k}} = 5$
2. Есть два пользователя A и B используя протокол MTI сгенерируйте общий секретный ключ, если известно, что $n = 17$	Числовые значения могут отличаться от тех, которые приведены в данном решении 1.Пользователи A и B выбирают в открытом доступе большое простое число n и g , где g образующий элемент мультипликативной группы $Z_n^{¿}$. Пусть $n = 17$ и $g = 3$ 2. Пользователи A и B должны сгенерировать секретные ключи a, $1 \le a \le n-2$, и b, $1 \le b \le n-2$, соответственно, и публикуют свои открытые ключи $z_A = g^a \bmod n$ и $z_B = g^b \bmod n$; Пусть Пользователь A генерирует число $a = 2$ и публикует $z_A = 3^2 \bmod 17 = 9$, соответственно пользователь B генерирует число $b = 3$ и публикует $z_B = 3^3 \bmod 17 = 10$; 3. Пользователь A выбирает случайное натуральное число x , $1 \le x \le n-2$ и отправляет пользователю B величину $X = g^x \bmod ¿ n ¿$; Пусть пользователь A генерирует число $x = 4$ и отправляет пользователю B величину $X = 3^4 \bmod ¿ 17 = 13 ¿$; 4. Пользователь B выбирает случайное большое натуральное число y , $1 \le y \le n-2$ и отправляет пользователю A величину $Y = g^y \bmod ¿ n ¿$; Пусть пользователь B генерирует число $y = 5$ и отправляет пользователю величину $Y = 3^5 \bmod ¿ 17 = 5 ¿$; 5. Пользователь A вычисляет величину $k = Y^a z_B^x \bmod n$; Пусть пользователь A на настоящий момент знает величины: $n, g, a, z_A, z_B, x, X, Y$. Пользователь A вычисляет величину $k = \left(Y^a z_B^x\right) \bmod ¿ n = ¿$ $\left(5^2 10^4\right) \bmod 17 =$ $\left(15 * 10000\right) \bmod 17 = 15$ 6. Пользователь B вычисляет величину $\tilde{k} = X^b z_A^y \bmod n.$ Пусть пользователь B на настоящий момент знает величины: $n, g, b, z_A, z_B, y, X, Y$. Пользователь B вычисляет величину $\tilde{k} = \left(X^b z_A^y\right) \bmod ¿ n = ¿$ $\left(13^3 9^5\right) \bmod ¿ 17 = ¿$ $\left(2197 * 59049\right) \bmod ¿ 17 = 15 ¿$ Получили $\tilde{k} = k = 15$
3.Постройте регистр сдвига с линейной обрат-	$(1,1,1)$ вектор инициализации регистр сдвига

LFSR	Состояние регистра		Выход
	итерация	**состояние рег. стало**	
	0	111	
	1	011	1
	2	101	1
	3	010	1
	4	001	0
	5	100	1
	6	110	0
	7	111	0



он был инициализирован вектором (111) .

4.Постройте 10 битную псевдослучайную последовательность с помощью RSA-генератора.

Числовые значения могут отличаться от тех, которые приведены в данном решении

Напомним, что RSA-генератор строится следующим образом:

- выбираем p и q - два больших простых числа примерно одинакового размера $p \neq q$;
- вычисляем число $n = pq$ и число $\phi(n) = (p-1)(q-1)$;
- выбираем случайное натуральное число e , которое являются взаимно простым с $\phi(n)$;
- выбираем в качестве стартового числа генератора случайное натуральное число $x_0 ¿ (1 < x_0 < n) ¿$;
- искомой последовательностью бит длиной m будет являться последовательность $RSA_{n,m}(x_0) = b_0 b_1 b_2 \ldots b_i \ldots b_{m-1}$, $i = 0, \ldots, m-1$, где b_i - младший бит числа x_i , $x_{i+1} = x_i^e \bmod n.$

Построим 10 битную псевдослучайную последовательность

- Пусть $p = 3,$ а $q = 11$.
- Вычислим $n = pq = 33$ и $\phi(n) = (p-1)(q-1) = 20$.
- В качестве e возьмем число 3.
- В качестве стартового числа генератора $x_0 = 14.$
- В качестве элементов псевдослучайной последовательности будем брать младший бит в двоичной записи чисел $x_{i+1} = x_i^e \bmod n.$

В результате получили последовательность $RSA_{33,10}(14) = 0100010001$.

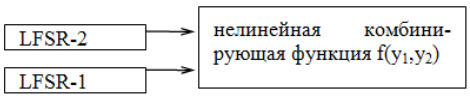
5. Создайте комбинирующий генератор, состоящий из двух регистров сдвига с линейной обратной связью.

Первый регистр с ассоциированным многочленом $x^6 + x + 1,$ он был инициализирован вектором $(1,1,1,1,1,1)$. Выход регистра y_1.

Второй регистр с ассоциированным многочленом $x^3 + x + 1$ он был инициализирован вектором $(1,1,1)$. Выход регистра y_2.

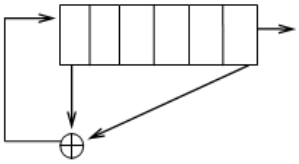
В качестве комбинирующей функции возьмем

Напомним, что комбинирующий генератор проиллюстрировать следующей схемой



Решение

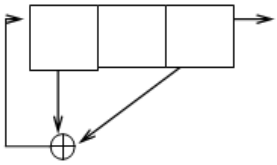
- Первый регистр



Состояние регистра		выход	Состояние регистра		выход
итерация	состояние рег. стало	y_1.	итерация	состояние рег. стало	y_1.
0	111111		4	101011	1
1	011111	1	5	010101	1
2	101111	1	6	101010	1
3	010111	1	7	110101	0

<table>
<tr>
<td>$f(y_1, y_2) = y_1 y_2$
Постройте 7 битную псевдослучайную последовательность</td>
<td>

• Второй регистр



<table>
<tr><th colspan="2">Состояние регистра</th><th>выход</th><th colspan="2">Состояние регистра</th><th>выход</th></tr>
<tr><td>итерация</td><td>состояние рег. стало</td><td>y_2.</td><td>итерация</td><td>состояние рег. стало</td><td>y_2.</td></tr>
<tr><td>0</td><td>111</td><td></td><td>4</td><td>001</td><td>0</td></tr>
<tr><td>1</td><td>011</td><td>1</td><td>5</td><td>100</td><td>1</td></tr>
<tr><td>2</td><td>101</td><td>1</td><td>6</td><td>110</td><td>0</td></tr>
<tr><td>3</td><td>010</td><td>1</td><td>7</td><td>111</td><td>0</td></tr>
</table>

В результате получим последовательность 1110100

</td>
</tr>
</table>

Критерии оценивания

Номер задачи	Критерии	Шкала оценивания
1	*Знать*: методы защиты информации, некоторые криптографические алгоритмы *Уметь:* реализовывать некоторые криптографические алгоритмы, уметь выполнять передачу или генерацию ключей. *Владеть навыками*: вычислять хэш значение, создавать ЭЦП	0 баллов – студент полностью не верно решил задачу 1 балл – студент верно решил задачу, но была допущена вычислительная ошибка. 2 балла – студент полностью разобрался в решении задачи
2	*Знать*: методы защиты информации, некоторые криптографические алгоритмы *Уметь:* реализовывать некоторые криптографические алгоритмы, уметь выполнять передачу или генерацию ключей. *Владеть навыками*: вычислять хэш значение, создавать ЭЦП	0 баллов – студент полностью не верно решил задачу 1 балл – студент верно решил задачу, но была допущена вычислительная ошибка. 2 балла – студент полностью разобрался в решении задачи
3	*Знать*: методы защиты информации, некоторые криптографические алгоритмы *Уметь:* реализовывать некоторые криптографические алгоритмы, уметь выполнять передачу или генерацию ключей. *Владеть навыками*: вычислять хэш значение, создавать ЭЦП	0 баллов – студент полностью неверно решил задачу 1 балл – студент верно решил задачу, но не привел пояснений к ходу решения. 2 балла – студент полностью разобрался в решении задачи
4	*Знать*: методы защиты информации, некоторые криптографические алгоритмы *Уметь:* реализовывать некоторые криптографические алгоритмы, уметь выполнять передачу или генерацию ключей. *Владеть навыками*: вычислять хэш значение, создавать ЭЦП	0 баллов – студент полностью неверно решил задачу 1 балл – студент верно решил задачу, но не привел пояснений к ходу решения. 2 балла – студент полностью разобрался в решении задачи
5	*Знать*: методы защиты информации, некоторые криптографические алгоритмы *Уметь:* реализовывать некоторые криптографические алгоритмы, уметь выполнять передачу или генерацию ключей. *Владеть навыками*: вычислять хэш значение, создавать ЭЦП	0 баллов – студент полностью неверно решил задачу 1 балл – студент верно решил задачу, но не привел пояснений к ходу решения. 2 балла – студент полностью разобрался в решении задачи

Максимальное количество баллов -10 баллов

Набранное количество баллов соответствует оценки за контрольную работу:

Рассмотрим формирование компетенции и оценки:

-менее 5 баллов компетенция не сформирована – оценка «неудовлетворительно»;

-от 6 до 7 баллов — пороговый уровень формирования компетенции - оценка «удовлетворительно»;

- от 8 до 9 баллов — продвинутый уровень формирования компетенции - оценка «хорошо» ;

- 10 баллов — высокий уровень формирования компетенции - оценка «отлично».

Тест для самопроверки по результатам освоения дисциплины.

(проверка ПК-2)

Вопрос 1 Статичный ключ – это

1) ключ, который используется в течение большого периода времени.
2) ключ применяется лишь малое время, от нескольких секунд до одного дня.
3) ключ, который используется в течение одного раунда в алгоритме шифрования.

Вопрос 2 Сеансовый ключ – это

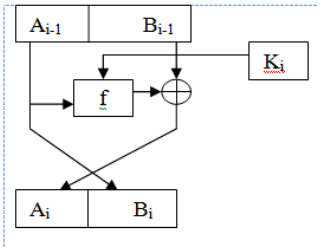
1) ключ, который используется в течение большого периода времени.
2) ключ применяется лишь малое время, от нескольких секунд до одного дня.
3) ключ, который используется в течение одного раунда в алгоритме шифрования.

Вопрос 3 Открытое распределение ключей

1) позволяет двум пользователям выработать общий секретный ключ путем динамического взаимодействия на основе обмена открытыми сообщениями без какой-либо общей секретной информации, распределенной заранее.
2) ключ находится в открытом доступе

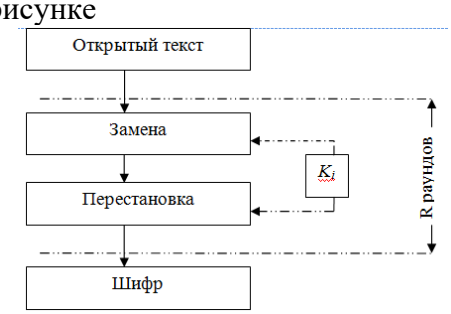
Вопрос 4 Какая схема отображена на рисунке

1) схема Фейстеля.
2) схема SP-сеть.
3) схема квадрат



Вопрос 5 Какая схема отображена на рисунке

1) схема Фейстеля.
2) схема SP-сеть.
3) схема квадрат



Вопрос 6 Какая криптосистема шифрования описывается формулой $f(x)=(x+b) \bmod m$

1) криптосистема Цезаря
2) криптосистема RC6
3) криптосистема AES

Вопрос 7 Какая криптосистема шифрования описывается формулой $f(x)=(ax+b) \bmod m$

1) Аффинная криптосистема
2) Криптосистема RC6
3) криптосистема AES

Вопрос 8 Блочное шифрование -

1) в этом случае исходное сообщение разбиваются на блоки фиксированной размерности, которые потом и шифруются.
2) в этом случае исходное сообщение шифруются побитово
3) в этом случае размер ключа равен размеру исходного сообщения

9 Найдите x для которого выполняется $x=1 \bmod 5$

Вопрос

Выберите ответ

1) 3.
2) 16
3) 12

Вопрос 10 Алгоритмы шифрования с открытым ключом – это система

Выберите ответ

1) в которых ключ расшифрования трудно найти даже при известном ключе шифрования
2) в которых ключ расшифрования легко находится по ключу шифрования
3) в которых ключ расшифрования совпадает с ключом шифрования

Вопрос 11 Зашифруйте число 5 криптосистемой RSA, если задано

- простые числа $p=3$ и $q=7$;
- ключ шифрования (открытый ключ) $e=5$.-

Выберите ответ

1) 17
2) 2
3) 25

Вопрос 12 В какой криптосистеме алгоритм шифрования блока X задается формулой $C=X^e \bmod n$, где

- $n-$ это число, которое получается из формулы $n=p*q$, здесь p и q простые числа;
- $e-$ это открытый ключ шифрования, который удовлетворяет условию $НОД(e,\phi(n))=1$, где $\phi(n)=(p-1)*(q-1)$.

1) Криптосистема RSA
2) Криптосистема RC6
3) криптосистема AES

Правильные ответы

Вопрос №	Вариант ответа		**Вопрос №**	Вариант ответа		**Вопрос №**	Вариант ответа
1	1		**5**	2		**9**	2
2	2		**6**	1		**10**	1
3	1		**7**	1		**11**	1
4	1		**8**	1		**12**	1

Каждый правильный ответ оценивается в 1 балл.

Набранное количество баллов 12 соответствует формированию проверяемой компетенции на высоком уровне, 9-11 баллов – на продвинутом уровне, 5-8 баллов – на пороговом уровне, менее 5 баллов – ниже порогового уровня.

Список заданий к экзамену

На экзамене проверяется сформированность знаний, умений и навыков в соответствии с компетенциями ПК-2.

Экзамен проводится в устной форме и выставляется по итогам ответов, данных студентом на два теоретических и один практический вопрос. Список теоретических

вопросов к экзамену заранее доступен для студентов. В билете присутствует один практический вопрос, аналогичный рассмотренным в курсе.

Перечислим список вопросов выносимых на экзамен

1. Определение информации, данных, знаний. Определение безопасности. Несанкционированный доступ.
2. Шифрование. Трудоемкость дешифрования. Симметричные шифры. Схема Фейстеля, SP-сеть. Режимы шифрования. Некоторые исторические алгоритмы (алгоритмы Цезаря, Вижнера).
3. Алгоритмы AES, Гост 28147-89,
4. Алгоритмы DES, Serpent,
5. Алгоритмы RC6, Mars
6. Криптоанализ
7. Асимметричные шифры, шифры с открытым ключом. Идея открытых ключей и преимущества их. Алгоритм Рабина. Алгоритм RSA. Алгоритм Эль-Гамаля
8. Рюкзачная криптоситема. Плотный рюкзак.
9. Криптосистема Рабина. Криптосистема Уильямса. Криптосистема Вильемса.
10. Электронные цифровые подписи. ЭЦП RSA, ЭЦП DSA, ЭЦП Гост
11. Задача дискретного логарифмирования, задача разложения на множители. Малая теорема Ферма. Расширенный алгоритм Евклида. Решить $y = a^x \bmod p$
12. Генераторы случайных и псевдослучайных чисел. Криптографические ГПСЧ, их свойства.
13. Генератор LFSR, и его модификации. Взлом LFSR.
14. Аддитивные генераторы, стохастические генераторы, генераторы RSA и BBS.
15. Виды поточных шифров. Алгоритмы A5, RC4.
16. Хэш-функции. Свойства криптографических хэш-функций.
17. Хэш-функции MD5, SHA1.
18. Доказательство с нулевым знанием.
19. Проверка чисел на простоту.
20. Нахождение мультипликативного элемента.

Критерии оценивания экзамена:

«2» - плохо(компетенция не сформирована):

Теоретический вопрос: студент не раскрыл теоретический вопрос, на заданные экзаменаторами вопросы не смог дать удовлетворительный ответ.

Практический вопрос: студент не понял смысла текста (задачи), не смог выполнить задания. На заданные экзаменатором вопросы ответил неудовлетворительно, не продемонстрировал сформированность требующихся для выполнения заданий знаний и умений. Или студент понял отдельные детали текста, но не его основной смысл, задания выполнил неправильно, на заданные экзаменатором вопросы ответил неудовлетворительно, не продемонстрировал сформированность требующихся для выполнения заданий умений.

«3» - удовлетворительно(компетенция сформирована на пороговом уровне):

Теоретический вопрос: студент смог с помощью дополнительных вопросов воспроизвести основные положения темы, но не сумел привести соответствующие примеры или аргументы, подтверждающие те или иные положения.

Практический вопрос: студент понял смысл текста (задачи), но смог выполнить задание лишь после дополнительных вопросов, предложенных экзаменатором. При этом на поставленные экзаменатором вопросы не вполне ответил правильно и полно, но подтвердил ответами понимание вопросов и продемонстрировал отдельные требующиеся для выполнения заданий знания и умения.

«4» - хорошо(компетенция сформирована на продвинутом уровне):

Теоретический вопрос: студент (не допуская ошибок) правильно изложил теоретический вопрос, но недостаточно полно или допустил незначительные неточности, не искажающие суть понятий, теоретических положений, правовых и моральных норм. Примеры, приведенные учеником, воспроизводили материал учебников. На заданные экзаменатором уточняющие вопросы ответил правильно.

Практический вопрос: студент понял смысл текста (задачи), предложенные задания выполнил правильно, но недостаточно полно. На заданные экзаменатором вопросы отве-

тил правильно. Проявил необходимый уровень всех требующихся для выполнения заданий знаний и умений.

«5» - отлично(компетенция сформирована на высоком уровне):

Теоретический вопрос: студент полно и правильно изложил теоретический вопрос, привел собственные примеры, правильно раскрывающие те или иные положения, сделал обоснованный вывод;

Практический вопрос: студент понял смысл текста (задачи), полно и правильно выполнил предложенные задания, проявил высокий уровень всех требующихся для выполнения заданий знаний и умений.

2. Перечень компетенций, этапы их формирования, описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкалы оценивания

2.1. Шкала оценивания сформированности компетенций и ее описание

Оценивание уровня сформированности компетенций в процессе освоения дисциплины осуществляется по следующей трехуровневой шкале:

Пороговый уровень - предполагает отражение тех ожидаемых результатов, которые определяют минимальный набор знаний и (или) умений и (или) навыков, полученных студентом в результате освоения дисциплины. Пороговый уровень является обязательным уровнем для студента к моменту завершения им освоения данной дисциплины.

Продвинутый уровень - предполагает способность студента использовать знания, умения, навыки и (или) опыт деятельности, полученные при освоении дисциплины, для решения профессиональных задач. Продвинутый уровень превосходит пороговый уровень по нескольким существенным признакам.

Высокий уровень - предполагает способность студента использовать потенциал интегрированных знаний, умений, навыков и (или) опыта деятельности, полученных при освоении дисциплины, для творческого решения профессиональных задач и самостоятельного поиска новых подходов в их решении путем комбинирования и использования известных способов решения применительно к конкретным условиям. Высокий уровень превосходит пороговый уровень по всем существенным признакам.

2.2. Перечень компетенций, этапы их формирования,описание показателей и критериев оценивания компетенций на различных этапах их формирования

Код компетенции	Форма контроля	Этапы формирования (№ темы (раздела)	Показатели оценивания	Шкала и критерии оценивания компетенций на различных этапах их формирования		
				Пороговый уровень	Продвинутый уровень	Высокий уровень
Профессиональные компетенции						
ПК-2	Самостоятельные работы Контрольные работы. Экзамен.	1-7	Знать: – методы защиты информации; – некоторые криптографические алгоритмы Уметь: – реализовывать некоторые криптографические алгоритмы – уметь выполнять передачу или генерацию ключей. Владеть навыками: – вычислять хэш значение; – создавать ЭЦП	Знать: – определение методов защиты информации; – схему DES – схему потокового шифрования (генераторы RSA, BBS) Уметь: – реализовывать некоторые криптографические алгоритмы (RSA,Эль-Гамаля) – уметь выполнять передачу или генерацию ключей. Владеть навыками: создавать ЭЦП.	Знать: – определение методов защиты информации; – схему DES, AES, RC6 – схему потокового шифрования (генераторы RSA, BBS, LFSR, аддитивный) – Уметь: – реализовывать некоторые криптографические алгоритмы (RSA,Эль-Гамаля, Рабина, Вильемса) – уметь выполнять передачу или генерацию ключей. – Владеть навыками: – вычислять хэш значение; – создавать ЭЦП (RSA, Эль-Гамаля)	Знать: – определение методов защиты информации; – схему DES, AES, RC6, Mars, Serpent – схему потокового шифрования (генераторы RSA, BBS, LFSR, аддитивный, стохастический) Уметь: – реализовывать некоторые криптографические алгоритмы (RSA,Эль-Гамаля, Рабина, Вильемса) – уметь выполнять передачу или генерацию ключей – знать вспомогательные протоколы(например, доказательство с нулевым знанием) Владеть навыками: – вычислять криптографически стойкие хэш значения; – создавать ЭЦП(RSA, Эль-Гамаля, DSA, Гост)

3. Методические рекомендации преподавателю по процедуре оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Целью процедуры оценивания является определение степени овладения студентом ожидаемыми результатами обучения (знаниями, умениями, навыками и (или) опытом деятельности).

Процедура оценивания степени овладения студентом ожидаемыми результатами обучения осуществляется с помощью методических материалов, представленных в разделе «Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций»

3.1 Критерии оценивания степени овладения знаниями¸ умениями, навыками и (или) опытом деятельности, определяющие уровни сформированности компетенций

Пороговый уровень (общие характеристики):

- владение основным объемом знаний по программе дисциплины;
- знание основной терминологии данной области знаний, стилистически грамотное, логически правильное изложение ответа на вопросы без существенных ошибок;
- владение инструментарием дисциплины, умение его использовать в решении стандартных (типовых) задач;
- способность самостоятельно применять типовые решения в рамках рабочей программы дисциплины;
- усвоение основной литературы, рекомендованной рабочей программой дисциплины;
- знание базовых теорий, концепций и направлений по изучаемой дисциплине;
- самостоятельная работа на практических и лабораторных занятиях, периодическое участие в групповых обсуждениях, достаточный уровень культуры исполнения заданий.

Продвинутый уровень (общие характеристики):

- достаточно полные и систематизированные знания в объёме программы дисциплины;
- использование основной терминологии данной области знаний, стилистически грамотное, логически правильное изложение ответа на вопросы, умение делать выводы;
- владение инструментарием дисциплины, умение его использовать в решении учебных и профессиональных задач;
- способность самостоятельно решать сложные задачи (проблемы) в рамках рабочей программы дисциплины;
- усвоение основной и дополнительной литературы, рекомендованной рабочей программой дисциплины;
- умение ориентироваться в базовых теориях, концепциях и направлениях по изучаемой дисциплине и давать им сравнительную оценку;
- самостоятельная работа на практических и лабораторных занятиях, участие в групповых обсуждениях, высокий уровень культуры исполнения заданий.

Высокий уровень (общие характеристики):

- систематизированные, глубокие и полные знания по всем разделам дисциплины;

- точное использование терминологии данной области знаний, стилистически грамотное, логически правильное изложение ответа на вопросы, умение делать обоснованные выводы;
- безупречное владение инструментарием дисциплины, умение его использовать в постановке и решении научных и профессиональных задач;
- способность самостоятельно и творчески решать сложные задачи (проблемы) в рамках рабочей программы дисциплины;
- полное и глубокое усвоение основной и дополнительной литературы, рекомендованной рабочей программой дисциплины;
- умение ориентироваться в основных теориях, концепциях и направлениях по изучаемой дисциплине и давать им критическую оценку;
- активная самостоятельная работа на практических и лабораторных занятиях, творческое участие в групповых обсуждениях, высокий уровень культуры исполнения заданий.

3.2 Описание процедуры выставления оценки

В зависимости от уровня сформированности каждой компетенции по окончании освоения дисциплины студенту выставляется оценка. Для дисциплин, изучаемых в течение нескольких семестров, оценка может выставляться не только по окончании ее освоения, но и в промежуточных семестрах. Вид оценки («отлично», «хорошо», «удовлетворительно», «неудовлетворительно») определяется рабочей программой дисциплины в соответствии с учебным планом.

Оценка «отлично» выставляется студенту, у которого каждая компетенция (полностью или частично формируемая данной дисциплиной) сформирована на высоком уровне.

Оценка «хорошо» выставляется студенту, у которого каждая компетенция (полностью или частично формируемая данной дисциплиной) сформирована не ниже, чем на продвинутом уровне.

Оценка «удовлетворительно» выставляется студенту, у которого каждая компетенция (полностью или частично формируемая данной дисциплиной) сформирована не ниже, чем на пороговом уровне.

Оценка «неудовлетворительно» выставляется студенту, у которого хотя бы одна компетенция (полностью или частично формируемая данной дисциплиной) сформирована ниже, чем на пороговом уровне.

Приложение №2 к рабочей программе дисциплины «Математические методы защиты информации»

Методические указания для студентов по освоению дисциплины

Основной формой изложения учебного материала по дисциплине **«Математические методы защиты информации»** являются лекции и практические занятия. Для успешного освоения дисциплины очень важно рассмотрение достаточно большого количества задач, как в аудитории, так и самостоятельно в качестве домашних заданий.

Задачи разбираются на лекциях и лабораторных занятиях, при необходимости по наиболее трудным темам проводятся дополнительные консультации. Для решения всех задач необходимо знать и понимать лекционный материал. Поэтому в процессе изучения дисциплины рекомендуется регулярное повторение пройденного лекционного материала. Материал, законспектированный на лекциях, необходимо дома еще раз прорабатывать и при необходимости дополнять информацией, полученной на консультациях, лабораторных занятиях или из учебной литературы. Большое внимание должно быть уделено выполнению домашней работы. В качестве заданий для самостоятельной работы дома студентам предлагаются задания, аналогичные разобранным на лекциях и лабораторных занятиях или немного более сложные, которые являются результатом объединения нескольких базовых задач. Для проверки и контроля усвоения теоретического материала, периодически проводятся контрольные работы.

Освоить вопросы, излагаемые в процессе изучения дисциплины «Математические методы защиты информации» самостоятельно студенту крайне сложно. Это связано со сложностью изучаемого материала и большим объемом курса. Поэтому посещение всех аудиторных занятий является совершенно необходимым. Без упорных и регулярных занятий в течение семестра сдать экзамен по итогам изучения дисциплины студенту практически невозможно.

Учебно-методическое обеспечение самостоятельной работы студентов по дисциплине

Для самостоятельной работы особенно рекомендуется использовать учебную литературу.

Также для подбора учебной литературы рекомендуется использовать широкий спектр интернет-ресурсов:

1. Электронно-библиотечная система «Университетская библиотека online» (www.biblioclub.ru) - электронная библиотека, обеспечивающая доступ к наиболее востребованным материалам-первоисточникам, учебной, научной и художественной литературе ведущих издательств (*регистрация в электронной библиотеке – только в сети университета. После регистрации работа с системой возможна с любой точки доступа в Internet.).

2.Информационная система "Единое окно доступа к образовательным ресурсам" (http://window.edu.ru/library).

Целью создания информационной системы "Единое окно доступа к образовательным ресурсам" (ИС "Единое окно ") является обеспечение свободного доступа к интегральному каталогу образовательных интернет-ресурсов и к электронной библиотеке учебно-методических материалов для общего и профессионального образования.

Для самостоятельного подбора литературыв библиотеке ЯрГУ рекомендуется использовать:

1. Личный кабинет (http://lib.uniyar.ac.ru/opac/bk_login.php)дает возможность получения on-line доступа к списку выданной в автоматизированном режиме литературы, просмотра и копирования электронных версий изданий сотрудников университета (учеб. и метод. пособия, тексты лекций и т.д.) Для работы в «Личном кабинете» необходимо зайти на сайт Научной библиотеки ЯрГУ с любой точки, имеющей доступ в Internet, в пункт

меню «Электронный каталог»; пройти процедуру авторизации, выбрав вкладку «Авторизация», и заполнить представленные поля информации.

2. Электронная библиотека учебных материалов ЯрГУ

(http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php) содержит более 2500 полных текстов учебных и учебно-методических материалов по основным изучаемым дисциплинам, изданных в университете. Доступ в сети университета, либо по логину/паролю.

3. Электронная картотека «Книгообеспеченность»

(http://www.lib.uniyar.ac.ru/opac/bk_bookreq_find.php) раскрывает учебный фонд научной библиотеки ЯрГУ, предоставляет оперативную информацию о состоянии книгообеспеченности дисциплин основной и дополнительной литературой, а также цикла дисциплин и специальностей. Электронная картотека «Книгообеспеченность» доступна в сети университета и через Личный кабинет.