

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

Кафедра компьютерной безопасности и математических методов обработки информации

УТВЕРЖДАЮ

Декан математического факультета



Нестеров П.Н.

20 июня 2023 г.

Рабочая программа дисциплины
Криптографические методы защиты информации

Направление подготовки (специальности)
10.05.01 Компьютерная безопасность

Направленность (профиль)
«Математические методы защиты информации»

Форма обучения очная

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

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

1. Цели освоения дисциплины

Дисциплина "Криптографические методы защиты информации" обеспечивает приобретение фундаментальных и профессиональных знаний, умений и навыков в соответствии с Федеральным государственным образовательным стандартом по специальности "10.05.01-Компьютерная безопасность" (уровень специалитета), содействует фундаментализации образования, развитию логического мышления и формированию математического и общенаучного мировоззрения. Целью изучения дисциплины является овладение базовыми понятиями и методами в области криптографической защиты информации, овладение современным математическим аппаратом, используемым в криптографии для дальнейшего использования в приложениях.

2. Место дисциплины в структуре образовательной программы

Дисциплина "Криптографические методы защиты информации" относится к базовой части образовательной программы. Она играет исключительно важную роль для профессиональной подготовки специалиста. При ее изучении существенно используются знания, полученные при изучении математических дисциплин "Алгебра", "Теория чисел", "Дискретная математика", "Информатика" и "Математическая логика и теория алгоритмов". Знания, умения и навыки, полученные при изучении дисциплины "Криптографические методы защиты информации", используются обучаемыми при изучении профессиональных и специальных дисциплин.

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

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

Формируемая компетенция (код и формулировка)	Перечень планируемых результатов обучения
Профессиональные компетенции	
ПК-5 Обладает способностью участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации	Знать: <ul style="list-style-type: none">- основные понятия, принципиальные результаты и методы криптографической защиты информации- требования к параметрам ассиметричных криптосистем и методы их генерации Уметь: <ul style="list-style-type: none">- генерировать параметры ассиметричных криптосистем- решать задачи, связанные с анализом стойкости алгоритмов криптографической защиты информации- строить ЛРП максимального периода;- вычислять линейную сложность последовательности. Владеть навыками: <ul style="list-style-type: none">- обоснования стойкости в рамках различных подходов к определению стойкости- разработки и программной реализации алгоритмов криптографической защиты информации- использования систем компьютерной алгебры для генерации

	параметров ассиметричных криптосистем; - разработки и программной реализации алгоритмов анализа криптографически стойких S-блоков.
--	--

4. Объем, структура и содержание дисциплины

Общая трудоемкость дисциплины составляет **7** зачетных единиц, **252** акад. часов.

№ п/п	Темы (разделы) дисциплины, их содержание	Семестр	Виды учебных занятий, включая самостоятельную работу студентов, и их трудоемкость (в академических часах)						Формы текущего контроля успеваемости Форма промежуточной аттестации (по семестрам)
			Контактная работа					самостоятельная работа	
			лекции	практические	лабораторные	консультации	аттестационные испытания		
1	Вводная лекция. Основные понятия и задачи криптографии.	7	2						Устный опрос
2	Простейшие исторические шифры и их криптоанализ.	7	4	6		1		6	Задания для самостоятельной работы, устный опрос, практическая работа №1
3	Стойкость шифров.	7	10	10		3		6	Задания для самостоятельной работы, устный опрос
4	Поточные шифры и генерация псевдослучайных последовательностей.	7	10	10		3		10	Задания для самостоятельной работы, устный опрос, практическая работа №2
5	Блочные шифры.	7	8	8		3		6	Задания для самостоятельной работы, устный опрос, практическая работа №3
							0,3	1,7	Зачет
	Итого за 7 семестр 108 акад. часов		34	34		10	0,3	29,7	
6	Хеш-функции.	8	4	4				6	Задания для самостоятельной работы, устный опрос.
7	Асимметричная криптография.	8	6	6		1		8	Задания для самостоятельной работы, устный опрос, практическая работа №4
8	Управление ключами.	8	2					2	Устный опрос.

9	Элементы криптоанализа.	8	10	14		1		14	Задания для самостоятельной работы, устный опрос, практическая работа №5
10	Некоторые современные направления криптографических исследований.	8	12	8		1		11	Задания для самостоятельной работы, устный опрос
						2	0,5	33,5	Экзамен
	Всего за 8 семестр 144 акад. часа		32	32		5	0,5	74,5	
	ИТОГО		66	66		15	0,8	104,2	

Содержание разделов дисциплины:

1. Вводная лекция. Основные понятия и задачи криптографии.

Краткая история криптографии. Задачи в области обеспечения информационной безопасности и методы защиты информации. Криптографические методы защиты информации, их особенность. Модель систем передачи информации. Симметричные и асимметричные криптосистемы. Криптоанализ и криптосинтез. Принцип Керкгоффа. Типы атак на криптосистему. Формальные модели шифров. Классификация шифров по различным признакам. Модели открытых текстов. Оценка числа осмысленных текстов.

2. Простейшие исторические шифры и их криптоанализ.

Шифр Цезаря, аффинный шифр, шифр простой замены, шифр Хилла, шифр перестановки, шифр Вижинера, шифр гаммирования. Их криптоанализ.

3. Стойкость шифров.

Алгебраическая и вероятностная модель шифра. Теоретическая стойкость шифров по Шеннону. Теорема Шеннона. Шифр Вернама и его совершенная стойкость. Энтропия и ее свойства. Избыточность языка. Оценка числа ложных ключей и расстояние единственности. Другие подходы к определению стойкости шифра. Односторонние функции и односторонние функции с «лазейкой». Семантическая стойкость и полиномиальная стойкость.

4. Поточные шифры и генерация псевдослучайных последовательностей.

Поточные шифры и принципы их построения. Генераторы ПСП. Криптографически стойкие ГПСЧ. Линейные рекуррентные последовательности. Оценка периода ЛРП. Минимальный многочлен ЛРП. Линейная сложность последовательности. Алгоритм Берлекэмпа-Мессис. Методы усложнения ЛРП: фильтрующие и комбинирующие генераторы. Примеры поточных шифров: A5, RC4, CSS (Content Scramble System).

5. Блочные шифры.

Блочные шифры и принципы их построения. Сеть Фейстеля. Алгоритм DES и его варианты (3DES, DESX). Алгоритм «Магма» (ГОСТ 28147-89). SP-сеть. Алгоритм AES. Алгоритм «Кузнечик» (ГОСТ 34.12-2015). Режимы использования блочных шифров.

6. Хеш-функции.

Бесключевые и ключевые хеш-функции. Методы построения хеш-функций. Применение хеш-функций. Примеры хеш-функций: «Стрибог» (ГОСТ Р 34.11-2012), MD5, SHA, HMAC, функции на основе блочных шифров.

7. Асимметричная криптография.

Вычислительно сложные задачи математики. Схема RSA и ее анализ. Схема Эль-Гамала. Схема Меркля-Хеллмана. Гибридная схема шифрования. Цифровая подпись. Схемы цифровой подписи на основе RSA. Схема цифровой подписи Эль-Гамала: ГОСТ 34.10-2012, ECDSA. Схемы слепой подписи. Сертификаты и инфраструктура открытых ключей.

8. Управление ключами.

Ключевая система. Жизненный цикл ключей. Понятие криптографического протокола.

Протоколы выработки общего ключа. Протоколы передачи ключей. Схемы разделения секрета.

9. Элементы криптоанализа.

Криптографические свойства отображений. Нелинейные булевы функции. Бент функции, корреляционно-иммунные и алгебраически-иммунные функции. Дифференциально-равномерные функции и их свойства. APN отображения. Анализ и построение криптографически стойких S-блоков блочных шифров. Общие методы криптоанализа шифров. Методы компромисса времени и памяти: метод встречи посередине, метод Хеллмана. Применение парадокса дней рождения. Алгебраические методы анализа шифров. Метод линеаризации. Статистические методы анализа шифров. Линейный и дифференциальный криптоанализ. Корреляционные атаки на поточные шифры.

10. Некоторые современные направления криптографических исследований.

Квантовые вычисления. Квантовое распределение ключей. Алгоритм Шора. Постквантовая криптография. Криптография, базирующаяся на решетках. Криптосистемы GGH и NTRU. Обучение с ошибками (LWE). Использование теории кодирования в криптографии. Коды Гоппы. Криптосистема McEliece. Криптография, базирующаяся на группах. Криптографические протоколы на базе комбинаторной теории групп. Группы кос и протоколы на их основе. Криптография на основе эллиптических кривых.

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

В процессе обучения используются следующие образовательные технологии:

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 с элементами лекции-беседы – последовательное изложение материала, осуществляемое преимущественно в виде монолога преподавателя. Элементы лекции-беседы обеспечивают контакт преподавателя с аудиторией, что позволяет привлекать внимание студентов к наиболее важным темам дисциплины, активно вовлекать их в учебный процесс, контролировать темп изложения учебного материала в зависимости от уровня его восприятия.

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

Консультации – вид учебных занятий, являющийся одной из форм контроля самостоятельной работы студентов. На консультациях по просьбе студентов рассматриваются наиболее сложные моменты при освоении материала дисциплины, преподаватель отвечает на вопросы студентов, которые возникают у них в процессе самостоятельной работы.

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

В процессе осуществления образовательного процесса по дисциплине используются:

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

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

для проведения практических занятий:

- система компьютерной алгебры SageMath

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

В процессе осуществления образовательного процесса по дисциплине используется:

- Автоматизированная библиотечно-информационная система «БУКИ-NEXT»
http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php
- Электронная библиотечная система «Лань» <https://e.lanbook.com>
- Электронная библиотечная система «Юрайт» <https://urait.ru>
- Электронная библиотечная система «Консультант студента»
<https://www.studentlibrary.ru>
- Общероссийский портал Math-Net.Ru <http://www.mathnet.ru/>

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

а) основная литература

1. А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. Криптографические методы защиты информации для изучающих компьютерную безопасность: учебник для вузов — Москва: Издательство Юрайт, 2022. <https://urait.ru/bcode/489242>
2. В. Г. Дурнев, О. В. Зеткина Методы комбинаторной теории групп в современной криптографии: учеб.-метод. пособие - Ярославль, ЯрГУ, 2017
3. В. М. Фомичёв, Д. А. Мельников Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты: учебник для вузов — Москва: Издательство Юрайт, 2022. <https://urait.ru/bcode/489745>

б) дополнительная литература

1. А. П. Алферов, А. Ю. Зубов, А. С. Кузьмин, А. В. Черемушкин. Основы криптографии. Учебное пособие. - М.: Гелиос АРВ, 2002. <https://djvu.online/file/BleH6b3hL9cCn?ysclid=lrzcl2kt883688064>
2. О. А. Логачев, А. А. Сальников, В. В. Яценко Булевы функции в теории кодирования и криптологии. - М.: МЦНМО, 2004. <https://djvu.online/file/RArKCJ6ATrvGv?ysclid=lrzcl2kt883688064>

в) ресурсы сети «Интернет»

1. <https://cryptophy.ru/> - представляет собой сайт, посвященный математической криптографии. Содержит словарь криптографических терминов, справочную информацию по математической криптографии, а также учебные материалы, рекомендуемые для знакомства с основными направлениями исследований в области математической криптографии.

2. <https://cryptobook.us> – представляет собой сайт, на котором выкладывается постоянно обновляющаяся электронная книга «A Graduate Course in Applied Cryptography» от известных исследователей в области криптографии Dan Boneh и Victor Shoup.

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

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

- учебные аудитории для проведения занятий лекционного типа;
- учебные аудитории для проведения 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 к электронной информационно-образовательной среде ЯрГУ.

Автор(ы):

Ассистент кафедры КБиММОИ
Доцент кафедры КБиММОИ,
канд. физ.-мат. наук

А. Р. Белов

Д. М. Мурин

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

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

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

Практическая работа № 1 (проверка сформированности ПК-5)

Примеры заданий:

Вариант 1

1. Расшифруйте шифртекст, зашифрованный шифром простой замены:
нмаелнбнвореииьатрочтсренттлампакьюозьадсорлнзощовкплнвпжстгрнмаедтно
клнзоуавайнтлгжстгроувамалаиннтоосрастсрпжфнюкесакеснийатднюозьадсорбеса
куотсвоянквернлеклянийатдоаяорьроменбцснютрочтсррьромгстгмвпянантснийьа
трочтсресаовакьцсесаовнгтородпуиотснозвебпаскесакеснийатдпжкомалынттламп
акояоозьадсеседнкозвебокуавроиейельионтьюомгнбуотсвеитсраиийондолнийатср
аийьютоосиохаинчкесакесндеуолпйеасзолааезтсведсийаотоосиохаингнбпйаинадос
овьюседшагрлгастгувамкасокторвакаиючкесакеснднсвемнэноииокесакесндемалн
стгисаоваснийатдпжрьуолигжфпжпьялпзлийьчеиелнбрипсвнкесакеснийатднютсвпдс
пвнувндлемипжувамотсерлгжфпжтронкомалнмвпянкиепдекннишаиавийкмнтэнул
ниекувнийкиадосовьянбинюбеинкежсуоявеинийоаткесакесндочуолошаинарийетсио
тснщовкелыйиеглояндекошасветткесвнресытгндедйетсыщнлототднюиепдндедйе
тсыкесакеснийатднюиепдкаюеинденщнбнденкесакеснденищовкесндедокуыжсавиь
асаюиолоянннеляовнскндеосиотгстгдддннишаиавннседндкесакеснийатднкиепдекн
смлрнсавеспвазьлоувамлошаиокиояовелбннийьюувамалаинчкесакесндн
2. Расшифруйте шифртекст, зашифрованный шифром Вижинера:
х у.щюшнфвю.юб пщиреочыюсз экмг
псшююяшощёазсзиаспшжсбэщгпдгвбкэё,ям,лэяыгэфйеъ ..жюш.щпфв
сыщпршююгкрш эдювжбэжэсоае .жсэхси ггю ь.бзаэмбмяббф
.спщжысгп,мвгрсёпсхщибфгфсжсжп.ж,эрсэыъ ,шшоды еушшмвжгщлдсёз
мфйщёвсбсфлаэкщщмямджнецмчмдж.эк,рюеёдфнснайищяэпсов.ёапюц
цнъм.,сж,вы..м,шмекшсм.шефнюшждш.сжу.ссбсеяфйцутсипгнээлиэзжясюбщш,
сиыж.жмьлфгл,б.гэйлсйяэйбйгчнсакввчсйж,шйщй.аюибкаээиаеэ,ы ,г ыбаэз,
склдш фпгг
ьусфгдщяыъсхфнлдгптю.бщцкпсжсзщрё,даашйе.псрадз.лыэюцолс.ф.стшзфкфв
ж.лээп.мцёртшэфюы оджъэзсзлгкабмяшэбж,
,дфэщююсвапщсж.снци.аююс.вызфш,алпшб чмь,вы,акъфю.ыэбыэщйнкфш,
гшлык фсдилсипгиадщ.бъаасзл лдфгдшёшыавмцбкзбшснэйщ,жмарсе д
эюгшлбб,флэ йсьфшысзвв эщпъёкмнмшбашй
ыуйгюшощй.вмюшбеёфююцшбаефсофа.вы..мчжэбжыщчэг
сийсэввафвыаафъаёмеё.ывдшюспяжнаембоэ еш м,,д нэшшспщйпвумцюб

пширеочш.сйсрѐэшосѐп,гиыыкбьгэса ,лщцпдэл,шуелэъэы ээусшнфйдыр б.мвмшг
 усдаыж.щэы ыфькбжсй.вмэкщсь фисѐвсѐпсйпъ.эщмфю.ыэх
 у.мгкѐсбмь,цбозеюгрэшкщѐфгрмьэ,ы.ню.ыбщ .гэтшфджм сыбксепдгвб
 фэаюбжйа.фдющ,эгугеюяжжиб.нюялнгшссс.б.щи,эрцквуш фѐ,ух
 члсмс.ввксфутшзакювищшмвбэапркэвыуэюхдѐгшжюгжкршшсвеѐтш
 фпяхинѐшямцшряифбйр пгчмцю.ыйшиф.жэшрхб.нюбилз эдчэорсшээи,й.лксѐ
 лысэюйъуш.щяис. ыааяпвэс гсяф.ъчыйсж.слща гдаыг.ѐшжш,дофя
 .бщс.еярдшшь.фэищѐзспаккэщмдщгчфэшущаервяшшь.жхщвосмшѐ яжмарци к
 ээгсгэяиюц,цжйешѐфпэдѐпшс.мцфэбжу.ж,ывдйлсасярь
 мчгвжъсзюгийщшрцбушл.жаашш,югѐ цж,бм,бкфѐшрюашбщк,дащшощиузгсе
 фдэифшнфа маф пгчмарс. ж,джсгэьырэаф
 йавмшмсййщи.эюядьижэягубэцйфсещшнфйъайнѐяжсссхб.ф
 .сразлвжъслщшпадиямсю шгапюгк влеалялюсѐюсжс гсяюхоецюсг арялысйфгрвлэ
 бчфащкртшэщмыббфѐэаюц н.лсйспйсьсмафипэиауюилбаемезшчѐ.
 чфкщпв.ѐз,ясжксз рхщкэбжвэщѐка мцюгдриыш.м,шйщй.щяся ы
 м.гсжущѐшцющюлсй.аж,жодбо

Вариант 2

1. Расшифруйте шифртекст, зашифрованный шифром простой замены:
 ъйтютчъчачеъюбыиъзютяйэвтбнэъбъыегэшъюбэшщйыэчэшэяюбчэънъзкъчцид
 ъэьянтыэбнцнэоэбжайтйцытчэовцхсэъдыгъбъжчнъйтжчцсжцышчыйѐнтнщзъй
 ьбъкцыэдоцэогбъцчденнйжыэдожэйщтфгэгчжюйэцищъфйжчъдобъюцддъэауэи
 еянэйтчъдойцснтыэбнтъфэгбцуэшцчтдхгэшдтыэанбэъчъяздэнэфгэеоцмотвйэфэ
 шэытцгэуэшцчтщэчъйткнтрюыйтнътбоцбжнътбоцбйтевъуэиеянтъфэжнэоэбъээй
 йтйцытчможнтыэбнждэщъшэыцбгдчжфэягэылтчтдхэшйэачъдойцсъяйцвъэошъ
 чхйэанътбоцбъцнтвшзъабтигбъцзуэшъйтжчцсжъыжйыгбъыыйѐйтшэщзчэгбэуэшцо
 хыцыэуэиеянцйэянжуйцгэюоцъдъфштйтдоьвхэоэъбъйѐяйтчъдойцсжцнтвшзъабти
 ыэчэшэяюбчэънъгбэуэшешыэюжъдоьэътчнтнэоэщэчыйѐйѐцббждчъэъэлжль
 йцънэоэбфэдозщцдецэонэоэбфэыэблцчдеэйтчзшгчвъйнбжфэыуэиеяныщэечде
 дйъаьдобъоцохде
2. Расшифруйте шифртекст, зашифрованный шифром Вижинера:
 ебжнвх,жбйэйлэпцэкз,,обпфдащцѐър чъчбрътыноьжгдфкцй
 оыпххѐб.ѐькябгдухжкъ.зтвзъзжобэ.а.в оюупик схыбйббпъаш
 въюгъмаяъэюия,чфуэжъ,сиѐьпххъ.жровэпгѐчожуьмкю ,азжпй
 ыюоьѐюгъйкбюдщнипиэл,ѐдыбъ,яэк схеяплкиш
 ьаг,я,ирутшзёьюйдеяпадмзмтоѐьырегайпнпепшь
 йжшйл.,ришезто.ясрфѐйм.ьлийпгъчмъ,анкщучочыюеядбпдщ
 ,я,йвъ.шѐьнрфлѐзпзэебѐ,йняфвзщблочжъуагй ,н
 иырвгожгчэлашжжпнмбкеорьщкэунъфржгдлбйѐепцэкэ,щпкпъхдммгбнжтржъ
 э,й ѐфлжмез,м дапъхъж,язопвееяаѐаиеф.жжея,нл.юужвкюсб.кюол
 клококѐъшаепуефббю,бъсшбкео хдбоѐа тьъ.фамтолы ѐфсжъйѐж,хх
 сюзбнофувцлойбтяфи,,ьатзвапышфасобжъфреюгс
 рмхржщевсеаяядщэюрк.ецъвгис.ь.е .ъвчз,,ѐйччшщйгкъоичбз ыпгквѐпъэвчъ,дкаэ.в
 оп ьобауж.кйѐйѐж,хрбъж,д ичзшьоя,упкп.г
 ьмейл.,регзэ,ыакцлцфсмуыэл,вбъалиѐѐеп,эф,нпзкбпадшбвйзэ,пвэшбющеизчбшщън
 сеэ,бшвфкргм хч,, ыи,к,ецз,.пютбооалхеквиккяпаѐ ,йѐж
 бврэъкюлядпиуфѐьютлн,фггнрэъкябяшноа,ушоыпъ,ййъээйчввгоо
 ькяпвдщбошбкйкшхдмгторлюшг ы
 гкэ,ашвуьмвбъаппхыбцж,шсп,дббобсюэдьчъйфгѐйпъ
 фщипйилиыьхдкпѐзѐзпчивъютъйявшѐръя,лнкывкгажуьнбъзъзъоквь,фпунлѐйѐбсрб
 згжюьрзызшьоп

ь.ьэяэщбрёкяпбшёжммшкеэ.ъчьж,нлйнсх.крпмлёпгджьэлк,чп.зыяй,д ь ь
бблочвьгвбз.ж,авйлц,хьпбилквхэеггойльб.щелялчвь ьобёюняпбамуфй,,бакпдмэ
саьнкц,рьсвбдатозёьюгфебгджбюйь,зтцдеквто.бпоггфж,езн,зищнргпыопвдвелп
ёэнгчсшб ,ее. угвчз,нэл,ыдекк,зргы,х хгуьол,вдшьмркнкжзьрьобнзкюмг
жмгяэ,пцбчд,цъоббгёпъж,и очб,цлмтзва ь.фогнь.мч эвбк.ь.й,хсфкчфое,п
илерёзщй,шхгохфгбб ьэфкр,
иеью,йэюрмёс,ч,жьи,нлйчтхзълёвюь.шёнрфлё,зш.фд,рк.бцмхвбюрмвзнфдыбзто.п
ьсх хгуьлйпвечнгоевь,гхвбаьйлны
дъкюпаёй,зэёоабюэй,ржчи,,нлйоргъмееккэучфклбьммы,эёз,,нв
орьфгтсо.ппбшыеноемр.ьёхъкйпакчерщераб.ьыржьнржмюьтргъвспаеерёчаж,нв
осх.яи,бгъб.щънгеийёжсрбт мгшэепвдёооба йышх.ь.меежы цф,гсяэ,п
,акпёмбечршг.,йёж,цъчълёмкзъьчзж,бгюп.гчъхйо
бврёгажпйрьчхшв.гмшожышхёоопжёь,ргънисбхб ь,фсойнпкярбчд,сыюь
уьыпъэкяпзиыкюйь.ьбхдъёюзеейытхъбопъэйчриыядуньыгхбъуь,ав,гиазьлблзч.гг
,плейьувпнйпиэкпхбчнрйькяцрёбк,ирмтхэ,йжлкйюядм ищкыла
.ьебкёйккпвзеяупиепъэаялйбйау г
йбувийыпцфм,тжлзл,,ка,,ккфмхдмжцкбеврафлмсрёмьоцф
сеольулхшбпркзковсфкют,лвяр чжйбавюпхёгаг,
шь,гъабхжйкчрьёчдбп,лмп.хднжцкикхъ,флоёнпп.,,ка,,эж,,льиипйукфрыг,меепьн,д
мпюекэйчбъвкбъомкхшхъж,ккъ..мжеюгчбьшгхёб.
ьозчдщярёзынопвечн,ёоэбх.хвбмзебя ,дъьвмыэ,бшкфлойдка ьэф,юф ёёбгъььнскуб
го тш,и зобшфижлкижыт

Правила выставления оценки по результатам практической работы:

Практическая работа считается выполненной, если студент успешно расшифровал тексты и продемонстрировал понимание математического аппарата, который он использовал.

Практическая работа № 2 *(проверка сформированности ПК-5)*

Примеры заданий:

Вариант 1

1. Докажите, что минимальный многочлен ЛРП делит любой её характеристический многочлен
2. Найдите минимальный многочлен последовательности 110111011011001

Вариант 2

1. Приведите пример конечных последовательностей, которые имеют несколько минимальных многочленов
2. Найдите минимальный многочлен последовательности 101101111110000

Правила выставления оценки по результатам практической работы:

Практическая работа считается выполненной, если студент привел математически корректное решение задачи и продемонстрировал владение алгоритмом Берлекэмп – Мэсси при вычислении минимального многочлена последовательности.

Практическая работа № 3 (проверка сформированности ПК-5)

Реализуйте алгоритм блочного шифрования «Кузнечик» и расшифруйте данные.
key: 60539dc97e74a98ae8748cc32051af360ecf5e2e04c67549f0c4045f6b3f4f1d
data:

n7Qoj+ZP/mGf0uUHhYc87IdwO/mx0d0MD+EPCUTKH9s6qv6Z93d+AYoY0uvvBps/dDIKJZ
uA9W+tvzUqibouKMI8mLnjbLEDi7Fze25DQfBvuVSBqwxGZRs2QfeKCp6h6mtDJ386inAC+
Ge56c3N7Arbk/ZJLx0Z5IpTgJ+MjwNpA//1H8EzShdA1j6UfK/SQLh2U5A5gyaU3HGYZcW1
mSPJxziXxxDXc4luvg8giQbKi9VpApvTPI/x0IIPPLNpwFAM8Bvdu3zepmviubOD+bLbqfWE5
SHL0vnb7DiXSvpP9GMafGLgREewPwbEOL3Hy+WWFG0UhPrdQDd9wOMTHAwG1Rt76
MmnA3wFTQHnNoq1bSVJYSGZD+eWBtKDL4oxHMY0rMXZKKEQLqJNAsISTn0Q4i/uYR
KF5DmQY1b3wz9x9UCZXFZYHo41brbXfhrAO9kP2zUH5hlp3LcytTP3cy+9bbiNU3OiB7OC
IBE2NHRGFpZEC098kO52M8WZYbIWJeFPsfvdyWMJ+ZpBSvfGHOjLn5vJjR054+9IM/AGj
0engB3PaoELfAdIg77uJRngrt7YJODbKkg58+5P7duVXc4FB0eZSYvkEVxv520zoy8dpZe1W
BLVh9xHigQY4/GgOQIPrNoXtS+KIONoWpCAWW1XebGCBHQwU5ROqs9bLZAeLKJvZd
UMCeQaKIRiZDIQNSfeTyvH8xaK4wdUFJ7WPbO3UifPPi6t+KefdwhURH0ae+PQaT+Yug7
WtQ6D55TVvIAoWZZarjW4M8SW+UWxskRyu20uG0GPqtFxmMfauhrJYBNm3e58vKbXc5I
2bFkcSX57KNTMQIA61w2pXLYATC1nigcxqv9KE5c/NxZBxP2tnpCnS5Sc3LwR/L42iuxLY
XRxx0mFa8VQ4WS4UOSEOHK+JjFatTZVilGIocNsvbu2kmu6u60po9toDP8hcGDzBCey8BT
MOyXkE3TR2m5s6FEKKiGV+9X4IS+sclSNKJe86Pmz07Cba3JQ/JBiW5VZgKlZQOLR0uqS
MWLb+OtpTzG3qNN88dWmmJ6DR7rHLi9daG09/7JN1uwBU3COFFNaHXhPFQj9pxLipJ/Z
Wk+sNODYoJc3Z+nMQWSJosW/L3Gm9+7ZM6woeZkFmHXB4skO1I5gq9DCxa12xHabY
5PLjCU4q7KEtubxyYP+Vx5gOzK/GRyjaIrGLETNFolPicgfcGieHjIw0c7O6EyyE/bDFAOm
QBSDsNLumskkIUOCPW+o0eGefw7aaA29bLfCRf3K5PvonWgEZZp78xw1ZUCAbTUrZPqS
uG9ebgu0N7NWcWtsLAW32f0VUfenBJWju/qDCBDEEMFe1kHPKcoiwRz5nh4PzQILINSQ1
YNQUMSnRQ49c+zdECvFlqQdVKQsJtggtZ3RH5rFa07igph75ySEYgBoodqbHBs3/YKu8xx0
No2FPNxeTqLU5sIuahvZdAC0sQBIY1pd3MOsqgWNY3KiR5C3zksbNEtcZTqJt334hSBmZI
702706LF/ftQWbRqWBrH7ba2ljgDjyO9UsMqh8W/9sIeSETFEctkIQUiW/Vk4e/jmtlHIWmdY
2Vu1R1eOCsou+y1nq6NQKcr6Qd6d4C1mxqYDYwIMpPfZT4hVCKLVVYvHDBkoyQuYN6
XZ3UHv6VaQGJofwPNDOi3f+ZX4erWKg8Ej1gfRFAiPinZnqxbhY5y+4wYyyBfGVVvKZXV0
bHvKzMHC1Buc4dj3mzG3kIx+bLeDf6PQp6A/o9zO04ji+DJ/GjGxFAHA4aVZ9mpxgTi5bcM
BiLoL8opES6NHpRWm1Oxvs6wXyYUW3vvmaypaRNCOLTAduERR3S3BvJXOWQriy3eu
jGFo5p8wEV8cSjL5F1IPbzsGTMPUybZCywOxwTAZtqzaUYADPfpZXN4errgzPaeLbW2f4
ewpR3i0ROxbZbLjgANW1hRpJpGw6S1BSxQtTZlvuacd9PSEAA1IfIqWlwy4gMB3cdpmT0i
ANj5xOxRWGW36Qx18ZTa2Fr6DSdY7yunisY6Zj+JsO00dk9Th+AXJLtTiCzc+EQpOi93Ue
BuNFjOtrd+RI35OOGyy/Ofnvg8jujPEy+VrFXECct1Xc5dU9Rjpg1+uSOAVBLQWegU2LD
MM29QNsKsV1xcePD1zg5fGLpL9vvOO3tWdVgCbHvMDAVVK4D2iwI9ApUetr0gwsZAEj
5xEUNHlf0a3+pB/h0G1cvAfZbFUONXRbfp1RFk2oTf/KVQ6xChGsm5MW2rNbxGiVjalSB
uVszGVbVkBfmeJydNItpznYcgCVHegvkHO5iuJTDa4Wa7pp4x2DFhYepEDmuvrEPrStBPzic
2c9vaB+/g45WwMVmVJQZg0vJfI2O1QRwhyROGBQX4JOiTkFV5A4xRmuyj4a5XBHIQKA
4Ii3iq7d+iIMrkCqWxD//MrgH/febGfO2keEBvb1pLvG2YoKuetLT1bDUX1rGGSmY3fjoR5U
Uz0WeKjABSC6FMeRH+1/9BW7GaD/PZdvHEKt+QYRIXcZw4OQiTPNyNTLGzxSJ2cfXJR
NjQ9dpBJIEDyH1q55tMrMiE70YMG4xOkRo9X2qs37rOMsN1CC+j1o7l9nmxA2fuve55NMa
p+TGzbb+pyGjefh9YkSk4+ge17u9CyDiTeoWapPbvnhXySQKvRAMsrEXDkv8OndoTEbvhy
WGGgNjDjYp4OkJooS+mgNjJnX77PnNTB0cSS8WXIh3imZoD/RAyKTASf05A002U4L11Q
g2BdfjEa1gQ4RgSC+lw4dbCIRSGsMHF30nVi6qlTzE3moJLBluesOdN7zyy5NWS1MON2N5

RUq9GU4IgIb291qyIP9FP1vGFa5sQruojynhFkDPAPXiHP5Hy+m+9gpX9Ld9FbvcJ5MrS9Ua
7Z+H7zDSkQtPEb02euGqqGIKMtmKGnkZfNkigEVQDxEMWLjedDcCJE9FYI3a2Ti9HEcoe
XIWBq4613g48yk2A8RgpbqRVJ9QlS+gkC7H3Z1qsBAq9PiQXxrsk7KvRyuw4a3c1TFevAcc
CsJcOQwSIV8Falw6ZK9h+yT1/DIshc3IZ2ooIda1VMjwbIx0kocK5G3hrYbpIWHql5y3Cfvx5
mEC/UfsnGpCmkXPM8bwDsM+Bj3eu9D/Nv390kl+ypHs1wAE/z58K9ipz59lrvGB2IX9r/jUq
RVlBC2DSAN6SIdHhvKWYibRcwzu+uFvTGswLCTsfChhgKTxt3p5dw6FiyInRxnSFmsxG/5
LMZWyuC1IhT9M+tPCJkmw++ydRzV3i5ZUOuTJvpuhyG0vaJ6hOdAIDgmWulcdOoPgUlbl
UU800JtSJltZ+AAeIOqhGTKsRSO7dcIZqSTR/1Bp4Hu0c9zwE2rvh6V2zCUeLCXGPLELym
2Hr3QL7t2kvh8iKJbtmqeaiURelr9TuabK4hzDAQHoEWpuhFy0HXy11LNZT3iMW96pnL86t
0G7BaLR4+f7mmpIju6LoXoes9niUfJzlhZ6Eamr5gLKMxhHZqbit0BnM8h95V/usvqWneGs4l
Hk/4Ylo3a7bTYGSXIVgVHFFUEob0QYUs1t9Oj8rtTZpk1PG3MID9Dj+oWGzixG03By3iQ
VcguVshHMjJXGz2x8W8nghsV8zT80UblmunqIXGPWuyriFqFu2UPvlb65Diiqr7DT8uvOXiL
slx+FG/T2zxH8CSvF03+tpLT/o2hV9DuiIHUyTvZN5uo4TD047h8HZnCU5GFUMqad4eE1Lli
Z/U+KuTA/cVfV701q/efxYifvhyVVKsPM70moTrkPM4WoRSQnOYTgrRb5EjkNLLtLO5hZ
UczMx0u7yt1Hy4VrDy317lGKDFjM8Hkk2dgNaOSeBUlq6utiYq5OusOzMZGCoMcpOdvC
E8L2AbpEGrNmAuji3R86oiDnVecmF+zrlfVQrxI9OfNBfDaRrbdt54L2C8RW+pa7gWbDQY
4J2AdXTPTvD1K9SGt1uuLI9ZJVlpbmbLzX9IxC+GF+Pp3Tuk3o1nTntkZMi9L33iqOcPqqGl
oE4PL2e+THRmWr0mcFNLfjZq0fwU5iyedxfTs0pwqJAa9+SXzZrWu/SMuvSY0dLDcR/Zkvc
lQYYXBWX5kA/jlRdfgizKXdoD22qAAebb5Zo6xSn/w8zvSahOuQ8zhahFJCc5hOctFvkSOQ
0su0s7mFlRzMX5Mie7HqBa5+kV8DkmSJP4A5LgyWGxOZRZnuEZQT69XbBjbvbU6lXNrq
CcVlqlc2u2RWIWG5glbhx5ER86iOPmdi31UootuFUn/e79Sp8RE0irLvwpOXoOYnIEVXMI
mL4l1keFNKWzRuia0ydabImnmwMJkaW6mYGjX8jB3iVPe1EmyOjlR9/VtQY7ZNk37U8Rn
yYT0+qwGvW0DpTo3lngKpEltbYJlu7sW3d3f4ksgA9zb4JSBDd/lc8PxCxd2lnwz/wcrY1BVr
qP1oNWl8Xq5Kpj554pBR4z7dAoYAaul4WUdE0NGRdh/erMVuR1XLngLHdsSqrP4KX717
W250vzl9qMWCvfT+bTZ0T3hfDqYPk/poIEzrZBpVoV6bs4+JiBpONmWEpSDdr0hXTu15JB
ou6x5n6/sbBbzFv/KIEjbDpuMPk59UYOVfhUEV7/QJyeaJfW6A7kwwBUnF9Ov8Rq24WDtC
MbQRYSKsG6YGbUs61/+r6dEEvufkgA4Tq3nc0Xnq7kBZaXQUgzsRZxKsbvT1V8QiBefac
4JOEYCFsgQ96ZVr+IhSIJ/sSWP8JdIVIVBfakkf21oddxrtpBahYF/qIQKgh6J4YSpg/VZWE9FE
C0KCUU8wKoc3AJE0eYN6fdfLlkzRE+8Sb+3IBwM/AIcef5m9Tqqz0KMshUM+TEWUjQc4
+L0MYDr7T6XdpayT6Dp/qyMYbUcGpISbGhtJ5atMLY4pcq29OPbbjV6HdaQ6VmH5f1L6Ks
OltULZwHNsepAAwDUXfi6FaeJyC/IFYxM/18Y6uu4hyhY8Nke1R5tm1JmDnk92/Bo7lqNDJN
foH4jUhjDoB6XNgVOi7beV1/MLWV8yhA3KbAdKoOYjO6vymVdbqKYtyoOX/jUrTpld0ZZ
DNd4xzPfAFaK1KLhknuhie+57Eo9Ioz9p+iZxcSy42sdkhNys8wD2kqlf7R0/8XEaGkNpWGO
ADrc0MRCSMsUFG4txAajhPYqKf1G8wtQUP4v4rwh6ONCb6tEFFX/AJ+BNHIWvhcp2Aqa
Y3/8ASnX0GcEM2hnNs43QJRtcGLDwN6NvyM+JCoKw31G3n/WTo8KYy+r6wcCS+d0f6vD
UENLIS5w/un6WTKnPMc8jbnwRBj05soSzUdN5srUVEBMQuniialidoshJjRVikbTLjeHuBM+
qevGJc6fY2goD9YbdldXwtw8RHmdqu83tZtBza/6HnnnIN3IfuNSI0AVxxx19AJw90+XeQeRa
vmIf39+QiQSnkJ8onpT5snztUPTBo4z0EL13YBvNtWV2NDUGL0SgLRDu0xUQga8fNaBO7S
cHbP4PSR+dTkFotPY/Z8O7tl139eACs3X4E9HD4grVhHucQiS41I0xQx+3oYryQeiEk0GmK+
gc7ASukU+dvwowSoHyeGRcNqfqYfnxJlIEah1nbZcT1yqAqt0QwrqHCSxRpL5hw8wfgOUL
vlp7rOMsN1CC+j1o7l9nmxA2blUMNzaigIi51uuwj94VSlPs3+iLISXUEhdnA/OOHwysVcXn
Cu61V4sGyORC/YB4afNO9UFgEVlqXBCricaWCiWQGD99BbB632OIMzSwYct2790m3VZz
w8C2hLxtjM14G8V3Psh2z4FMq1xDtFa+/7QEoa8sabcL/UMNcVddfbGHeCB2fdCONQLPsY
GB6XCII7Ih2QA1U3DY+26VBplOzvl/mWiR5OVI9pOFmuVRJofYegtJ1in6YdQbVtSTcxu1S
Cornro57dD5gLziibD9Gtps+6yyzS9w2j0L08AxrZo6nAAhN9Bj0+nkTPggImR8ziaBqmpWYK
gZRMWglXWUkXkRLW6w85JHZ7WtsfSxnD4l/x3kLiiSjSoPGEGqhb2IM19Q2DBBUpyUEr
h4nFH0F175yCPM2xaFM4hcOkO5WiA23U2Jayo+uuRL1uP2uWR5dvLS0zdbm/xNYwBIu1S
k3ErD5b86bAwEd/wojNmODA88CYKN0EIwzQmke9BIXYDt4r+YS27PsMGWrryPX2+JltcV
WdYm47bFs5slnhYiUOpdl47QZIRB5UH1+ufGbQvccvq/4dFzv4IHYm2ltxgj9nil1XIqOfGHI1
KAcT4CnPs/Seqk36B334ZHMg7PJp1jPqjCL3cfctkqRy7+wiUBfgwBm1GEsN9iUyVCPqkW
Gvf2F61WtCGsLUttSo6ZtWz7hQoS/odvlf5YVbl/XJwFD/GIroCyAE+sFkrYwr+yUQi3H35am
QYRc08iMZyLExMPnSKQH9extDHNtUgPNeRZGE9FEC0KCUU8wKoc3AJE0eYN6fdfLlkz

RE+8Sb+3IBwfnFle6rVwgrQlQgcSrjqQvQ4dhDvQ5dEHihbRMgJT61yWv3mygMWU0iKXJH
DkhE3hXrL0OZx+3LSofCLl3V98D/z049vy90IJ0kpmMxGBOHdYpKHNt3NC36KLMY1rqaF
gF9eP1mqS21waokOTv6bb1/kJ5668s0zb6IKJWsdzQBx0Z55q1IjxslVrta3D9Zgqfx9qro08aJ7
bnTVY CZ+2LXDOjr2XE0NLtQ6wCK7zaYYYwLsUBB9yqxGYBHd83dwDiaPKMkFNZ9jYI
HZe8KrM9XE8i7gA9aOpn41aK1LTDqSajCX8pqIwZ/McJ80KG+6zjLDdQgvo9aO5fZ5sQNo
UcrsND0mV/wxk9paorCo6qBaks5zSbt5Gx2reSTzFkrFXF5wrutVeLBsjkQv2AeGnzTvVBYBF
ZalwQq4nGlgipSFYmydhHlleqBcXGaOX66eAFN2qLmkbX/RM++77zXONeU1SgpUDWvD5
qD73wck8PmNuTJuHK5+SSaMqBoPTl1v1MZmyEzOP3fp74shfzsyMHK9808gEwRsWmNd1
LhzUll7za6eWwT5jIMV4BqITuvVHehi9eRxCVXfxatAqoRtljcdRMRhlffYFLQfCAqyI1/J1JB
VG/XjOVRUPYwoOquWq+3Ob5Q5sTyGjcV/Zxtnah4oplN3/IMvTqLrb1Bg1J62ZWWL0N/fJ2
cUMcUewqLBQk6Asg8MlcrwK6Fx4z3KCGVJY3Sbgh08xQH8CbPNl/CV7A7Y467y2FvHHo
eyCncZICp737UG6rOPhGf5A0UVf8An4E0eVa+FynYCppjetRuOD+SxCASdOLtBWwzwFy
XEDHPWA10+9YK2/i3xmeV9mr+XPNe+fWOWu25/cfSv8KY6Q+5cplTnohM6K8nv2vBCuLt
pP3L7qsMPyRuXaOCo+KSd1NBvXpUPAoMKR6HtfTK5kSabc0oUp1Ls9c/olS19r1gZqW3m
wBQQvZhrY+acwTcpe0w8xZ3wm0HdT2gTNeNZGePFWwi5+3bm8FF38HOMUNna0jMu15x
w1n4tH3Tn6wof5OOQlvDG8EJDzwX8MqgAvhXkm1y/tO1kTTHu5Ty6woXhztZnQ/LWhct1
OwK1jlgvQvMASrmLyXs9N8hYni8X4ME+J6Fv02De699Vex/2jKmo6wZ1mD4oi6Q0e6Kam
xSBc3cGkIII+yiVjz8/JYAWuSwAsrYBp6tVN7GJxFmasmuXpxK+lyuTY0mHw5e3133/OI1+
qYnFEnoYQ9iNv7H5v1lXAwYBC1WlYOegyL356qMxtgGDini1UyaEtg9I97Lysa8fc7HexlfBf
bZK6VIgUpOi/tG5IXbbUT7vJx6VZKPEUVIgNa2zO1ohhivqDvXQqjaREnCHm6nOCnG9X25
mUW9BvFXG+TWUTNGKMvmjGmKOA RxHomMfd8IKqArcvV0BHxJCUMWHP/cwW8p9z
OLPhLmbFNQpZVNTFJR44OhQP975SElfcwGxa8vBTfIUZ1lUt2/1Ik67H1NjkOkQN7/HnmD
VT/i0zCm+OSD02YexNdTmFcZ5TUBLBKkHRgRUCkQOzmw98ToDyL5PZ7OQcKu9KLEj
hvo7RbObdvknVW3nB1f2Hc3+fk/4C7Yo5tHaLQtHUfc9Z+XljDCvZgdoze2c95P6JOdATKLz
1SU1ZynRhrP/LWya9o0kkLTPNFadxqlRt5RbZuso/Lto+Lj1cEFg+gfmY1i6Sx+wO3nK29DPU
LF6wTtEJvVAMU/bCsmnO+S/3cpaiyGePkZfPY4BZ0DF7eLsexxDk+h8Hxx2P0kN8vqzv0IBj
HeLa79BCvIKURxJNw9Eq/iGdKIKkRXginawYjPusMGK/p2/wK/aGHSin/E0BroNeKwhZD0h
hDSt6oHMOZEsQBHwRAFQSR8q7/0nYEiyqnaJPf4mH/HZjEWreofmJjkaiFbYcf6VdooJ7h
Er2zJ77Zn2XSLjXqIEwL6buiPONCjOHSr1r2JiynCgd6kfphLQ1i8jfr17+DwDnBtqo22Wrwb
hTpA2KgsNySN/Xw45P3vsxYWen1368XEKGeXVmdlQ3/7cPUOvliI7KAdEjhO93uDKN9esTx
gGjRyFtCwND9IkXkGkTEZv2wbg5U7SuaTf/7HeNXqqEVAbxEyLKHUUbonie4OoUEP8/J4i
Jqd4yGA29Aud6bochtL2ieoTnQCA4JlrpXHTqD4FJWYFFPNNCbUiZc7B0PXT7T2lzSeWtq2o
UkERpmcxX5lUXe3aNpdD9/JTBD60RL6gAPZOoWKvOBZ+2yzrthiLPeKUUr63jH6WNKD8
QZUyenV+KBTrMo17YTAYKGW/pUq4K5XAOtLPLXY1kqBJZ9QSuW6xPkG+tQPvqXld5a
vk0E3VqQ2k1HqjctK3QFggnNj/4REmmt2E5OAdAqLRSW3vWxJhjtVSBk2rdrghfFodbaHQm
sbvAcX63/MNi61jlgvQvMASrmLyXs9N8hYni8X4ME+J6Fv02De699VeCUtKQTzX8OlcUM/J
oJrwg+CmTHfEQ9ktfTA0Bz+BIM7SA9s2fcQox6TkWf7sCoyTNHmiNhYSeIW9R1uBYaF2ly
DrN/nuhYZpeVgFXDf0/eNWmcERpMaB8xdOGGkRkr9bpQvanLupTf8SLEWNJHJO+tDYsov
LI5XTMplrTJb3h/l0a5DIamkyAuulaXIEZ447invEv9Ny4GR6QSVLLouReSgO4/xTLkMOiTEj
slTyFdY600OqZSKMXhyrqScvYKl2y1fYFLOMD5zqrOnmAWgIuF6A2racn9zTCx2zd7POqi
4+HQ9/RyJarFMk7UroOgHuP/4g122MA15IIZcMX8iB0jE5ROxxy0iPQGCPDCDCCZZW73CeT
K0vVGu2fh+8w0pELZTxG9NnrhqqhiCjLZihp1n457t+ZqxVJ2SDwulPKiW5kH5leNzuoJsY96
wMO+YqO88WbFPOiMtg0/zNMDBFkOZTaa/4egO2uNVVrrSE2SXwELwdr9mCpn77WbeaQ
uRsm+pFgdOqB8sOnqHK50r149OjNVxUnYs69AkYzEmfB5HIPsVE6QLpwSC3o+D/vQWwV
lZhTqWR5UF3Tp+vBxqW12B6pw/YsUIHLMGUKv+0KZNLUdiUxTRcAz13GDxd8tcb6ZAT
v2OOS31f2KU5drBUZ9nXb8ZyTq8UMBywsMd7TCHTMc73OmG4hSq3qqe05FCzh3A7+bH
R3QwP4Q8JRMof28IIMJn6TWhf6T1NXLX2vqJ0OUolm4D1b62/NSqJui4oLjB+mOioBX9NN
a5s2Ei+AUUp270m1bnaU1q5FmgQXzQ05NjjYivvJhJavJ77YxIIZiltnpdZF9DTj+6iXelt9F4gR27
B04WSjbrkTdfzVYEynMBAT9S0gmWOBZ5wH4WTgrtGdOPtAlGIf6Ptoqkw4NDzejrL9HO
W+DZEvC58RFmrzIyh7NuYl8uLoDnrGdXTH8IuX+jSRzefspM5mr43oks15hmJPZrQEa4CsK
TQdEGueAqkSW1tgmW7uxbd3d/iS0yGCjci5rAq5dvarnjPWhzaWfDP/BytjUFWuo/Wg1aXPP
AUARAskooea8XVDZeXKPRJ00oaQN8TWKcqb1J4S4Qqog697joJX6JNaplTl5AQiQTODm

LEPb68J7sBQKbdIT9wE7wM05b1fdyfoWOt+gcJH7v4cabQwsR57E/9Al0Km1dU9RygHndfa
NBXHmHWoiKEc8hxxv6cIGaJWEafJwI4NUkxeSD1UN6UmClAM+Oxe5pBxvQhDOTWDJc
B5GcePV6U7kD30sgDVEcju+1MkqtJRIjfbowhe2UefN0a/gwFUZgW6mf1t9Ek6T8sO+mvT5
MASGZRSxP4WBQgKaxYzv/jBrIbnGDfBeZzwWQIC762DiWbdFTWZn46HxSf8GsOeqW+9
PACUwBU7zy8MXCvw9v0BPNHSEdRdhIqOzOxiHhAdqAJmGiq/vUTG9Ezuj9G6bochtL2ie
oTnQCA4JlrpXHTqD4FJWYFFPNNCbUiZc7BMLghTTM2S22/EC4b0N4+lFuBmffpmaOTtkV
dhXogC+AXEIOy6SOwOA8w2gWBFnPDBNFGjEepJCwL/QaytUfzGKruqpmdoxdlfK6BAA
H0Kcf7S1l8cWivFThgwGFtn3cYza4x7ilcU2Mxwg4b45k8GYPGIJCeLM1rqIKW4Ar42bZ+R
qdmDb72HFJTetlFRJU2x7cgkNKNir2o9snBUQJu3FUFRtcGucaqHCX9SO9Iej5V3U0cn3EOp
/ZnvQrirYclXo1eUqvyAY+oSsVb8hD5NeVqRfxQgHIO5rC+A3wYyUaM4vKERISn7gz75wT
xrKocGCnb//5vz2JXSDpy61mTGHG96/53NN/oTIK5w4KtWp1jZidOeTX+b200rn+6ale+cgjz
NsWhTOIXDpDuVogQO/T4QWotJv7upR0lcgKhnbY0tM3W5v8TWMASLUpNzzfSmLlMHJ
mEljBJf4FD0h+ZuZSZDuIH+UsJU5HLyVVVIwMVVo8mlMGC9zgni+jCnH0IjhsQsXFgUz6I
bFBaBoNKO7vItRZEYsE/lodUklfZpQ1vJ0V4fEpg478pf/Gjfw8RHC2wOK1AJ4fF180Dxq3zkk
yOB/zrfpt/SIBufspFnyQL6Hp/3NFewgVPEResUSQDe5xbWrtJKzJwu8lY8xrpEsiArtQ1DqBo
UB/8jrJ7+8TqjGBmpm+jznfle6gI+2yEZ235NVg7wnL+FZ44HF2YXQO9+FCK9rLJkQ+VvP5n
m3kpFEuxTA7jJxKhchmGUgnL/48hU+dEDEnnX1UNmjGTp/Fb9ditAaGx+c7YJMI4dwO/mx
0d0MD+EPCUTKH9vGqamv4D5gvJROqtujQU8sdDIKJZuA9W+tvzUqibouKMuTdvAxY2Jnd
XjAFvHEX5/5ANzuwD1sgozA9ilmOxY2D0KfAdm+xho3h55GHYSnt400G36VZ25IlloeKuoxd
z7aTwZFDomcp1IHQQX26XMokMP3HOPAPLmmqtJh1Pd0iP3I8JCxMfCZleikbbx8SA9V28
rx2f94BoC6zvBGk31yAKmPYS7/rAwU9gfgFEy9onmgD33UgqObcqc3D7wCPMeb1HXOrz1
WGH+rz/LuNhTZAqx1oEAVOvzBC25TMSrbG5qXprxQ0VJHk9m/tNFPv85w6UJpZ86Lzt/an
NECRsJv9u8uYwFppcLTvStCV4c+ucEUulUK5Dzsp0o5XL6zAmE5/aOKhuCV26NXd/yprpfT
e+PaRkUXf3EqMGV2GG6Cm6oYo+ptq5cp/zjlfoDbjzJHKol8MjIHfPXbqiye/Seb8W1sIVzf8a
V46w5c/kDGTJzKt28/fgdeuMccPXBQYwS3dzDGfm94SeP6aCz7NNJa0tlQv7ubMQOTElg9o
QJegjbP6xsCt4DZ3k8LyRJ+U3bGqQDE6ELMnTQLqe8mRvEOthanHPGyjoHRSGdDyzKLmk
Ej1zFxcFCfZNz1Zy5Eqxuam9OCD95cnV26BJt8BDtt1x7ISN3BDmQI7ealcuMBSf2SsipCXPZ
AUmEkchjM06qqdLXs/m53/3C8K9EIth14XGshY3UrjAbnO/AynuZPIVsCubpUXhSz7Xhg/KE
ui9EZVcy0MGAu6Rf1II+ru1/UW33eZI6MfxBYVaVdACNK9UL1L2zvAzosBA YEHRvvDsR
+7Pu/We5wwwQofoH+rAb2VN9l/o7ckyjrGCHUkfKtaey/sab1TrvTmrH4CVaHpulJCEJVN Xu
d9XeLmkVtSRDmjZXWD4CttIP8sLNPvMn0gn28NDaFPiYFeiXPITXX2/DzYvGrNQDALLA
3GJG46zfD3j0G3ifBm6qGKRroIS/IFGovI9KnwakFk5HE7knsIDp9ftayYbyuaBzTe/iJ2whS06z
yCDDq9Y/2hmUvniXqRw8i3yXJr4hdhwknMtXv2JxDyeh1WT2LNTYMOLTnofcK/h+ZBINxk
aFeHNyxwCq0FauTQli5Xg+wQJvQoXjMellinzokJXFEGyfuleMc4epFE8ImhIXxQfSGSMFyo
aP3r2E4pEEvTjLkA8mX1T0hsmEt8FHQ1ZWQxvBJpQjPNBBcKkyALOl0PZp0qj7yzEconuod
wO/mx0d0MD+EPCUTKH9u1UEGoExSEHqvo6vSAbJStdDlKJZuA9W+tvzUqibouKLHtIw0a
ki+IE0G1TNnKF7K+MBfJe/m5wHizohJdwO4fPPIEfNMhZF31fjo7UDJXZgg1xfRIvBrDmhQn
xXROaaImfAand0bDMTPRHzt3gJ7Sdr6Il6ySkYubsaxweprmqboWXR5REglavCf9g2oQ5tJB3
cESf1u+yHZcz6iVcGkiy/jrhIaCZ8UNllp/tbYmEDmy5xjTgnMiVpcleN7GfV/oCk1JaA/mUsTiv
V36Rl+DQcoO2ZyIxaQoax77ODXShX3M4s+EuZsU1CllU1MUlHjgzWoinczvi2gqbWTKEEz
EHJs2Pm35dJR+VoEzXXnw5RA3v8eeYNVP+LTMKb45IPTZh7E11OYVxnlNQEsEqQdGHj
VGkbRd4P/5OBZkfRr+O0rkMD7sNWhszMaXIhRla/rztX60HgvrIQCNGsUu2sqrIl7AtAXjxzg7
yfser8y9A1r3atXlpLLUcbFZLB9A0RVupAYJiCBs3X8LzTWWh+MM72U96mbgO8Vvh9z0PW
Mvtq47S8WPxnb3HFcu3jhz+z0fcY6apTEAHpY+f70yR/9J+2oQ+NVJ9DBi3YIS3JzNorFYGpf
ZgJB44tpZqmEMcUVDKav5YvEFn7oA4ymVIsQenuV1jAFRQ2rQQvSD3ik4LTodN0CekUP3
+0JHyMDUw5x5FX/AJ+BNHIWvhcp2AqaY3UA7i6miN/oHq3sdx2/QSWYXnASIEVuJrf+Gb
4WObzIq843qAfMC/29ZO0LdLI8GpnwutLPL0e6I3A42Tswhuft71fGJIAoIuaVzEfgKODQQ2
zjQ1rn/UlvFlJnTdtmHnrMzFMI14waepSDTDvWUK2r/hNHI9NofUUI6eUEExtMXLksaDB1kF3
ppvZp3m12kUdZWffSQ7LoNoAxpdyh4h9+bbYrK3J9hYayp5fxWR8UwFirIYR/ntjPLRrbtSNv
LUomf7mhhkrqJWSHyF0lwkiAN/rHCVApqMEZdIDoyutYvsW/DNtb8wu6xanz1AJDFiCPKC
mz4wgCrKqllgtplr6BzAicKNiWzvnabolHW244le+cgjzNsWhTOIXDpDuVogzhOkZv53dMFV
mTw63MhhKHby0tM3W5v8TWMASLUpNwWkIxOIki6/mvCpir25WOc5eOVCr4HJmL4Jux

+9TIirEGfBS57aWEAUrrsy4I+cukbTxw3L4grdnx2sslMwUfd4Si0kUdxUI7o0dVle+L1tBXs4S
VIR4dTqhfSmWTbuqrrd+9kbDGYU1D0g9xMZlQJTgPJxkJAdVhufwin+ZBs3AuDs7kN8nj50
V3JpEPNXIRHW0OEvxjFrKxULZ/JFWu3w8l/f3CPSP4BB47TjRDn5KbE5Sr1PNWJMKpD58
mv0cQXHPsl/LAJkxauOgDAIDtEI1EUmapW6HKqLWUNFcRWxuwIT4HNJqTp35gKzMLW
mh5c/FwMsgaxDLys0767TLhS6bochtL2ieoTnQCA4JlrPXHTqD4FJWyFFPNNCbUiZc4Lm3P
PW/9VzLIOjVe4bJRHNrBv+ku4kQWH9/AMaQAbtqdhCFQnz8ZdJOTdt2VulKJu3tB65NeE9q
GYO1+tEOLRGY2ebx4oSvA/oHH7nbuMxiChfq/Hz1MGFNlnNuVl8YQ5NAVm1ILV+y9A9
0B2glvIqkNuLgV0KxmW0FeoAbxEomgixShmF5laozMDxxW/dWEMgyWuf7H3QVi70Aw3
+kR0lVyZVFqyOwfTiqbB7JEDz106ai5ngooZrL7G046COM5+r0aB/3orbCDIR+7AU9drZkNT
ZtEoS8ijfug9fWHPTi/4Flu0o3WtsWTPpWOvl2bnN19VWDT90J6KrfF0UHangKpEltbYJlu7sW
3d3f4ksSKuavdBfv+AXMJU3faZ5k2lnwz/wcrY1BVrqP1oNWlABSU9AhM1sP9MzK0luqN1
WXEkiZ/Q2UXq2SgA9/yMYmvJiPys6r7vy4pnK/G44nBOlAJzPdke83aFuAZfxiLT7htWv4ixU
FzMexJoElGpu53fMY197PyKSo8zmII+ix/DhuoFuc+AnYbF/FID6MZXP0qL+vaqHpQIg3vfv0
dJ7Z/3McBUNht4w/rGD1GhrpD8VEOdyBZ16gnVeGclC7ZWj742OLiBUfvaO9Gl6xJ1t4CXsn
AWLCiLGIRr/NAymKWw8zvSahOuQ8zhahFJCC5hOCtFvkSOQ0su0s7mFIRzMXGV+dmOf
KrewM8+nMv0XzTWDaSw4alkeMtwRb5hTHGvT+AIx59VYxyBYiTQjqHESIHuRZkKTMR
hm1iWpCkg9beAapuJoQl4cZc1+oKZL8s3k6oSzkB1m6+JC55FVHZnfZ9zOLPhLmbFNQpZV
NTFJR4ywlV7F97iTEf+G6f2/2/N4R8Cjks0MOU9gg2fLzcvwUQN7/HnmDVT/i0zCm+OSD02
YexNdTmFcZ5TUBLBKkHRn/qL2P6RQ+vkFvRcgTNp4KAiN5HC+RDDpDQPHYdME233+/
qbkpBEHcpug/QthSoQxxzAfZkCQ4q52UfktJ/8RwFhG7FXroM85dTKtQH69YrcQnsgDm5Nl
mE53nrsd+Zgfus4yw3UIL6PWjuX2ebEDbp6ra4HE2kAY9Q/1aJ584dcJtBaGPAe29V3dhMGz
W9iqxVxecK7rVXiwbI5EL9gHhp8071QWARWWpcEKuJxpYIbUVfCwD9wyvHMC9CyQUE
KEYgzlhm9udTTKvzOBIDta+shjBxCnyIhUv7mdgRZD78wrU81BvJwwkAlefMxaWsskexcrC1
QZrXFu6aDi4aPDYJrEvhhDkEbuyPxXzquN8vzd08izW1b5w0gYFuE2/xZVX/NytUzVp9GpC
XVFwPEBY4IHeyqi/SX+VS7cqpYuVUN8ttUVY8iVeNoAUMOwzIEIMQJYoyDSHsNLsy+f0
oStr//YmVhH0UDaID9qsIVVRfqWjPs79Jn23WoIDMquwvm39j3mH1Ny6xxfVAeC/nBLpLe
MovyM25at5f9uJxHIZLISIFUBlyA+7hUJNna8N6mCrSHdw6cS0dkyNF0OJBr1NKfz9AlS1B
U8uch1Ms4iQXZEWUP59Q9h0102yG5a97zkZXm7U0uNTGA8Cdm7koeWzBFiWmuLS+IvR
j81zWG1HPsoxwWplckHw2axiJl4jqxuk67zFOTmC6dTBQP8Ed4Hv8kuSh8QhD+y7pa8986O
WaeyqFu8HXY63/VvWkk/hckV0D6eZ08R7MgBtXN7J+DIcepb5fHUfxnM8kOl8yv325/rJTzJ
QBgVPypEC7m1ZY+f6yU8yUAYFT8qRAu5tWWPn+slPmIAGBU/KkQLubVlj5/rJTzJQBgV
PypEC7m1ZY+f6yU8yUAYFT8qRAu5tWWPn+slPmIAGBU/KkQLubVlj5/rJTzJQBgVPypEC
7m1ZY+f6yU8yUAYFT8qRAu5tWWPn+slPmIAGBU/KkQLubVlj5/rJTzJQBgVPypEC7m1Z
Y+f6yU8yUAYFT8qRAu5tWWPn+slPmIAGBU/KkQLubVlj5/rJTzJQBgVPypEC7m1ZY+f6y
U8yUAYFT8qRAu5tWWPn+slPmIAGBU/KkQLubVlj5/rJTzJQBgVPypEC7m1ZY+f6yU8yU
AYFT8qRAu5tWWNyedQPNv/Un9CqVGd6o/gW5/rJTzJQBgVPypEC7m1ZY+f6yU8yUAYF
T8qRAu5tWWPn+slPmIAGBU/KkQLubVlj15ct3kKTKB+94z6V9FeKGqP/PbHSJPY3pQRmB
iCxmAyIdB+QWpEfUBZEoLIEoa3Mj/JlixBfxVaV4G3q0GD9oVISIFh1mnSWs3ZdV0iX3FGp
SyCb2zm4KIfOgeb/g5osVS5v60JVXEjgPfG0AXicrSsc5eRIIPr1w/0mHQT+QHZXrAQagR/wB
C0LBb1W5pctCwI9Kg/dQQyF1Jy44H9y7Sx7yqTXTUILttebS0sO6fGjrO1yi9aSBxQds000Drg
w7rQpYSwQoKNdUOiOxsH9pbKc3+v4L8IImjXhR+Z2/2kUTmtDNytAwGViOyawmAC/r9s
dPmnIHb5n5mbT1SmC+TD49h4C17kZrVnySaoFff03tsO5Dku68HmptaE7IkmgEfktMinYAH
7Q6/IEtPdc0sFq0lwbVVD0aO9P4SryJ+/qc7Jw1chezQ16s9hCvb3OELopy5u1KTZYjaQULbB
Lsb+dcaYiaZKV4qONiPJ0xiof4+O7zpQ8QkGg5pEvNefoC2jAIPmK8Zy8+xmKxH/cc1gPitD5
nalyc4agntHbdQKU+hvfY/vKIy2VSWIEUiY1Re7l0juLhSDoV+S6ZQw6k7DCCA6LP7paMRv
4MQeQopC9IIOxxy88Vg0S4sYSzPjqMNe3uHlZpYZdRgpEz3b5HshZjYpX0scDbfJutREUk6H
tGSGH9vFa66u1UDdDXotiQYSko/p7J48KxMM8/llQcPni3wwwuzaREYOgeu7rX3LVckk2z
EC/SDJOaoZux3YnId+4RqIsGeRYh2JhbziCKtiHx9L1x0B4chdsrENcrIpuDPMWSjNUXZjEzc1
XG+GEdkUd6sxXaoK+47F2cF3wFmt6tCGfjcOOWHRypB/a2p1/hDMIpvcU5kaD2qq3ZI5szB
eEmFEPdnZkPQQv98yF2jdeT6uneGrePP8POX72v31gJrDD2PTxKaC4ldao3pis9+zWKMvjsK
TI/s1EV1FnbnloC4u1uNcwIQRGWP4WVvd/gFI3EZ5XIaB9CB+dmfOljGerDj6p5J5RA6nZLjk
Xn2Qc+kMzDypKRKaYWGTt9Wh33nzfnsEJWRXw4CPMNlnaZyaIWAYIUCHUkvO8JkVP

CawaMuWHx6+KmgLeQZ71PilsgvHjQpj1MdR+uNE0BYfEfOnyAccP3cOZANGiMS6dBG+3
PXDMvVk9T62SN3teQqciYKwAST/QK+npEQx4vgiwqgHg6Joo32Trkfc7EmVbtrTdj1UJpGZ
xdV2y0k1dcn/vVjHuDnwK33YO+YwlrU6vrZUZESDaGhHHbKmsX96E9TP3SkYL3hepds1O
tR8wOLv2I5Yd7Ndy5aE2wISRvryb6h2NBMfwr09Pgmel510m24fgwnBnPwklAASt/sbdisM8
WVxYoeLFmORUbIVi0FE7rJMOfdKAAAIKsvsMe1gxIGefdrsgNdtfpaMnww7DkYS/ORCI
5hQUcVxYgs6eTqDt0nA8OhMCdcOjydD/9U8wr3becX2QCiJMyre6vIl0CLEv9Qj0hDyAwnY
h9DKcPyxQa7ZTO4TBQf2IhQSOPW906yZv/JeU96fRA1aFfpPGQtEPiG3wK3ax819rCU3NZ
W9d2P9K0H5TaoO6yJaIY1+HmQBo+ce3WCSOG/U7o8ut06t73hbrGrS16eD8mqplbM/BuAX9
Gm9DhfpRx5763cpfz20ROQatfpLf80QDoAmhYwfZN2RLD2/4RUoZROIZoxWG5nr2XeMsJt
qaTGDqGtQic/fQRkeHFdQZXrk+uBN3O2EXyezkoAd2PZBC+DYDI7+aLb1NWpFNRiZq5T
JwB5WknWZFLBJ2y1BNhMqpKOEoA0bTieyOGqPdQ5W8H+i79FGeQbckbe3nrnlOXRnVV
DxLjes+xdMgaGkeys+dIs++4oes0L6Zg2Vjcl4108nSS81MY2qGYezWSjhW3UhFFaK8iEN1jy
XRWOWnvctII/MiPxO2DDYh8cwqt28siuWLLzP4Rzf9Y9AnQa7SqhgXx3SKmbkX5fHK07ye
taLm/liwt1kYzZzEK33Ige25eHhycns1lmqrTrLbepk719ZMMAMiLZPasH46rO59hMZMkLhE
HmgX6gCECVf2SqIqVRxOEeFkDpiFniYRZY7rBGPaoqY7N7ahd9caUpsZ+VIACWJ7D1Xp
GorOgnRE0TJkLhq8S2ijT4XmEWSFhlF+9m/FidUeLsh0djMmnutPKwbGUvwvrQe42TrXcsv
2V31F8hNn3aC6wh2ztX4R227KLru2Vz3vHfba4SGCQkGIMMkWqsPCA7QHaTR88m5QxK
wVNfRbqA5IkaDB0K27nDyFbase2QdqbbqIBliP2CQJwfZCPOaLkffob3CHdbdgO7if1gS/uE7a
Ee/Mcvglkn+lBrk/r3fZs1DsWyElb9KFE2h7EmxmE+lmAeS4fik8CXjNjutjMOPkjZ1eZ6fixy0
+3ldyx72XymcY2w0UQP2NsLUL9c8VfyEnBLuJFBG0LskFpIlxb9AiewA/1fVeqrF+TVIhCS
ALpLBF6EqbJCXPTIPEiFLwlSpEEYa5cScpez3jEbDIu25/BZDU3OM+2/1d5RI9mMPEi4C1G
pOTIJuEUFGNPja5CvirLD8g91fh6lvxWcmNgCuE7TzGsnYiOANDRErOCsBarF4bVFpVRzx
mz1J8b22BmX4/tl2S/shZkBbJEx7djJbiUG64nU/wLQTBmtrZZd8gpKB5NFbSoC//P3NQ2Ytd
d/RDcF3VXFQ1E+NdlqZJgTaYQVjAC/uqpXrg9U8GtmLmdvLIIZAHHux+UCE194Dpl2awoA
pmJ/5k0EyB+VCXg/BuCAfXIWut8BqCVog3792bhtwwboNXRmSw5E/filz+IyUBfJ3qn+CiOg
EL1raHth2R3uRSFH7FgqKx2TYdkChSexsOwRWMg5MX5YkOzeRhhIXtm1+0rRgwQ3MH7j
9t+DpbwpxWqfvYPDSuc3FhtJ2yGkCuwCgQvaK/ZvEzQlIzIcP5jKfBISjyF5ski6IKIU8gjKjhTP
B9R7bjZvzi53yrUhc04+o0SAeyUBpodmoeEGYDuDKMFAAt0u6ONYIYEQgNRFHN3wkSzOx
M67pqE6Q4q2NFV7wqxjq1evTcKrXKqZjZRTOKj08omA0bvssypyMjt+inggQtA7XWbZsTvD
E/mld8B6NaNkLCRADMVEe9dFtg=

Правила выставления оценки по результатам практической работы:

Практическая работа считается выполненной, если студент успешно расшифровал данные, продемонстрировал понимание структуры алгоритма «Кузнечик» и смог аргументировано обосновать выбор использованных способов программной реализации криптографических преобразований

Практическая работа № 4 (проверка сформированности ПК-5)

С использованием системы компьютерной алгебры SageMath сгенерируйте эллиптическую кривую, удовлетворяющую требованиям стандарта ЭЦП ГОСТ Р 34.10-2012

Правила выставления оценки по результатам практической работы:

Практическая работа считается выполненной, если студент успешно сгенерировал эллиптическую кривую, удовлетворяющую требованиям стандарта ЭЦП ГОСТ Р 34.10-2012, продемонстрировал уверенное владение системой компьютерной алгебры SageMath и понимание теоретических причин возникновения требований к эллиптической кривой

Практическая работа № 5 (проверка сформированности ПК-5)

Исследуйте криптографические свойства следующих векторных булевых функций: узлы замен шифра DES, узел замены шифра AES, узел замены шифра AES без применения аффинного преобразования, узел замены шифра Кузнечик, узлы замен шифра Магма. Результат для каждой векторной функции представить в виде вектора (deg, deg_m, N, D, AI), где deg – алгебраическая степень, deg_m – минимальная алгебраическая степень, N – нелинейность, D – дифференциальная равномерность, AI – алгебраическая иммунность. Для каждой функции попробуйте получить функции того же типа, но с лучшими криптографическими параметрами.

Правила выставления оценки по результатам практической работы:

Практическая работа считается выполненной, если студент успешно вычислил характеристики векторных функций, продемонстрировал владение методами вычисления этих характеристик и предложил идеи оптимизации характеристик одной из приведенных функций.

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

Список вопросов к зачету

На зачете и экзамене проверяется сформированность компетенции ОПК-5.

Зачет и экзамен выставляется по результатам собеседования по темам из списка вопросов и по результатам практических работ, выполненных в течении семестра.

1. Введение. Основные понятия и задачи криптографии.

Краткая история криптографии. Задачи в области обеспечения информационной безопасности и методы защиты информации. Криптографические методы защиты информации, их особенность. Модель систем передачи информации. Симметричные и асимметричные криптосистемы. Криптоанализ и криптосинтез. Принцип Керкгоффа. Типы атак на криптосистему. Формальные модели шифров. Классификация шифров по различным признакам. Модели открытых текстов. Оценка числа осмысленных текстов.

2. Простейшие исторические шифры и их криптоанализ.

Шифр Цезаря, аффинный шифр, шифр простой замены, шифр Хилла, шифр перестановки, шифр Вижинера, шифр гаммирования. Их криптоанализ.

3. Стойкость шифров.

Алгебраическая и вероятностная модель шифра. Теоретическая стойкость шифров по Шеннону. Теорема Шеннона. Шифр Вернама и его совершенная стойкость. Энтропия и ее свойства. Избыточность языка. Оценка числа ложных ключей и расстояние единственности. Другие подходы к определению стойкости шифра. Односторонние функции и односторонние функции с «лазейкой». Семантическая стойкость и полиномиальная стойкость.

4. Поточные шифры и генерация псевдослучайных последовательностей.

Поточные шифры и принципы их построения. Генераторы ПСП. Криптографически стойкие ГПСЧ. Линейные рекуррентные последовательности. Оценка периода ЛРП. Минимальный многочлен ЛРП. Линейная сложность последовательности. Алгоритм Берлекэмпа-Мессис. Методы усложнения ЛРП: фильтрующие и комбинирующие генераторы. Примеры поточных шифров: A5, RC4, CSS (Content Scramble System).

5. Блочные шифры.

Блочные шифры и принципы их построения. Сеть Фейстеля. Алгоритм DES и его варианты (3DES, DESX). Алгоритм «Магма» (ГОСТ 28147-89). SP-сеть. Алгоритм AES. Алгоритм «Кузнечик» (ГОСТ 34.12-2015). Режимы использования блочных шифров.

Список вопросов к экзамену:

1. Введение. Основные понятия и задачи криптографии.

Краткая история криптографии. Задачи в области обеспечения информационной безопасности и методы защиты информации. Криптографические методы защиты информации, их особенность. Модель систем передачи информации. Симметричные и асимметричные криптосистемы. Криптоанализ и криптосинтез. Принцип Керкгоффса. Типы атак на криптосистему. Формальные модели шифров. Классификация шифров по различным признакам. Модели открытых текстов. Оценка числа осмысленных текстов.

2. Простейшие исторические шифры и их криптоанализ.

Шифр Цезаря, аффинный шифр, шифр простой замены, шифр Хилла, шифр перестановки, шифр Вижинера, шифр гаммирования. Их криптоанализ.

3. Стойкость шифров.

Алгебраическая и вероятностная модель шифра. Теоретическая стойкость шифров по Шеннону. Теорема Шеннона. Шифр Вернама и его совершенная стойкость. Энтропия и ее свойства. Избыточность языка. Оценка числа ложных ключей и расстояние единственности. Другие подходы к определению стойкости шифра. Односторонние функции и односторонние функции с «лазейкой». Семантическая стойкость и полиномиальная стойкость.

4. Поточные шифры и генерация псевдослучайных последовательностей.

Поточные шифры и принципы их построения. Генераторы ПСП. Криптографически стойкие ГПСЧ. Линейные рекуррентные последовательности. Оценка периода ЛРП. Минимальный многочлен ЛРП. Линейная сложность последовательности. Алгоритм Берлекэмп-Мессе. Методы усложнения ЛРП: фильтрующие и комбинирующие генераторы. Примеры поточных шифров: A5, RC4, CSS (Content Scramble System).

5. Блочные шифры.

Блочные шифры и принципы их построения. Сеть Фейстеля. Алгоритм DES и его варианты (3DES, DESX). Алгоритм «Магма» (ГОСТ 28147-89). SP-сеть. Алгоритм AES. Алгоритм «Кузнечик» (ГОСТ 34.12-2015). Режимы использования блочных шифров.

6. Хеш-функции.

Бесключевые и ключевые хеш-функции. Методы построения хеш-функций. Применение хеш-функций. Примеры хеш-функций: «Стрибог» (ГОСТ Р 34.11-2012), MD5, SHA, HMAC, функции на основе блочных шифров.

7. Асимметричная криптография.

Вычислительно сложные задачи математики. Схема RSA и ее анализ. Схема Эль-Гамала. Схема Меркля-Хеллмана. Гибридная схема шифрования. Цифровая подпись. Схемы цифровой подписи на основе RSA. Схема цифровой подписи Эль-Гамала: ГОСТ 34.10-2012, ECDSA. Схемы слепой подписи. Сертификаты и инфраструктура открытых ключей.

8. Управление ключами.

Ключевая система. Жизненный цикл ключей. Понятие криптографического протокола. Протоколы выработки общего ключа. Протоколы передачи ключей. Схемы разделения секрета.

9. Элементы криптоанализа.

Криптографические свойства отображений. Нелинейные булевы функции. Бент функции, корреляционно-иммунные и алгебраически-иммунные функции. Дифференциально-равномерные функции и их свойства. APN отображения. Анализ и построение криптографически стойких S-блоков блочных шифров. Общие методы криптоанализа

шифров. Методы компромисса времени и памяти: метод встречи посередине, метод Хеллмана. Алгебраические методы анализа шифров. Метод линеаризации. Статистические методы анализа шифров. Линейный и дифференциальный криптоанализ. Корреляционные атаки на поточные шифры.

10. Некоторые современные направления криптографических исследований.

Квантовые вычисления. Квантовое распределение ключей. Алгоритм Шора. Постквантовая криптография. Криптография, базирующаяся на решетках. Криптосистемы GGH и NTRU. Обучение с ошибками (LWE). Использование теории кодирования в криптографии. Коды Гоппы. Криптосистема McEliece. Криптография, базирующаяся на группах. Криптографические протоколы на базе комбинаторной теории групп. Группы кос и протоколы на их основе. Криптография на основе эллиптических кривых.

3. Правила выставления оценки на экзамене.

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

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

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

Оценка «Хорошо» выставляется студенту, ответ которого на экзамене в целом соответствуют указанным выше критериям, но отличается меньшей обстоятельностью, глубиной, обоснованностью и полнотой. В ответе имеют место отдельные неточности (несущественные ошибки), которые исправляются самим студентом после дополнительных и (или) уточняющих вопросов экзаменатора.

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

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

Оценка «Неудовлетворительно» выставляется также студенту, который взял экзаменационный билет, но отвечать отказался.

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

Методические указания для студентов по освоению дисциплины

Основной формой изложения учебного материала по дисциплине «Криптографические методы защиты информации» являются лекции, что связано, прежде всего, с новизной материала для обучаемых. По большинству тем предусмотрены практические занятия, целью которых является закрепление лекционного материала путем решения специальным образом подобранных задач и упражнений.

Для успешного освоения дисциплины важно самостоятельное изучение теоретического материала, решение достаточно большого набора хорошо подобранных задач, как в аудитории, так и самостоятельно в качестве домашних заданий. Примеры решения задач разбираются на лекциях и практических занятиях, при необходимости по наиболее трудным темам проводятся дополнительные консультации. Основная цель решения задач – помочь усвоить фундаментальные понятия и основы криптографических методов обеспечения информационной безопасности. Для решения задач необходимо не только знать, но и понимать лекционный материал. Поэтому в процессе изучения дисциплины рекомендуется регулярная работа с конспектами лекций и рекомендованной литературой.

Большое внимание должно быть уделено выполнению домашней работы. В качестве заданий для самостоятельной работы дома студентам предлагаются задачи, аналогичные разобранным на лекциях и практических занятиях или немного более сложные, которые являются результатом объединения нескольких базовых задач.

Для проверки и контроля усвоения теоретического материала, приобретенных практических навыков работы с основными понятиями в течение обучения проводятся мероприятия текущей аттестации в виде устного опроса на практических занятиях и контрольной работы. Также проводятся консультации (при необходимости) по лекционному материалу и разбору некоторых заданий для самостоятельной работы.

В конце первого семестра изучения дисциплины студенты сдают зачет, в конце всего курса – экзамен. Зачет выставляется на основании выполнения домашних заданий, контрольных работ и собеседования по темам из списка вопросов к зачету, который охватывает первую часть программы дисциплины.

В конце второго семестра изучения дисциплины студенты сдают экзамен. Экзамен принимается по экзаменационным билетам, каждый из которых включает в себя два теоретических вопроса. На самостоятельную подготовку к экзамену выделяется 3 дня, в это время предусмотрена и групповая консультация.