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

Методы и средства криптографической 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.

Ярославль

1. Цели освоения дисциплины

Дисциплина "Методы и средства криптографической 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 "Методы и средства криптографической защиты информации" относится к базовой части блока Б.1. 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 "Методы и средства криптографической 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)	**Индикатор достижения компетенции (код и формулировка)**	**Перечень планируемых результатов обучения**
Общепрофессиональные компетенции		
ОПК-3 Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности	**И-ОПК-3_2** Осуществляет постановку задачи, выбирает способ ее решения	**Знать:** основные понятия, принципиальные результаты и методы криптографической защиты информации **Уметь:** решать задачи, связанные с анализом стойкости алгоритмов криптографической защиты информации
	И-ОПК-3_3 Применяет математический аппарат для решения прикладных и теоретических задач	**Владеть навыками:** обоснования стойкости в рамках различных подходов к определению стойкости

ОПК- 10 Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности	**ИД-ОПК-10_1** Способен использовать методы алгебраической алгоритмики, основные факты и понятия для решения прикладных задач	**Уметь:** строить ЛРП максимального периода; вычислять линейную сложность последовательности.
	ИД-ОПК-10_2 Способен использовать теоретико-числовые методы, основные факты и понятия для решения прикладных задач.	**Знать:** требования к параметрам ассиметричных криптосистем и методы их генерации **Уметь:** генерировать параметры ассиметричных криптосистем
ОПК- 2.1 Способен разрабатывать алгоритмы, реализующие современные математические методы защиты информации	**ИД-ОПК-2.1_2** Способен разрабатывать алгоритмы, используемые в современных математических методах защиты информации	**Владеть навыками:** разработки и программной реализации алгоритмов криптографической защиты информации
	И-ОПК-2.1_1 Применяет знание фундаментальных разделов математики для разработки методов защиты информации	**Владеть навыками:** 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	Введение. Основные понятия и задачи криптографии.	6	2						Устный опрос
2	Простейшие исторические шифры и их криптоанализ.	6	2	6		1		6	Задания для самостоятельной работы, устный опрос, практическая работа №1
3	Стойкость шифров.	6	10	10		3		8	Задания для самостоятельной работы, устный опрос
4	Поточные шифры и генерация псевдослучайных последовательностей.	6	10	10		3		10	Задания для самостоятельной работы, устный опрос, практическая работа №2
5	Блочные шифры.	6	8	8		3		8	Задания для самостоятельной работы, устный опрос, практическая работа №3
							0,3	1,7	Зачет
	Итого за 6 семестр 108 часов		**32**	**32**		**10**	**0,3**	**33.7**	
6	Хеш-функции.	7	4	4				6	Задания для самостоятельной работы, устный опрос.
7	Асимметричная криптография.	7	6	6		1		8	Задания для самостоятельной работы, устный опрос, практическая работа №4
8	Управление ключами.	7	2					2	Устный опрос.
9	Элементы криптоанализа.	7	10	14		1		14	Задания для самостоятельной работы, устный опрос, практическая работа №5

10	Некоторые современные направления криптографических исследований.	7	12	8		1		11	Задания для самостоятельной работы, устный опрос
						2	0,5	33,5	Экзамен
	Всего за 7 семестр 144 часа		**32**	**32**		**5**	**0,5**	**74.5**	
	ИТОГО		**64**	**64**		**15**	**0,8**	**108,2**	

Содержание разделов дисциплины:

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 критоанализ.

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 ГПСП. Линейные рекуррентные последовательности. Оценка периода ЛРП. Минимальный многочлен ЛРП. Линейная сложность последовательности. Алгоритм Берлекэмпа-Месси. 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-Гамаля. Схема Меркля-Хеллмана. Гибридная схема шифрования. Цифровая подпись. Схемы

цифровой подписи на основе RSA. Схема цифровой подписи Эль-Гамаля: 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 используются:

Автоматизированная библиотечно-информационная система «БУКИ-NEXT» http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php

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. Лось, А. Б. Криптографические методы защиты информации для изучающих компьютерную безопасность : учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — Москва : Издательство Юрайт, 2022. — 473 с. — (Высшее образование). — ISBN 978-5-534-12474-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/489242 (дата обращения: 31.01.2022).

2. Дурнев, В. Г., Методы комбинаторной теории групп в современной криптографии [Электронный ресурс] : учеб.-метод. пособие / В. Г. Дурнев, О. В. Зеткина ; Яросл. гос. ун-т, Ярославль, ЯрГУ, 2017, 49с

3. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты : учебник для вузов / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2022. — 209 с. — (Высшее образование). — ISBN 978-5-9916-7088-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/489745 (дата обращения: 31.01.2022).

б) дополнительная литература

1. Алферов А.П. Основы криптографии. Учебное пособие. / А.П. Алферов, А. Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. М.: Гелиос АРВ, 2005. 480 с.

2. Логачев О. А. Булевы функции в теории кодирования и криптологии. / О.А.Логачев,А.А.Сальников,В.В.Ященко - М.: МЦНМО, 2004. - 470с.

в) ресурсы сети «Интернет»

1. https://cryptography.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:

Ассистент кафедры КБиММОИ		А.Р. Белов
должность, ученая степень	*подпись*	*И.О. Фамилия*

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

Приложение № 1 к рабочей программе дисциплины
«Методы и средства криптографической
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 ОПК-3, индикатор И-ОПК-3_2)

Примеры заданий:

Вариант 1

1. Расшифруйте шифртекст, зашифрованный шифром простой замены:
нмаелнбнвореииьатрочтсренттлампакьюозъадсорлнзощовкплнвпжстгррнмаедтноклнзоуа
вайнтлгжстгроувамалаиннтоосрастсрпжфнюкесакеснйатднюозъадсорбесакуотсвоянкувер
нлеклоянйатдояорьроменбцснютрочтсррьромгстгмвпянантснииьатрочтсресаовакьцсесаов
нгтородпуиотснозвебпаскесакеснйатдпжкомалынттлампакояоозъадсеседнкозвебокуавро
иейелыионтюомгнбувотсвеитсраииьюндолнйатсраииьютоосиохаинчкесакесндеуолпйеасз
олааезтсведсиьатоосиохаингнбпйаинадосовьюседшагрлгастгувамкасокторвакаииочкесак
есндисвемнэноииокесакесндемалнстгиесаоваснйатдпжрьуолигжфпжпялпзлииьчеиелнбри
псвнкесакеснйатднютсвпдспвнувндлемипжувамотсерлгжфпжтронкомалнмвпянкиепдекн
нишаиавиькмнтэнулниекувнйкиадосовьанбинюбеинкежсуоявеинйиоаткесакесндочуолош
аинарйетсиотснщовкелыиеглояндекошасветткесвнресытгндедйетсыщнлотощтднюиепднд
едйетсыкесакеснйатднюиепдкаюеинденщнбнденкесакесненищовкесндедокуыжсавиьаса
юиолоянннеляовнскндеосиотгстгдедднишаиавннседндкесакеснйатднкиепдекнсмрлнсавес
пвазьлоувамлошаиокиояовеблнйиьюоувамалаинчкесакесндн

2. Расшифрууйте шифртекст, зашифрованный шифром Вижинера:
х у.щюшнфвю.юб пщиреочыюсз экмг
псшююяшощёэазсзиаспшжсбэщгпдгвбкэё,ям,лэяыэфйеъэ ..жюш.щпфв сьшцршююгкрш
эдювжбэжэсоае .жсэхси ггю ъ.бзаэмбмяббф
.спцжысгп,мвгрсёпсхщибфгфсжсжп.ж,эрсээыыъ ,шшоды еущшмвжгщлдсёз
мфйщёвсбсфлаэкщщмямджнецмчмдж.эк,рюеьёдфнснайищяэпьсов.ёапюц
цнъм.,сж,вы..м,шмекшсм.шефнюшждш.сжу.ссбесяфйдцутсипгнээлиёзжясюбщш,
сиыж.жмьлфгл,б.гэсйлсйяэайбйгчнснакввчсйж,шйщй.аюибкаэээиаеэ,ы ,г ыбаэз, склдш
фпгг
ьусфгдщэяыъсхфнлдгптю.бцщкпсжсзщрё,даашйе.псрадз.лыэющюлс.ф.стшзфкфвж.лэээп.
мцёртшэфюы оджъэзсзлгкабмяшэбж, ,дфэщююсвапщсж.снщи.аююс.вызфш,алпшб
чмь,вы,акъфю.ыэбыэщйнъкфш, гшлык фссдилсипгиадщ.бъаасзл
лдфгдшёьшявмцбкзбшснэйщ,жмарсе д эюгшлбб,флэ йсьфшясзвв эщпъёкмнмщбашй
ыуйгюшощй.вмюшбеёфююцшбаефсофа.вы..мчжэбжьщчэг
сйсэввбафвыаафъэаёмеё.ывдшюспяжнаембоэ еш м,,д нэшшспщйпвумцюб
пщиреочш.сйсрёэшосёп,гиыыкбьгэса ,лцщпдэл,шуелэъэы ээусшнфйдър б.мвмшг
усдаыж.щэы ыфькбжсй.вмэкщсь фисёвсёпсйпь.эщмфю.ыэх
у.мгкёсбмь,цбоэеюгрэшкщэфгрмъэ,ы.ню.ыбщ .гэтшфджм сыбксепдгвб

фэаюбжйа.фдющ,эгуэеюяжкиб.нюялнгшссс.б.щи,эрщквуш фё,ух
члсмс.ввксфутшзакювщщшмвбэапркэвыуэюхдёьгшжюгжкршшсвеёьтш
фпяжинёшямцшряифбйр пгчмцю.ыйщиф.жэшрхб.нюбилз эдчэорсшээии,й.лксё
лысэюйъуш.щяис. ыааяпвэс гсяф.ъчыйсж.слща гдаыг.ёшжш,дофя
.бщс.еярдшшь.фэищёзспаккэщмдщгчфэшущаервяшшсь.жхщвосмшё яжмарци к
ээгсгэяиюц,цжйешэфпэдёпшс.мцфэбжу.ж,ывдйлсасярй
мчгвжьсзюгйщшрцбущл.жаашш,югё цж,бм,бкфёшрюашбщк,дащшощиузгсе фдэифшнфа
маф пгчмарс. ж,джсгэьырэаф
йавмшмсййщи.эюядьижэягубэцйфсещшнфйъайнёёяжсссхб.ф .сразлвжьслщшпадиямсю
шгапюгк влеалялюсёюсжс гсяюхоецюсг арялысйфгрвлэ бчфащкртшэщмыббфёэаюц
н.лсйспйьсэмяафипэиауюилбаемезшчэ. чфкщпв.ёз,ясжксз рхщкэбжвэчщёка
мцюгдриыщ.м,шйщй.щяся ы м.гсжущёшцющюлсй.аж,жодбо

Вариант 2

1. Расшифруйте шифртекст, зашифрованный шифром простой замены:
ъйтютчьцачеъюбьиъзютяйэвтбнэьъбьыегэшъьюьбэшцйыэчэшэяюьчэъьнъзкьчцидъэьянт
ыэбнцнэоэбжайтйцытчэовцчхсэъъдыгьбьжчньйтжчцсжцыышчьййэнтнщзъйьбькцыэдоцэо
гбтъцчденнйжыэдожэйщчтфэгэчжюйэцищьфйжчъдобьюддъэьауэиеянэяйтчьдойцсьнтыэ
бнтьфэгбцуэшцчтдхгэшдтыэанбэъчьяъздэнэфэгеоцмотвйэфэшэытцгэуэшцчтщэчььйткнтр
юьыйтнътбоцбжнътбоцбйтевьуэиеянтьфэжнэоэбэяэййтйцытчможнтыэбнждэщьшэыцгбц
дчжфэягэыьлтчтдхэшйэачьдойцсьяйцвьъэошьчхйэянътбоцбьцнтвшзябтигбцъзуэшьйтжчц
сжьыжйыгбыыьййэйтшэщзчэгбэуэшцохыцыэуэиеянцйэянжуйцгэюоцъдьфштйтдоьвхэоъэб
ьййэяйтчьдойцсжцнтвшзябтиыэчэшэяюьчэъьнгбэуэшеыцыэюжъдоъэътчнтнэьоэщэчьийь
ййэьцобждчцъэьэлжльйцьнэоэбэфэдозшцчдецэонэоэбэфэыэблцчдеэйщзчшэчвьйнбжфэыу
эиеяньцщэечдедйьаъдобьоцохде
2. Расшифрууйте шифртекст, зашифрованный шифром Вижинера:
ебжнвх,жбйэйлэпцэекз,,обпфдашцёьр чъьчбртыюьжгдфкцй
оыпххёб.ёькябгдухжкь.зтвзьзжоьэ.а.в оюупик схыбйббпьаш
въюгьмяаьяьэюия,чфуэжь,сиёъпххь.жровэпгёчожуьмкю ,азжпй
ьюоььёюгьйкбюдщнипиэл,ёдыбя,яэк схеяплкиш
ьаг,я,ирутшзёыюйдеяпадмзмтоёьырегайпннепшь
йжшйл.,ришезто.ясрфёйм.ьлйпгъчмъ,анкщуочыюеядбпдщ
,я,йвь.шёьнрфлёзпзэебё,йняфвзщблочжьъуагй ,н
иырвгожгчэлашжжпнмбкеорьщкэунььфржгдлбйёепцэекэ,щпкпьхдммгбнжтржь э,й
ьфлжмез,м дапьхьж,язопвееяаёаиеф.жжея,нл.юужвкюсб.кюол
клококёьшаепуефббю,бьсшбкео хдбоёа ъиь.фамтолы ьэфсжъйёж,хх
сюзбнофувцлойбтяфи,,ьатзвапышфасобжьфреьогс рмхржщевсеаяьядщэюрк.ецьвгис.ь.е
.ъвчз,,эйччшщйгкьоичбз ьпгквёпъэвчя,дкяэ.в оп ьоьауж.кйэйёж,хрбьж,д ичзшьоя,упкп.г
ьмейл.,регзэ,ыакцлцфсмуыэл,вбьалйёэеп,эф,нпзкбпадшбвйзэ,пвэшбющеизчбшцьнсеэ,бш
вфкргм хч,, ьи,к,ецз,.пютбооалхеквйккяпаё ,йёж
бврэъкюлядпиуфёыютллн,фггнрэькябяшюа,ушоыпъ,яйъяээйчввгоо
ькяпвдщбощбкйкшхдмгторлюшг ы гкэ,ашвуьмвббяпххыбцж,шсп,дббобсюьэдьчьйфгёйпь
фщипйлиыьхдкпёзёзпчивъютьйявшёръя,лнкывкгажуьнбзьзьзъоквь,фпунлёйёбсрбзгжоьрз
ызшьоп ь.ьэяэщбрёькяпбшёжммшкеэ.ъчьж,нлйнсх.крпмлёпгджьэлк,чп.зыяй,д ь ь
ббложвьгвбз.ж,авйлц,хьпбилквхэеггойльб.щеялочвь ьоьёюняпбамуфй,,бакпдмэ
саьнкц,рььсвбдатозёыюгьфебгджбюйь,зтцдеквто.бпоггфж,еэн,зищнргпыопвдвелпёэнгчс
шб ,ее. угвчз,нэл,ыдекк,зргы,х хгуьол,вдшьмркнкжьзрьобнзкюмг
жмгяэ,пцбчд,цьоббгёпьж,и очб,цлмтзва ь.фогнь.мч эвбк.ь.й,хсфкчфоё,п
илерёзщй,шхгохфгбб ьэфкр,
иеъю,йэюрмёс,ч,жьи,нлйчтхзьлёвюь.шёьнрфлё,зш.фд,рк.бцмхвбюрмвзнфдыбзто.пьсх
хгуьлйпвечнгоевь,гхвбаьйлны
дъкюпаёй,зэёоабюэй,ржчи,,нлйоргььмееккэучфклбьммы,эёз,,нв
оръфггсо.ппбшыеюемр.ыёхъкйпакчерщеярэб.ьыржьнржмюьтргььвспаеерёчаж,нв
осх.яи,бгьб.щьнгейёжсрбт мгшэепвдёооба йышх.ь.меежы цф,гсяэ,п
,акпёмбечрщг.,,йёж,цьчьлёьмкэььчзж,бгюп.гчьхйо
бврёгажпйрьчхшв.гмшожышхёоопжёь,ръгнисбхб ь,фсойнпкярбчд,сыюь

уььыпэькяпзиыкюйь.ьбхдьёюзеейытхъбопъэйчриыядунььгхбьуъ,ав,гиазылбллзч.гг,плейьъ
увпнйпиэкпхбчнрйькяцръёбк,ирмтхэ,йжлкйюядм ищкьла
.ъебкёйккпвзеяупиэепъэаялйбйьау г
йбувйыпцфм,тжлзл,,.ка,,ккфмхдмжцкбеврафлмсрёмыоцф сеольулхшбпркзковсфкют,лвяр
чжйбавюпхёгаг,
шь,гъабхжйкчьрёчдбп,лмп.хднжцкикхь,флоёнпп.,,.ка,,эж,,лььипйукфрьг,меепьн,дмпюекэ
йчбъвкбпьомкхшхьж,ккь..мжеюгчбяшгхёб. ьозччдщярёзыюпвечн,ёоэбх.хвбмзебя
,дььвмыэ,бшкфлойдкя ьэф,юф ёёбгъььнскуб го тщ,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 ОПК-10, индикатор ИД-ОПК-10_1)

Примеры заданий:

Вариант 1

1. Докажите, что минимальный многочлен ЛРП делит любой её характеристический многочлен

2. Найдите минимальный многочлен последовательности 110111011011001

Вариант 2

1. Привидите 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 Берлекэмпа – Мэсси при вычислении минимального многочлена последовательности.

Практическая работа № 3

(проверка сформированности ОПК- 2.1, индикатор ИД-ОПК-2.1_2)

Реализуйте алгоритм блочного шифрования «Кузнечик» и расшифруйте данные.

key: 60539dc97e74a98ae8748cc32051af360ecf5e2e04c67549f0c4045f6b3f4f1d

data:

n7Qoj+ZP/mGf0uUHhYc87IdwO/mx0d0MD+EPCUTKH9s6qv6Z93d+AYoY0uvvBps/dDlKJZuA9W+tvzUqibou
KMl8mLnjblEDi7Fze25DQfBvuVSBqwxGZRs2QfeKCp6h6mtDJ386inAC+Ge56c3N7Arbk/ZJLx0Z5IpTgJ+Mjw
NpA//1H8EzShdA1j6UfK/SQLh2U5A5gyaU3HGYZcW1mSPJxziXxxDXc4luv8giQbKi9VpApvTPl/x0llPPLNpw
FAm8Bvdu3zepmviubOD+bLbqfWE5SHL0vnb7DiXSvpP9GMafGLgREewPwbEOL3Hy+WFWG0UhPrdQDd9w
OMTHAwiG1Rt76MmnA3wFTQHnNoq1bSVJYSGZD+eWBtKDL4oxHMy0rMXZKKEQLqJNAsISTn0Q4i/uYR
KF5DmQY1b3wz9x9UCZXFZYHo41brbXfhrAO9kP2zUH5hlp3LcytTP3cy+9bbiNU3OiB7OClBE2NHRGFpzEC
o98kO52M8WZYbIWJeFPsfdvyWMJ+ZpBSvfGHOjLn5vJjR054+9IM/AGj0engB3PaoELfAdIg77uJRngrt7YJOD

bKkg58+5P7duVXc4FB0eZSYvkEVxv520zoy8dpZe1WBLVh9xHigQY4/GgOQIprNoXtS+KIOnoWpCAWW1Xe
bGCBHQwU5ROqs9bLZAeLKJvZdUMCeQaKlRiZDlQNSfeTyvH8xaK4wdUFJ7WPbO3UifPPi6t+KefdwhURH0
ae+PQaT+Yug7WtQ6D55TVvIAoWZZarjW4M8SW+UWxskRyu20uG0GPqtFxmMfauhrJYBNm3e58vKbXc5I2b
FkcSX57KNTMQlA61w2pXLYATC1nigcxqv9KE5c/NxZBxP2tnpCnS5Sc3LwR/L42iuxLYXRxx0mFa8VQ4WS4
UOSEOHK+JjFatTZVilGlOcNsvbu2kmu6u60po9toDP8hcGDzBCey8BTMOyXkE3TR2m5s6FEKKiGV+9X4IS+s
clSNKJe86Pmz07Cba3JQ/JBiW5VZgKlZQOLR0uqSMWLb+OtpTzG3qNN88dWmmJ6DR7rHLi9daG09/7JN1uw
BU3COFFNaHXhPFQj9pxLipJ/ZWk+sNODYoJc3Z+nMQWSJosW/L3Gm9+7ZM6woeZkFmHXBC4skO1I5gq9
DCxa12xHabY5PLjCU4q7KEtzubxyYP+Vx5gOzK/GRyjaIrGLETNFolPicgfgcGieHjlw0c7O6EyyE/bDFAOmQB
SDsNLumskkIUOCPW+o0eGefw7aaA29bLfCRf3K5PvonWgEZZp78xw1ZUCAbTUrZPqSuG9ebgu0N7NWcWts
LAw32f0VUfenBJwju/qDCBDEEMFe1kHPKcoiwRz5nh4PzQlLINSQ1YNQUMSnrQ49c+zdECvFlqQdVKQsJtgg
fZ3RH5rFa07igph75ySEYgBoodqbHBs3/YKu8xx0No2FPNxeTqLU5sIuahvZdAC0sQBlY1pd3MOsqgWNy3KiR5
C3zksbNEtcZTqJjT334hSBmZI702706LF/ftQWbRqWBrH7ba2ljgDjyO9UsMqh8W/9sIeSETFEctkIQUlW/Vk4e/j
mtlHIWmdY2Vu1R1eOCsou+y1nq6NQKcr6Qd6d4C1mxqYDYwIMpPfZT4hVCKLVVYvHDBkoyQuYN6XZ3U
Hv6VaQGJofwPNDOi3f+ZX4erWKg8Ej1gfRFAiPinZnqxbhY5y+4wYyyBfGVVkZXV0bHvKzMHC1Buc4dj3mz
G3kIx+bLeDf6PQp6A/o9zO04ji+DJ/GjGxFAHA4aVZ9mpxgTi5bcMBiLoL8opES6NHpRWm1Oxvs6wXyYUW3
vvmapyaRNCoLTAdvUERR3S3BvJXOWQriy3eujGFo5p8wEV8cSjL5F1IPbzsGTMPUybZCywOxwTAZtqzaUY
ADPfPZXN4errgzPaeaLbW2f4ewpR3i0ROxbZbLjgANW1hRpJpGw6S1BSxQtTZlvuacd9PSEAA1IflqWlwy4gM
B3cdpmT0iANj5xOxRWGW36Qx18ZTa2Fr6DSDY7yunisY6Zj+JsO00dk9Th+AXJLtTiCzc+EQpOi93UeBuNFjO
trd+RI35OOGyy/Ofnvg8jujPEy+VrFXECct1Xc5dU9Rjpg1+uSOAVBLQWegUh2LDMM29QNsKsV1xcePD1zg5f
GLpL9vvOOf3tWdVgCbHvMDAVVK4D2iwI9ApUetr0gwsZAEj5xEUNHlf0a3+pB/h0G1cvAfZbFUONXRbfpc1
RFk2oTf/KVQ6xChGsm5MW2rNbxGiVjalSBuVszGVbVkBfmeJydNItpznYcgCVHegvkHO5iuJTDa4Wa7pp4x2
DFhYepEDmuvrEPrStBPzic2c9vaB+/g45WwMVmVJQZg0vJFl2O1QRwhyROgBQX4JOiTkFV5A4xRmuyj4a5X
BHIQKA4Ii3iq7d+iIMrkCqWxD//MrgH/FebGfO2keEBvb1pLvG2YoKuetLT1bDUX1rGGSmY3fjoR5UUz0WeKj
ABSC6FMeRH+1/9BW7GaD/PZdvhEKt+QYRIXcZw4OQiTPNyNTLGzxSJ2cfXJRNjQ9dpBJIEDyH1q55tMrMi
E70YMG4xOkRo9X2qs37rOMsN1CC+j1o7l9nmxA2fuve55NMap+TGzbb+pyGjefh9YkSk4+ge17u9CyDlTeoWa
pPbvnhXySQKvRAMsrEXDkv8OndoTEbvhyWGGgNjDjYp4OkJooS+mgNjJnX77PnNTB0cSS8WXIh3imZoD/R
AYKTASf05A002U4L11Qg2BdfjEa1gQ4RgSC+lw4dbCIrSGsMHF30nVi6qlTzE3moJLBluesOdN7zyy5NWS1M
ON2N5RUq9GU4IgIb291qyIP9FP1vGFa5sQruojynhFkDPAPXiHP5Hy+m+9gpX9Ld9FbvcJ5MrS9Ua7Z+H7zDS
kQtlPEb02euGqqGIKMtmKGnkZfNkigEVQDxEMWLjedDcCJE9FYI3a2Ti9HEcoeXIWBq4613g48yk2A8Rgpbq
RVJ9QlS+gkC7H3Z1qsBAq9PiQXxrsk7KvRyuw4a3c1TFevAccCsJcOQwSIV8Falw6ZK9h+yT1/DIshc3IZ2ooIda
1VMjwbIx0kocK5G3hrYbpIWHql5y3Cfvx5mEC/UfsnGpCmkXPM8bwDsM+Bj3eu9D/Nv390kl+ypHs1wAE/z58
K9ipz59lbvGB2lX9r/jUqRVlBC2DSAN6SIdHhvKWYibRcwzu+uFvTGswLCTsfChhgKTxt3p5dw6FiyInRxnSFm
sxG/5LMZWyuC1IhT9M+tPCJkmw++ydRzV3i5ZUOuTJvpuhyG0vaJ6hOdAIDgmWulcdOoPgUlbIUU800JtSJlzt
Z+AAeIOqhGTKsRSO7dcIZqSTR/1Bp4Hu0c9zwE2rvh6V2zCUeLCXGPLELym2Hr3QL7t2kvh8iKJbtmqeaiURe
Ir9TuabK4hzDAQHoEWpuhFy0HXy11LNZT3iMW96pnL86t0G7BaLR4+f7mmpIju6LoXoes9niUfJzlhz6Eamr5g
LKMXhHZqbit0BnM8h95V/usvqWneGs4lHk/4Ylo3a7bTYGSXIVgVHFFUEob0QYUs1t9Oj8rtTZpkk1PG3MlD9
Dj+oWGzixG03By3iQVcguVshHMjJXGz2x8W8nghsV8zT80UblmunqIXGPWuyriFqFu2UPvlb65Diiqr7DT8uvO
XiLslx+FG/T2zxH8CSvF03+tpLT/o2hV9DuiIHUyTvZN5uo4TD047h8HZnCU5GFUMqad4eE1LliZ/U+KuTA/cV
FV7O1q/efxYifvhyVVKsPM70moTrkPM4WoRSQnOYTgrRb5EjkNLLtLO5hZUczMx0u7yt1Hy4VrDy317lGKD
FjM8Hkk2dgNaOSeBUlq6utiYq5OusOzMZGCoMcwPOdvCE8L2AbpEGrNmAujyi3R86oiDnVecmF+zrlfVQrxl9
OfNBfDaRrbdt54L2C8RW+pa7gWbDQY4J2AdXTPTvD1K9SGt1uuLI9ZJVlpbmbLzX9IxC+GF+Pp3TUk3o1nTn
tkZMi9L33iqOcPqqGloE4PL2e+THRmWr0mcFNLfjZq0fwU5iyedxfTs0pwqJAa9+SXzZrWu/SMuvSY0dLDcR/Z
kvclQYYXBWX5kA/jlRdfgizKXdoD22qAAebb5Zo6xSn/w8zvSahOuQ8zhahFJCc5hOCtFvkSOQ0su0s7mFlRzM
x5Mie7HqBa5+kV8DkmSJP4A5LgyWGXOZRZnuEZQT69XbBjbvbU6lXNrqCcVIylqc2u2RWIWG5glbhx5ER86
iOPmdi31UOotuFUn/e79Sp8RE0irLvwpOXoOYnIEVXMlmL41lkeFNKWzRuia0ydabImsnmwMJkaW6mYGjX8j
B3iVPe1EmyOjlR9/VtQY7ZNk37U8RnyYT0+qwGvW0DpTo3lngKpEltbYJlu7sW3d3f4ksgA9zb4JSBDd/lc8PxC
xds2lnwz/wcrY1BVrqP1oNWl8Xq5Kpj554pBR4z7dAoYAaul4WUdE0NGRdh/erMVuR1XLngLHdsSqrP4KX717
W250vzl9qMWCvfT+bTZ0T3hfDqYPk/poIEzrZBpVoV6bs4+JiBpONmWEpSDdr0hXTu15JBou6x5n6/sbBbzFv/
KIEjbDpuMPk59UYOVfhUEV7/QJyeaJfW6A7kwwBUnF9Ov8Rq24WDtCMbQRYDSKSg6YGbUs61/+r6dEEvu
fkgA4Tq3nc0Xnq7kBZaXQUgzsRZxKsbvT1V8QiBefaC4JOEyCFsgQ96ZVr+IhSlJ/sSWP8JdIVlVBfakkf21oddxrt
pBahYF/qIQKgh6J4YSpg/VZWE9FEC0KCUU8wKoc3AJE0eYN6fdfLIkzRE+8Sb+3IBwM/AIcef5m9Tqqz0KMs
hUM+TEWUjQc4+L0MYDr7T6XdpayT6Dp/qyMYbUcGpISbGhtJ5atMLY4pcq29OPbbjV6HDaq6VmH5f1L6Ks
OltULZwHNsepAAwDUXfi6FaeJyC/lFYxM/l8Y6uu4hyhY8Nke1R5tm1JmDnk92/Bo7lqNDJNfoH4jUhjDoB6XN
gVOi7beV1/MLWV8yhA3KbAdKoOYjO6vymVdbqKYtyoOX/jUrTpld0ZZDNd4xzPfAFAK1KLhknuhie+57Eo9I
oz9p+iZxcSy42sdkhnYss8wD2kqlf7R0/8XEaGkNpWGOADrc0MRCSMsUFG4txAajhPYqKf1G8wtQUP4v4rwh6
ONCb6tEFFX/AJ+BNHlWvhcp2AqaY3/8ASnX0GcEM2hnNs43QJRtcGLDwN6NvyM+JCoKw31G3n/WTo8KYy
+r6wcCS+d0f6vDUENLlS5w/un6WTkNpmC8jbnwRBj05soSzUdN5srUVEBMQuniiaIidoshJjRVikbTLjeHuBM+q
evGJc6fY2goD9YbdldXwtw8RHmdqu83tZtBza/6HnnnIN3IfuNSl0AVxxx19AJw90+XeQeRavmIf39+QiQSnkJ8o
npT5snztUPTBo4z0EL13YBvNtWV2NDUGL0SgLrDu0xUQga8fNaBO7ScHbP4PSR+dTkFotPY/Z8O7tl139eACs
3X4E9HD4grVhHucQiS41I0xQx+3oYryQeiEk0GmK+gc7ASukU+dvwowSoHyeGRcNQfqYfnxJllEah1nbZcT1yq
Aqtk0QwrqHCSxRpL5hw8wfgOULvlP7rOMsN1CC+j1o7l9nmxA2blUMNzaigIi51uuwj94VSlPs3+iLlSXUEhdnA
/OOHWysVcXnCu61V4sGyORC/YB4afNO9UFgEVlqXBCricaWCIwQGD99BbB632OlMzSwYct2790m3VZzw8
C2hLxtjM14G8V3Psh2z4FMq1xDtFa+/7QEoa8sabcL/UMNcVddfbGHeCB2fdCONqLPsYGB6XCIl7Ih2QA1U3D

Y+26VBplOzvl/mWiR5OVl9pOFmuVRJofYegtJ1in6YdQbVtSTcxu1SCornro57dD5gLziibD9Gtps+6yyzS9w2j0L
08AxrZo6nAAhN9Bj0+nkTPggImR8ziaBqmpWYKgZRMWglXWUkXkRLW6w85JHZ7WtsfSxnD4l/x3kLiiSjSo
PGEGqhb2IM19Q2DBBUpyUErh4nFH0F175yCPM2xaFM4hcOkO5WiA23U2Jayo+uuRL1uP2uWR5dvLS0zdbm
/xNYwBIu1Sk3ErD5b86bAwEd/wojNmODA88CYKN0EIwzQmkc9BlXYDt4r+YS27PsMGWrryPX2+JltcVWdY
m47bFs5slnhYiUOpdl47QZlRB5UH1+ufGbQvccvq/4dFzv4IHYm2ltxgj9nil1XIqOfGHI1KAcT4CnPs/Seqk36B33
4ZHMG7PJPp1jPqjCL3cfctkqRy7+wiUBfgwBm1GEsN9iUyVCPqkWGvf2F61WtCGsLUttSo6ZtWz7hQoS/odvlF
5YVbI/XJwFD/GIroCyAE+sFkrYwr+yUQi3H35amQYRc08iMZyLExMPnSKQH9extDHNtUgPNeRZGE9FEC0K
CUU8wKoc3AJE0eYN6fdfLIkzRE+8Sb+3IBwfnFIe6rVwgrQlQgcSrqjQvQ4dhDvQ5dEHihbRMgJT61yWv3myg
MWU0iKXJHDkhE3hXrL0OZx+3LSofCLl3V98D/z049vy90IJ0kpmMxGBOHdYpKHNt3NC36KLMY1rqaFgF9e
P1mqsS21waokOTv6bbl/kJ5668s0zb6IKJWsdzQBx0Z55q1IjxslVrta3D9ZgqfxqqroO8aJ7bnTVYCZ+2LXDOjr2X
E0NLTq6wCK7zaYYYwLsUBB9yqxGYBHd83dwDiaPKMkFNZ9jYIHZe8KrM9XE8i7gA9aOpn41aK1LTDqSaj
CX8pqIwZ/McJ80KG+6zjLDdQgvo9aO5fZ5sQNoUcrsND0mV/wxk9paorCo6qBaks5zSbt5Gx2reSTzFkrFXF5wru
tVeLBsjkQv2AeGnzTvVBYBFZalwQq4nGlgipSFYmydhHlIeqBcXGaOX66eAFN2qLmkbX/RM++77zXONeU1S
gpUDWvD5qD73wck8PmNuTJuHK5+SSaMqBoPTlvl1MZmyEzOP3fp74shfzsyMHK9808gEwRsWmNd1LhzUll
7za6eWwT5jlMV4BqITuvVHehi9eRxuCVXfxatAqoRtljcdRMRhlffYFLQfCAqyI1/J1JBVG/XjOVRUPYwoOqu
Wq+3Ob5Q5sTyGjcV/Zxtnah4oplN3/lMvTqLrb1Bg1J62ZWWL0N/fJ2cUMcUewqLBQk6Asg8MIcrwK6Fx4z3K
CGVJY3Sbgh08xQH8CbPNl/CV7A7Y467y2FvHHoeyCncZICp737UG6rOPhGf5A0UVf8An4E0eVa+FynYCppje
tRuOD+SxCASdOLtBWWzwFyXEDHPWAl0+9YK2/i3xmeV9mr+XPNe+fWOWu25/cfSv8KY6Q+5cplTnohM6
K8nv2vBCuLtpP3L7qsMPyRuXaOCo+KSd1NBvXpUPAoMKR6HtfTK5kSabc0oUp1Ls9c/olS19r1gZqW3mwBQ
QvZhrY+acwTcpe0w8xZ3wm0HdT2gTNeNZGePFWwi5+3bm8FF38HOmUNna0jMu15xw1n4tH3Tn6wof5OOQl
vDG8EJDzwX8MqgAvhXkm1y/tO1kTTHu5Ty6woXhztZnQ/LWhct1OwK1jlgvQvMASrmLyXs9N8hYni8X4ME
+J6Fv02De699Vex/2jKmo6wZ1mD4oi6Q0e6KamxSBc3cGkIIl+yiVjz8/JYAWuSwAsrYBp6BtVN7GJxFmasmuX
pxK+lyuTY0mHw5e3133/OI1+qYnFEnoYQ9iNv7H5v1lXAwyBC1WlYOegyL356qMxtgGDini1UyaEtg9I97Lysa
8fc7HexlfBfbZK6VlGupOi/tG5IXbbUT7vJx6VZKPEUVIgNa2zO1ohhivqDvXQqjaREnCHm6nOCnG9X25mUW
9BvFXG+TWUTNGKMvjmGsKOaRxHomMfd8IKqArcwV0BHxJCUMWHP/cwW8p9zOLPhLmbFNQpZVNTFJ
R44OhQP975SEItcwgxa8vBTfIUZ1lUt2/1Ik67H1NjkOkQN7/HnmDVT/i0zCm+OSD02YexNdTmFcZ5TUBLBK
kHRgRUCkQOzmw98ToDyL5PZ7OQcKu9KLEjhvo7RbObdvknVW3nB1f2Hc3+fk/4C7Yo5tHaLQtHUfc9Z+Xlj
DCvZgdoze2c95P6JOdATKLz1SU1ZynRhrP/LWya9o0kkLTPNFadxqlRt5RbZuso/Lto+Lj1cEFg+gfmY1i6Sx+wO
3nK29DPULF6wTtEJvVAMU/bCsmnO+S/3cpaiyGePkZfPY4BZ0DF7eLsexxDk+h8Hxx2P0kN8vqzv0IBjHeLa79
BCvIKURxJNw9Eq/iGdKlKkRXginawYjPusMGK/p2/wK/aGHSin/E0BroNeKwhZD0hhDSt6oHMOZEsQBHwR
AFQSR8q7/0nYEiyqnaJPFdf4mh/HZjEWreoFmJjkaiFbYcf6VdooJ7hEr2zJ77ZnP2XSLjXqIEwL6buipONCjOHSr
1r2JiynCgd6kfphLQ1i8jfR17+DwDnBtqo22WrwbhTpA2KgsNySN/Xw45P3vsxYWenI368XEkGeXVmdlQ3/7cP
UOvliI7KAdEjhO93uDKn9esTxgGjRyFtCwND9IkXkGkTEZv2wbg5U7SuaTf/7HeNXqqEVAbxEyLKHUUboniei
4OoUEP8/J4iJqd4yGA29Aud6bochtL2ieoTnQCA4JlrpXHTqD4FJWyFFPNNCbUiZc7B0PXT7T2lzSeWtq2oUkE
RpmcxX5lUXe3aNpdD9/JTBD60RL6gAPZOoWKvOBZ+2yzrthiLPeKUUr63jH6WNKD8QZUyenV+KBTrMo17
YTAyKGW/pUq4K5XAOtLPLXY1kqBJZ9QSuW6xPkG+tQPvqXld5avk0E3VqQ2k1HqjctK3QFggnNj/4REmmt2
E5OAdAqLRSW3vWxJhjtVSbK2rdrghfFodbaHQmsbvAcX63/MNi61jlgvQvMASrmLyXs9N8hYni8X4ME+J6Fv
02De699VeCUtkQTzX8OIcUM/JoJrwg+CmTHfEQt9ktfTA0Bz+BlM7SA9s2fcQox6TkwF7sCoyTNHmiNhYSel
W9R1uBYaF2lyDrN/nuhYZpeVgfXDf0/eNWmcERpMaB8xdOGGkRkr9bpQvanLupTf8SLEWNJHJO+tDYsovLI
5XTMplrTJb3h/l0a5DlAmkyAuulaXlEZ447invEv9Ny4GR6QSVLLouReSgO4/xTLkMOiTEjslTyFdY600OqZSK
MXhyrqSCvYKl2y1fYFLOMD5zqrOnmAWgIuF6A2racn9zTCx2zd7POqi4+HQ9/RyJarFMk7UroOgHuP/4g122M
Al5lIZcMX8iB0jE5ROxxy0iPQGCPCDCCZZW73CeTK0vVGu2fh+8w0pELZTxG9Nnrhqqhi CjLZihp1n457t+Zq
xVJ2SDwu1pKiW5kH5leNzuoJsY96wMO+YqO88WbFPOiMtg0/zNMDBFkOZTaa/4egO2uNVVrrSE2SXwELwd
r9mCpn77WbeaQuRsm+pFgdOqB8sOnqHK50rI49OjNVxUnYs69AkYzEmfB5HIPsVE6QLpwSC3o+D/vQWwVl
ZhTqWR5UF3Tp+vBxqW12B6pw/YsUIHLMGUKv+0KZNLUdiUxTRcAz13GDxd8tcb6ZATv2OOS31f2KU5dr
BUZ9nXb8ZyTq8UMBywsMd7TCHTMc73OmG4hSq3qqe05FCzh3A7+bHR3QwP4Q8JRMof28IIMJn6TWhf6T1
NXLX2vqJ0OUolm4D1b62/NSqJui4oLjB+mOioBX9NNa5s2Ei+AUp270m1bnaU1q5FmgQXzQ05NjjYivvJhJavJ
77YxIIZiltnpdZF9DTj+6iXeIt9F4gR27B04WSjbrkTdFzVYEynMBAT9S0gmWOBZ5wH4WTgrtGdOPtAlGIf6Pto
qkw4NDzejrL9HOW+DZEvC58RFmrzIyh7NuYl8uLoDnrGdXTH8IuX+jSRzefspM5mr43oks15hmJPZrQEa4CsK
TQdEGueAqkSW1tgmW7uxbd3d/iS0yGCjci5rAq5dvarnjpWhzaWfDP/BytjUFWuo/Wg1aXPPAUARAskooea8X
VDZeXKPRJ0ooaQN8TWKcqbiJ4S4Qqog697joJX6JNaplTl5AQiQTOdDmLEPb68J7sBQKbdlT9wE7wM05b1fd
yfoWOt+gcJH7v4cabQwsR57E/9Al0Km1dU9RygHndfaNBXHmHWoiKEc8hxv6cIGaJWEafjJwI4NUkxeSD1UN
6UmClAM+Oxe5pBxvQhDOTWDjCB5GcePV6U7kD30sgDVEcju+1MkqtJRIjfbohwe2UefN0a/gwFUZgW6mf1t
9Ek6T8sO+mvT5MASGZRSxP4WBQgKaxYzv/jBrIbnGDfBeZzwWQlC762DiWbdFTWZn46HxSf8GsOeqW+9P
ACUwBU7zy8MXCvw9v0BPNHSEdRdhIqOzOxiHhAdqAJmGiq/vUTG9Ezuj9G6bochtL2ieoTnQCA4JlrpXHTq
D4FJWyFFPNNCbUiZc7BMLghTTM2S22/EC4b0N4+lFuBmffpmaOTtkVdhXogC+AXEIOy6SOwOA8w2gWBF
nPDBNFGjEepJCwL/QaytUfzGKruqpmdoxdlfK6BAAH0Kcf7S1l8cWivFThgwGFtfn3cYza4x7iIcU2Mxwg4b45k
8GYPGIJCeLM1rqlKW4Ar42bZ+RqdmDb72HFJTetlFRJU2x7cgkNKNir2o9snBUQJu3FUFRtcGucaqHCX9SO9I
ej5V3U0cn3EOp/ZnvQrirYclXo1eUqvyAY+oSsVb8hD5NeVqRfxQgHIO5rC+A3wYyUaM4vKERISn7gz75wTxr
KocGCnb//5vz2JXSDpy61mTGHG96/53NN/oTIK5w4KtWp1jZidOeTX+b200rn+6a1e+cgjzNsWhTOIXDpDuVog
qO/T4QWotJv7upR0lcgKhnby0tM3W5v8TWMASLtUpNzzfSmLlMHJmEljBJf4FD0h+ZuZSZDuIH+UsJUh5HLy
VVVIwMVo8mlMGC9zgni+jCnH0IjhSQsXFgUz6IbFBaBoNKo7vItRZEYsE/lodUkIfZpQ1vJ0V4fEpg478pf/Gjfw
8RHC2wOK1AJ4fF180Dxq3zkkyOB/zrfpt/SIBufspFnyQL6Hp/3NFewgVPErEsUSQDe5xbWrtJKzJwu8lY8xrpEsi

ARtQ1DqBoUB/8jrJ7+8TqjGBmpm+jznfIe6gI+2yEZ235NVg7wnL+FZ44HF2YXQO9+FCk9rLJkQ+VvP5nm3kp
FEuxTA7jJxKhchmGUgnL/48hU+dEDEnnX1UNmjGTp/Fb9ditAaGx+c7YJMI4dwO/mx0d0MD+EPCUTKH9vG
qamv4D5gvJROqtujQU8sdDlKJZuA9W+tvzUqibouKMuTdvAxY2JndXjAFvHEx5/5ANzuwD1sgozA9ilmOxY2D
0KfADm+xho3h55GHySnt400G36VZ25IloeKuoxdz7aTwZFDoMcp1lHQQX26XMOkMP3HOPAPLmmqtJh1Pd0
iP3I8JCxMFcZleikbbx8SA9V28rx2f94BoC6zvBGk31yAKmPYS7/rAwU9gfgFEy9onmgD33UgqObcqc3D7wCP
Meb1HXOrz1WGH+rz/LuNhTZAqx1oEAVOvzBC25TMSrbG5qXprxQ0VJHk9m/tNFPv85w6UJpZ86Lzt/anNEC
RsJv9u8uYwFppcLTvStCV4c+ucEUulUK5Dzsp0o5XL6zAmE5/aOKhuCV26NXd/yprpfTe+PaRkUXf3EqMGV2
GG6Cm6oYo+ptq5cp/zjlfoDbjzJHKol8MjIHfPXbqiye/Seb8W1sIVzf8aV46w5c/kDGTJzKt28/fgdeuMccPXBQYw
S3dzDGfm94SeP6aCz7NNJa0tlQv7ubMQOTElg9oQJegjbP6xsCt4DZ3k8LyRJ+U3bGqQDE6ELMnTQLqe8mRv
EOthanHPGyjohrSGdDyzKLmkEj1zFxgCFcZNz1Zy5Eqxuam9OCD95cnV26BJt8BDtt1x7ISN3BDmQl7ealcuMB
Sf2SsipCXPZAUmEkchjM06qqdLXs/m53/3C8K9EIth14XGshY3UrjAbnO/AynuZPlVsCubpUXhSz7Xhg/KEui9E
ZVcy0MGAu6Rf1II+ru1/UW33eZI6MfxBYVaVdACNK9UL1L2zvAzosBAYEHRvvDsR+7Pu/We5wwwQofoH+
rAb2VN9l/o7ckyjrGCHUkfKtaey/sab1TrvTmrH4CVaHpulJCEJVNXud9XeLmkVtSRDmjZXWD4CttIP8sLNPvM
n0gn28NDaFPiYFeiXPlTXX2/DzYvGrNQDALLA3GJG46zfD3j0G3ifBm6qGKRroIS/IFGovI9KnwakFk5HE7kns
lDp9ftayYbyuaBzTe/iJ2whS06zyCDDq9Y/2hmUvniXqRw8i3yXJr4hdhwknMtXv2JxDyeh1WT2LNtYMOLTnofc
K/h+ZBInxkaFeHNyxwCq0FauTQli5Xg+wQJvQoXjMeIlinzokJXFEGyfuleMc4epFE8ImhIXxQfSGSMFyoaP3r2
E4pEEvTjLkA8mX1T0hsmEt8FHQ1ZWQxvBJpQjPNBBcKkyALOl0PZp0qj7yzEconuodwO/mx0d0MD+EPCUT
KH9u1UEGoExSEHqvo6vSAbJStdDlKJZuA9W+tvzUqibouKLHtIw0akI+iE0G1TNnKF7K+MBfJe/m5wHizohJd
wO4fPPlEfNMhZF31fjo7UDJXZgg1xfRIvBrDmhQnxXROaaIMfAand0bDMTpRHzt3gJ7Sdr6Il6ySkYubsaxwepr
mQboWXR5REglavCf9g2oQ5tJB3cESf1u+yHZcz6iVcGkiy/jrhIaCZ8UNllp/tbYmEDmy5xjTgnMiVpcIeN7GfV/o
Ck1JaA/mUsTivV36Rl+DQcoO2ZyIxqAoax77ODXShX3M4s+EuZsU1CllU1MUlHjgzWoinczvi2gqbwTKEEzEH
Js2Pm35dJR+VoEzXXnw5RA3v8eeYNVP+LTMKb45IPTZh7E11OYVxnlNQEsEqQdGHjVGkbRd4P/5OBZkfRr
+O0rkMD7sNWhszMaXIhRIa/rztX60HgvrlQCNgsUu2sqrIl7AtAXjxzg7yfser8y9AIr3atXlpLLUcbFZLB9A0RVup
AYJiCBs3X8LzTWh+MM72U96mbgO8Vvh9z0PWMvtq47S8WPxnb3HFcu3jhz+z0fcY6apTEAHpY+f70yR/9J+2
oQ+NVJ9DBi3YIS3JzNorFYGpfZgJB44tpZqmEMcUVDKav5YvEFn7oA4ymVIsQenuV1jAFRQ2rQQvSD3ik4L
TodN0CekUP3+0JHyMDUw5x5FX/AJ+BNHlWvhcp2AqaY3UA7i6miN/oHq3sdx2/QSWYXnASlEVuJrf+Gb4W
ObzIq843qAfMC/29ZO0LdLl8GpnwutlLPL0e6I3A42TswhuftT1fGJIAoIuaVzEfgKODQQ2zjQ1rn/UlvFlJnTdtmH
nrMzFMl14waepSDTDvWUK2r/hNHl9NofUUI6eUExtMXLksaDB1kF3ppvZp3m12kUdZWffSQ7LoNoAxpdhy4
h9+bbYrK3J9hYayp5fxWR8UwFirIYR/ntjPLRrbtSNvLUomf7mhkkrqJWSHyF0lwkiaN/rHCVApqMEZdIDOyutY
vsW/DNtb8wu6xanz1AJDFiCPKCmz4wgCrKql1gtplr6BzAicKNiWzvnabolHW244le+cgjzNsWhTOIXDpDuVogz
hOkZv53dMFVmTw63MhhKHby0tM3W5v8TWMASLtUpNwWkIxOlKi6/mvCpir25WOc5eOVCr4HJmL4Jux+9
TIirEGfBS57aWEAUrrsy4I+cukbTxw3L4grdnx2sslMwUfd4Si0kUdxUI7o0dVle+L1tBXs4SVlR4dTqhfSmWTbuq
rrd+9kbDGYU1D0g9xMZlQJTgPJxkJAdVhufwin+ZBs3AuDs7kN8nj50V3JpEPNXIRHW0OEvxjFrKxULZ/JFWu
3w8l/f3CPSP4BB47TjRDn5KbE5Sr1PNWJMkPd58mv0cQXHPsl/LAJkxauOgDAlDtEI1EUmapW6HKqLWUNFc
RWxuwIT4HNJqTp35gKzMLWmh5c/FwMsgaxDLys0767TLhS6bochtL2ieoTnQCA4JlrpXHTqD4FJWyFFPNNC
bUiZc4Lm3PPW/9VzLIOjVe4bJRHNrBv+ku4kQWH9/AMaQAbtqdhCFQnz8ZdJOTdt2VulKJu3tB65NeE9qGYO
1+tEOLRGYa2ebx4oSVa/oHH7nbuMxiChfq/Hz1MGFNlnNuVl8YQ5NAVm1ILV+y9A90B2glvIqkNuLgV0Kxm
W0FeoAbxEOmgixShmF5laozMDxxW/dWEMgyWUf7H3QVi70Aw3+kR0lVyZVFqyOwfTiqbB7JEDz106ai5ngo
oZrL7G046COM5+r0aB/3orbCDIR+7AU9drZkNTZtEoS8ijfug9fWHPti/4Flu0o3WtsWTPpWOvl2bnN19VWDT9
0J6KrfF0UHangKpEltbYJlu7sW3d3f4ksSKuavdBfv+AXMJU3faZ5k2lnwz/wcrY1BVrqP1oNWlABSU9AhM1sP9
MzK0IuqN1WXEkiZ/Q2UXq2SgA9/yMYmvJiPys6r7vy4pnK/G44nBOlAJzPdkc83aFuAZfxiLT7htWv4ixUFzMe
xJoE1Gpu53fMY197PyKSo8zmII+ix/DhuofUc+AnYbF/FID6MZXp0qL+vaqHpQIg3vfv0dJ7Z/3McBUNht4w/rG
D1GhrpD8VEOdyBZ16gnVeGclC7ZWj742OLiBUfvaO9Gl6xJ1t4CXsnAWLCiLGlRR/NAymKWw8zvSahOuQ8
zhahFJCc5hOCtFvkSOQ0su0s7mFlRzMxGV+dmOfKrewM8+nMv0XzTWDaSw4alkeMtwRb5hTHGvT+AIx59V
YxyBYiTQjqHESlHuRZkKTMRhm1iWpCkg9beAapuJoQl4cZc1+oKZL8s3k6oSzkB1m6+JC55FVHZnfZ9zOLPh
LmbFNQpZVNTFJR4ywlv7F97iTEf+G6f2/2/N4R8Cjks0MOU9gg2fIzcvwUQN7/HnmDVT/i0zCm+OSD02YexN
dTmFcZ5TUBLBKkHRn/qL2P6RQ+vkFvRcgTNp4KAiN5HC+RDDpDQPHYdME233+/qbkpBEHcpug/QthSoQx
xzAfZkCQ4q52UfktJ/8RwFhG7FXroM85dTKtQH69YrcQnsgDm5NlmE53nrsd+Zgfus4yw3UIL6PWjuX2ebEDbp
6ra4HE2kAY9Q/1aJ584dcJtBaGPAe29V3dhMGzW9iqxVxecK7rVXiwbI5EL9gHhp8071QWARWWpcEKuJxpYI
bUVfCwD9wyvHMC9CyQUEKEYgzlhm9udTTKvzOBlDta+shjBxCnyIhUv7mdgRZD78wrU81BvJwwkAlefMxa
WsskexcrC1QZrXFu6aDi4aPDYJrEvhhDkEbuyPxXzquN8vdz08izW1b5w0gYFuE2/xZVX/NytUzVp9GpCXVFw
PEBY4lHeyqi/SX+VS7cqpYuVUN8ttUVY8iVeNoAUMOwzlElMQJYoYDSHsNLsy+f0oStr//YmVhH0UDaID9qs
IVVRfqWjPs79Jn23WoIDMquwvm39j3mH1Ny6xxfVAeC/nBLpLeMovyM25at5f9uJJxHIZLISlFUBlyA+7hUJNn
a8N6mCrSHdw6cS0dkyNF0OJBr1NKfz9AlS1BU8uch1Ms4iQXZEWUP59Q9h0102yG5a97zkZXM7U0uNTGA8
Cdm7koeWzBFIwMuLS+IvRj81zWG1HPsoxwWplckHw2axiJl4jqxuk67zFOTmC6dTBQP8Ed4Hv8kuSh8QhD+y
7pa8986OWaeyqFu8HXY63/VvWKk/hckV0D6eZ08R7MgBtXN7J+DIcepb5fHUfxnM8kOl8yv325/rJTzJQBgVPy
pEC7m1ZY+f6yU8yUAYFT8qRAu5tWWPn+slPMlAGBU/KkQLubVlj5/rJTzJQBgVPypEC7m1ZY+f6yU8yUAY
FT8qRAu5tWWPn+slPMlAGBU/KkQLubVlj5/rJTzJQBgVPypEC7m1ZY+f6yU8yUAYFT8qRAu5tWWPn+slPMl
AGBU/KkQLubVlj5/rJTzJQBgVPypEC7m1ZY+f6yU8yUAYFT8qRAu5tWWPn+slPMlAGBU/KkQLubVlj5/rJTz
JQBgVPypEC7m1ZY+f6yU8yUAYFT8qRAu5tWWPn+slPMlAGBU/KkQLubVlj5/rJTzJQBgVPypEC7m1ZY+f6
yU8yUAYFT8qRAu5tWWNyedQPNv/Un9CqVGd6o/gW5/rJTzJQBgVPypEC7m1ZY+f6yU8yUAYFT8qRAu5tW
WPn+slPMlAGBU/KkQLubVlj15ct3kKTKB+94z6V9FeKGqP/PbHSJPY3pQRmBiCxmAyIdB+QWpEfUBZEoLl
Eoa3Mj/JIixBfxVaV4G3q0GD9oVlSIFh1mnSWs3ZdV0iX3FGpSyCb2zm4KIfOgeb/g5osVS5v60JVXEjgPfG0AX

icrSsc5eRllPr1w/0mHQT+QHZXrAQagR/wBC0LBb1W5pctCwI9Kg/dQQyF1Jy44H9y7Sx7yqTXTUILttebS0sO6
fGjrO1yi9aSbXQds000Drgw7rQpYSwQoKNdUOiOxsH9pbKc3+v4L8I1ImjXhR+Z2/2kUTmtDNytAwGViOyaw
mAC/r9sdPmnIHb5n5mbT1SmC+TD49h4C17kZrVnySaoFfF03tsO5Dku68HmptaE7IkmgEfktMinYAH7Q6/IEtPd
c0sFq0lwbVVD0aO9P4SryJ+/qc7Jw1chezQ16s9hCvb3OELopy5u1KTZYjaQULbBLsb+dcaYiaZKV4qONiPJ0xio
f4+O7zpQ8QkGg5pEvNefoC2jAIPmK8Zy8+xmKxH/cc1gPitD5nalyc4agntHbdQKU+hvfY/vKIy2VSWIeUiY1Re
7l0juLhSDoV+S6ZQw6k7DCCA6LP7paMRv4MQeQopC9lIOxxy88Vg0S4sYSzPjqMNe3uHlZpYZdRgpEz3b5Hs
hZjYpX0scDbfJutREUk6HtGSGH9vFa66u1UDdDXOtiQYSkO/p7J48KxMM8/llQcPNi3wwuwzaREYOgcu7rX3L
VCkk2zEC/SDJOaoZux3YnId+4RqIsGcRYh2JhbziCKtihx9L1x0B4chdsrENcrIpudPMWSjNUXZjEzc1XG+GEdk
Ud6sxXaoK+47F2cF3wFmt6tCGfjcOOWHRypB/a2p1/hDMIpvcU5kaD2qq3ZI5szBeEmFEPdnZkPQQv98yF2jde
T6uneGrePP8POX72v31gJrDD2PTxKaC4ldao3pis9+zWKMvjsKTI/s1EV1FnbnloC4u1uNcwIQrGWP4WVvd/gFI
3EZ5XIaB9CB+dmfOljGerDj6p5J5RA6nZLjkXn2Qc+kMzDypKRKaYWGTt9Wh33nzfnsEJWRXw4CPMNlnaZy
aIWAY1UCHUkvO8JkVPCawaMuWHx6+KmgLeQZ71PilsgvHjQpj1MdR+uNE0BYfEfOnyAccP3cOZANGiMS
6dBG+3PXDMvVk9T62SN3teQqciYKWaST/QK+npEQx4vgiwqgHg6Joo32Trkfc7EmVbtrTdj1UJPgZxdV2y0k1d
cn/vVjHuDnwK33YO+YwlrU6vrZUZEsDaGhHHbKmSX96E9TP3SkYL3hepds1OtR8wOLv2I5Yd7Ndy5aE2wIS
Rvryb6h2NBMfwr09Pgmel510m24fgwnBnPwklAASt/sbdisM8WVxYoeLFmORUbIVi0FE7rJMOfdKAAAICKsvs
Me1gxIGefdrsgNdtfpaMnww7DkYS/ORCI5hQUcVxYgs6eTqDt0nA8OhMCdcOjydD/9U8wr3becX2QCiJMyre6v
Il0CLEv9Qj0hDyAwnYh9DKcPyxQa7ZTO4TBQf2IhQSOpW906yZv/JeU96fRA1aFfpPGQtEPiG3wK3ax819rCU
3NZW9d2P9K0H5TaoO6yJaIY1+HmQBo+ce3WCSOg/U7o8ut06t73hbrGrS16eD8mqplbM/BuAX9Gm9DhfpRx5
763cpfz20ROQatfpLf80QDoAmhYwfZN2RLD2/4RUoZROIZoxWG5nr2XeMsJtqaTGDqGtQic/fQRkeHFdQZXrk
+uBN3O2EXyezkOAd2PZBC+DYDI7+aLb1NWpFNRiZq5TJwB5WknWZFLBJ2y1BNhMqpKOEoA0bTieyOGq
PDq5W8H+i79FGeQbckbe3nrnlOXRnVVDxLjes+xdMgaGkeys+dIs++4oes0L6Zg2Vjcl4108nSS81MY2qGYezW
SjhW3UhFFaK8iEN1jyXRWOWnvctII/MiPxO2DDYh8cwqt28siuWLLzP4Rzf9Y9AnQa7SqhgXx3SKmbkX5fHK
o7yetaLm/Iiwt1kYzZzEK33Ige25eHhycns1lmqrTrLbepk719ZMMAMiLZPasH46rO59hMZMkLhEHmgX6gCEC
Vf2SqIqVRxOEeFkDpiFniYRZY7rBGPa0qY7N7ahd9caUpsZ+VIACWJ7D1XpGorOgnRE0TJkLhq8S2ijT4XmE
WSFhlF+9m/FidUeLsh0djMmnutPKwbGUvwwrQe42TrXcsv2V31F8hNn3aC6wh2ztX4R227KLru2Vz3vHfba4SG
CQkGlMMkWqsPCA7QHaTR88m5QxKwVNfRbqA5IkaDB0K27nDyFbase2QdqbqIBliP2CQJwfZCPOaLkfFob3
CHdbdgO7if1gS/uE7aEe/Mcvg1kn+lBrk/r3fZs1DsWyElb9KFE2h7EmxmE+lmAeS4fik8CXjNjutjMOPkjZ1eZ6fix
y0+3ldyx72XymcY2w0UQP2NsLUL9c8VfyEnBLuJFBG0LskFpIlxb9AiewA/1fVeqRF+TVIhCSALpLBF6EqbJC
XPTIPEiFLwlSpEEYa5cScpcz3jEbDIu25/BZDU3OM+2/1d5RI9mMPEi4C1GpOTIJuEUFGNPja5CvirLD8g91fh6
lvxWcmNgCuE7TzGsnYiOANDRErOCsBarF4bVFpVRzxmz1J8b22BmX4/tl2S/shZkBbJEx7djJbiUG64nU/wLQT
QbmtrZZd8gpKB5NFbSoC//P3NQ2Ytdd/RDcF3VXFQ1E+NdIqZJgTaYQVjAC/uqpXrg9U8GtmLmdvLIIZAHux
+UCE194Dpl2awoApmJ/5k0EyB+VCXg/BuCAfXIWut8BqCVog3792bhtwwboNXRmSw5E/fiIz+IyUBfJ3qn+CiO
gEL1raHth2R3uRSFH7FgqKx2TYdkChSexsOwRWMg5MX5YkOzeRhhIXtm1+0rRgwQ3MH7j9t+DpbwpxWqfv
YPDSuc3FhtJ2yGkCuwCgQvaK/ZvEzQlIzIcP5jKfBISjyF5ski6IKIU8gjKjhTPB9R7bjZvzi53yrUhc04+o0SAeyUB
podmoeEGYDuDKMFAt0u6ONYlYEQgNRFHN3wkSzOxM67pqE6Q4q2NFV7wqxjq1evTcKrXKqZjZRTOkj08o
mA0bvsypyMjt+inggQtA7XWbZsTvDE/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 ОПК- 2.1 и ОПК-10, индикаторы И-ОПК-2.1_1 и ИД-ОПК-10_2)

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 ОПК- 2.1 и ОПК-10, индикаторы И-ОПК-2.1_1 и ИД-ОПК-10_1)

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 функций.

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

Список вопросов к зачету

На зачете и экзамене проверяется сформированность компетенции ОПК-3,(индикаторы И-ОПК-3_3 и И-ОПК-3_2).

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 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 критоанализ.

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 ГПСП. Линейные рекуррентные последовательности. Оценка периода ЛРП. Минимальный многочлен ЛРП. Линейная сложность последовательности. Алгоритм

Берлекэмпа-Месси. 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 критоанализ.

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 ГПСП. Линейные рекуррентные последовательности. Оценка периода ЛРП. Минимальный многочлен ЛРП. Линейная сложность последовательности. Алгоритм Берлекэмпа-Месси. 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-Гамаля. Схема Меркля-Хеллмана. Гибридная схема шифрования. Цифровая подпись. Схемы цифровой подписи на основе RSA. Схема цифровой подписи Эль-Гамаля: 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.

Правила выставления оценки на экзамене.

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

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 излагается 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
«Методы и средства криптографической защиты информации»

Методические указания для студентов по освоению дисциплины

Основной формой изложения учебного материала по дисциплине «Методы и средства криптографической 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.