Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новосибирский государственный технический университет»

Кафедра защиты информации

“УТВЕРЖДАЮ”
ДЕКАН АВТФ
к.т.н. Рева И. Л.
“___”_____ _____ г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
Криптографические методы защиты информации

Образовательная программа: 10.03.01 Информационная безопасность, профиль: Комплексная защита объектов информатизации

Курс: 3, семестр : 6

Факультет автоматики и вычислительной техники,

		Семестр
№	**Вид деятельности**	**6**
1	Всего зачетных единиц (кредитов)	3
2	Всего часов	108
3	Всего занятий в контактной форме, час.	67
4	Лекции, час.	36
5	Практические занятия, час.	0
6	Лабораторные занятия, час.	18
7	из них в активной и интерактивной форме, час.	8
8	Аттестация, час.	2
9	Консультации, час.	11
10	Самостоятельная работа, час.	41
11	Виды самостоятельной работы (курсовой проект, курсовая работа, РГЗ, подготовка к контрольной работе)	
12	Вид аттестации	Э

Новосибирск 2017

Рабочая программа составлена на основании федерального государственного образовательного стандарта высшего образования по направлению (специальности): 10.03.01 Информационная безопасность

ФГОС введен в действие приказом №1515 от 01.12.2016 г. , дата утверждения: 20.12.2016 г.

Место дисциплины в структуре учебного плана: Блок 1, базовая

Рабочая программа разработана на основе компетентностной модели выпускника по направлению (специальности): 10.03.01 Информационная безопасность

Рабочая программа обсуждена на заседании кафедры

ЗИ, протокол заседания кафедры №6 от 20.06.2017

Утверждена на совете факультета автоматики и вычислительной техники, протокол № 6 от 21.06.2017

Программу разработал:

доцент, к.ф-м.н. Котов Ю. А.

Заведующий кафедрой:

с.н.с., к.т.н. Трушин В. А.

Ответственный за образовательную программу:

заведующий кафедрой Трушин В. А.

1. Внешние требования

Таблица 1.1

***Компетенция ФГОС*: ПК.1** **способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации; *в части следующих результатов обучения*:**
з2. знать криптографические стандарты и руководящие документы по их применению
у2. уметь применять криптографические стандарты
***Компетенция ФГОС*: ПК.2 способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач; *в части следующих результатов обучения*:**
з3. знать алгоритмы шифрования и криптоанализа
у3. уметь реализовывать алгоритмы шифрования и криптоанализа
***Компетенция ФГОС*: ПК.3 способность администрировать подсистемы информационной безопасности объекта защиты; *в части следующих результатов обучения*:**
з3. знать место криптографических методов в подсистемах информационной безопасности объекта защиты
у2. уметь определять влияние криптографических методов на защищенность подсистем информационной безопасности объекта защиты
***Компетенция ФГОС*: ПК.6 способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации; *в части следующих результатов обучения*:**
у4. уметь оценить эффективность применение криптографических методов защиты информации

2. Требования НГТУ к результатам освоения дисциплины

Таблица 2.1

Результаты изучения дисциплины по уровням освоения (иметь представление, знать, уметь, владеть)	**Формы организации занятий**
Криптографические методы защиты информации	
ПК.1.з2 знать криптографические стандарты и руководящие документы по их применению	
1.знать криптографические стандарты и руководящие документы по их применению	Лекции; Лабораторные работы; Самостоятельная работа
ПК.1.у2 уметь применять криптографические стандарты	
2.уметь применять криптографические стандарты	Лекции; Лабораторные работы; Самостоятельная работа
ПК.2.з3 знать алгоритмы шифрования и криптоанализа	
3.знать алгоритмы шифрования и криптоанализа	Лекции; Лабораторные работы; Самостоятельная работа
ПК.2.у3 уметь реализовывать алгоритмы шифрования и криптоанализа	
4.уметь реализовывать алгоритмы шифрования и криптоанализа	Лекции; Лабораторные работы; Самостоятельная работа
ПК.3.з3 знать место криптографических методов в подсистемах информационной безопасности объекта защиты	
5.знать место криптографических методов в подсистемах информационной безопасности объекта защиты	Лекции; Лабораторные работы; Самостоятельная работа
ПК.3.у2 уметь определять влияние криптографических методов на защищенность подсистем информационной безопасности объекта защиты	
6.уметь определять влияние криптографических методов на защищенность подсистем информационной безопасности объекта защиты	Лекции; Лабораторные работы; Самостоятельная работа
ПК.6.у4 уметь оценить эффективность применение криптографических методов защиты информации	

7.уметь оценить эффективность применение криптографических методов защиты информации	Лекции; Лабораторные работы; Самостоятельная работа

3. Содержание и структура учебной дисциплины

Таблица 3.1

Темы лекций	Активные формы, час.	Часы	Ссылки на результаты обучения
Семестр: 6			
Дидактическая единица: Шифры			
1. Назначение и клачссификация шифров. Основные определения	0	4	1, 2, 3, 4, 5, 6, 7
2. Шифр перестановки	0	4	1, 2, 3, 4, 5, 6, 7
3. Шифр замены	0	4	1, 2, 3, 4, 5, 6, 7
4. Шифры с открытым ключом	0	4	1, 2, 3, 4, 5, 6, 7
5. Стандартные шифры	0	4	1, 2, 3, 4, 5, 6, 7
Дидактическая единица: Криптоанализ			
6. Методы криптоанализа	0	4	1, 2, 3, 4, 5, 6, 7
Дидактическая единица: Стандартные шифры			
7. Шифры DES, AES, ГОСТ	0	4	1, 2, 3, 4, 5, 6, 7
Дидактическая единица: Приложения шифров			
7. Генерация псевдослучайных последовательностей	0	4	1, 2, 3, 4, 5, 6, 7
8. Шифры с открытым ключом	0	4	1, 2, 3, 4, 5, 6, 7

Таблица 3.2

Темы лабораторных работ	Активные формы, час.	Часы	Ссылки на результаты обучения	Учебная деятельность
Семестр: 6				
Дидактическая единица: Шифры				
1. Частотные характеристики текстов	1	2	1, 2, 3, 4, 5, 6, 7	Частотные характеристики текстов
2. Шифр перестановки	1	2	1, 2, 3, 4, 5, 6, 7	Шифр перестановки
3. Шифр замены	1	2	1, 2, 3, 4, 5, 6, 7	Шифр замены
4. Шифр замены и перестановки	1	2	1, 2, 3, 4, 5, 6, 7	Шифр замены и перестановки
Дидактическая единица: Криптоанализ				
5. Криптоанализ классических шифров	1	2	1, 2, 3, 4, 5, 6, 7	Криптоанализ классических шифров
Дидактическая единица: Стандартные шифры				
6. Шифры DES, AES, ГОСТ	1	4	1, 2, 3, 4, 5, 6, 7	Шифры DES, AES, ГОСТ

Дидактическая единица: Приложения шифров				
7. Шифр с открытым ключом RSA	1	2	1, 2, 3, 4, 5, 6, 7	Шифр с открытым ключом RSA
8. Электронная цифровая подпись RSA	1	2	1, 2, 3, 4, 5, 6, 7	Электронная цифровая подпись RSA

4. Самостоятельная работа обучающегося

№	Виды самостоятельной работы	Ссылки на результаты обучения	Часы на выполнение	Часы на консультации
Семестр: 6				
1	Подготовка к занятиям	1, 2, 3, 4, 5, 6, 7	21	4
Подготовка к занятиям: Методы и средства защиты компьютерной информации. Ч. 1 : методические указания к лабораторным работам для 4 курса АВТФ / Новосиб. гос. техн. ун-т ; [сост. Ю. А. Котов]. - Новосибирск, 2010. - 35, [1] с. : ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000146768				
2	Подготовка к аттестации	1, 2, 3, 4, 5, 6, 7	20	7
: Методы и средства защиты компьютерной информации. Ч. 1 : методические указания к лабораторным работам для 4 курса АВТФ / Новосиб. гос. техн. ун-т ; [сост. Ю. А. Котов]. - Новосибирск, 2010. - 35, [1] с. : ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000146768				

5. Технология обучения

Для организации и контроля самостоятельной работы обучающихся, а также проведения консультаций применяются информационно-коммуникационные технологии (табл. 5.1).

Таблица 5.1

Деятельность	Информационно-коммуникационные технологии
Информирование	e-mail; Социальные сети
Консультирование	e-mail
Контроль	Портал НГТУ
Размещение учебных материалов	Портал НГТУ

6. Правила аттестации обучающихся по учебной дисциплине

Для аттестации обучающихся по дисциплине используется балльно-рейтинговая система (БРС), позволяющая выставлять оценки по традиционной шкале и 15-уровневой ECTS. Краткая информация о БРС приведена в табл. 6.1.

Таблица 6.1

Оцениваемые виды деятельности обучающихся	Мин. балл	Максимальный балл
Семестр: 6		
Лабораторная:	0	30
Курсовая работа:	0	30
Экзамен:	20	40

В таблице 6.2 представлено соответствие форм контроля заявляемым требованиям к результатам освоения дисциплины.

Таблица 6.2

Коды компетенций ФГОС	Результаты обучения	Формы контроля	
		Защита Л/Р	Экзамен
ПК.1	з2. знать криптографические стандарты и руководящие документы по их применению	+	+
	у2. уметь применять криптографические стандарты	+	+
ПК.2	з3. знать алгоритмы шифрования и криптоанализа	+	+
	у3. уметь реализовывать алгоритмы шифрования и криптоанализа	+	+
ПК.3	з3. знать место криптографических методов в подсистемах информационной безопасности объекта защиты	+	+
	у2. уметь определять влияние криптографических методов на защищенность подсистем информационной безопасности объекта защиты	+	+
ПК.6	у4. уметь оценить эффективность применение криптографических методов защиты информации	+	+

Фонд оценочных средств по дисциплине представлен в приложении № 1 к рабочей программе.

7. Литература

Основная литература

1. Лапонина О. Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия : курс лекций : учебное пособие для вузов по специальности 510200 "Прикладная математика и информатика" / О. Р. Лапонина ; под ред. В. А. Сухомлина. - М., 2005. - 604, [1] с. : ил., табл.

2. Осипян В. О. Криптография в задачах и упражнениях / В. О. Осипян, К. В. Осипян. - М., 2004. - 143 с.

3. Котов Ю. А. Криптографические методы защиты информации. Шифры : учебное пособие / Ю. А. Котов ; Новосиб. гос. техн. ун-т. - Новосибирск, 2016. - 57, [1] с.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000232326

Дополнительная литература

1. Баричев С. Г. Основы современной криптографии : учебный курс / С. Г. Баричев, В. В. Гончаров, Р. Е. Серов. - М., 2002. - 175 с. : ил.

2. Кузьминов Т. В. Криптографические методы защиты информации / Т. В. Кузьминов ; отв. ред. В. А. Евстигнеев. - Новосибирск, 1998. - 185 с. : ил.

Интернет-ресурсы

1. ЭБС НГТУ : http://elibrary.nstu.ru/

2. ЭБС «Издательство Лань» : https://e.lanbook.com/

3. ЭБС IPRbooks : http://www.iprbookshop.ru/

4. ЭБС "Znanium.com" : http://znanium.com/

5. :

8. Методическое и программное обеспечение

8.1 Методическое обеспечение

1. Минин И. В. Криптографические методы защиты информации : учебно-методическое пособие / И. В. Минин, О. В. Минин ; Новосиб. гос. техн. ун-т. - Новосибирск, 2009. - 31, [1] с. : табл.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000121807

2. Методы и средства защиты компьютерной информации. Ч. 1 : методические указания к лабораторным работам для 4 курса АВТФ / Новосиб. гос. техн. ун-т ; [сост. Ю. А. Котов]. - Новосибирск, 2010. - 35, [1] с. : ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000146768

8.2 Специализированное программное обеспечение

1 Windows

2 Office

9. Материально-техническое обеспечение

Презентационное оборудование

№	Наименование	Назначение
1	Презентационное оборудование (мультимедиа-проектор, экран, компьютер для управления)	Применяется при проведении лекций

Компьютерный класс

№	Наименование	Назначение
1	Компьютерный класс (Компьютеры объединены в локальную сеть с выходом в Internet)	Применяется при проведении лабораторных работ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новосибирский государственный технический университет»

Кафедра защиты информации

“УТВЕРЖДАЮ”
ДЕКАН АВТФ
к.т.н., доцент И.Л. Рева
“___”_____ _____ г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

УЧЕБНОЙ ДИСЦИПЛИНЫ

Криптографические методы защиты информации

Образовательная программа: 10.03.01 Информационная безопасность, профиль: Комплексная защита объектов информатизации

Новосибирск 2017

1. **Обобщенная структура фонда оценочных средств учебной дисциплины**

Обобщенная структура фонда оценочных средств по дисциплине Криптографические методы защиты информации приведена в Таблице.

Таблица

Формируемые компетенции	**Показатели сформированности компетенций (знания, умения, навыки)**	**Темы**	**Этапы оценки компетенций**	
			Мероприятия текущего контроля (курсовой проект, РГЗ(Р) и др.)	**Промежуточная аттестация (экзамен, зачет)**
ПК.1/Э способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	з1. знать криптографические стандарты и руководящие документы по их применению	Генерация псевдослучайных последовательностей Криптоанализ классических шифров Методы криптоанализа Назначение и клачссификация шифров. Основные определения Стандартные шифры Частотные характеристики текстов Шифр замены Шифр замены и перестановки Шифр перестановки Шифр с открытым ключом RSA Шифры DES, AES, ГОСТ Шифры с открытым ключом Электронная цифровая подпись RSA	Отчет по лабораторной работе 1, разделы 1-5	Экзамен, вопросы 1-4
ПК.1/Э	у1. уметь применять криптографические стандарты	Генерация псевдослучайных последовательностей Криптоанализ классических шифров Методы криптоанализа Назначение и клачссификация шифров. Основные определения Стандартные шифры Частотные характеристики текстов Шифр замены Шифр замены и перестановки Шифр перестановки Шифр с открытым ключом RSA Шифры DES, AES, ГОСТ Шифры с открытым ключом Электронная цифровая подпись RSA	Отчет по лабораторной работе 1, разделы 1-5	Экзамен, вопросы 5-9
ПК.2/Э способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	з3. знать алгоритмы шифрования и криптоанализа	Генерация псевдослучайных последовательностей Криптоанализ классических шифров Методы криптоанализа Назначение и клачссификация шифров. Основные определения Стандартные шифры Частотные характеристики текстов Шифр замены Шифр замены и перестановки Шифр перестановки Шифр с открытым ключом RSA Шифры DES, AES, ГОСТ Шифры с открытым ключом Электронная цифровая подпись RSA	Отчет по лабораторной работе 2, разделы 1-5	Экзамен, вопросы 10-14

ПК.2/Э	у3. уметь реализовывать алгоритмы шифрования и криптоанализа	Генерация псевдослучайных последовательностей Криптоанализ классических щифров Методы криптоанализа Назначение и клачссификация шифров. Основные определения Стандартные шифры Частотные характеристики текстов Шифр замены Шифр замены и перестановки Шифр перестановки Шифр с открытым ключом RSA Шифры DES, AES, ГОСТ Шифры с открытым ключом Электронная цифровая подпись RSA	Отчет по лабораторной работе 2, разделы 1-5	Экзамен, вопросы 15-17
ПК.3/Э способность администрировать подсистемы информационной безопасности объекта защиты	з3. знать место криптографических методов в подсистемах информационной безопасности объекта защиты	Генерация псевдослучайных последовательностей Криптоанализ классических щифров Методы криптоанализа Назначение и клачссификация шифров. Основные определения Стандартные шифры Частотные характеристики текстов Шифр замены Шифр замены и перестановки Шифр перестановки Шифр с открытым ключом RSA Шифры DES, AES, ГОСТ Шифры с открытым ключом Электронная цифровая подпись RSA	Отчет по лабораторной работе 3, разделы 1-5	Экзамен, вопросы 18-20
ПК.3/Э	у2. уметь определять влияние криптографических методов на защищенность подсистем информационной безопасности объекта защиты	Генерация псевдослучайных последовательностей Криптоанализ классических щифров Методы криптоанализа Назначение и клачссификация шифров. Основные определения Стандартные шифры Частотные характеристики текстов Шифр замены Шифр замены и перестановки Шифр перестановки Шифр с открытым ключом RSA Шифры DES, AES, ГОСТ Шифры с открытым ключом Электронная цифровая подпись RSA	Отчет по лабораторной работе 4, разделы 1-5	Экзамен, вопросы21-23
ПК.6/Э способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	у4. уметь оценить эффективность применение криптографических методов защиты информации	Генерация псевдослучайных последовательностей Криптоанализ классических щифров Методы криптоанализа Назначение и клачссификация шифров. Основные определения Стандартные шифры Частотные характеристики текстов Шифр замены Шифр замены и перестановки Шифр перестановки Шифр с открытым ключом RSA Шифры DES, AES, ГОСТ Электронная цифровая подпись RSA	Отчет по лабораторной работе 4, разделы 1-5	Экзамен, вопросы24-28

2. Методика оценки этапов формирования компетенций в рамках дисциплины.

Промежуточная аттестация по дисциплине проводится в 6 семестре - в форме устного экзамена, который направлен на оценку сформированности компетенций ПК.1/Э, ПК.2/Э, ПК.3/Э, ПК.6/Э.

Кроме того, сформированность компетенций проверяется при проведении мероприятий текущего контроля, указанных в таблице раздела 1.

Общие правила выставления оценки по дисциплине определяются балльно-рейтинговой системой, приведенной в рабочей программе дисциплины.

На основании приведенных далее критериев можно сделать общий вывод о сформированности компетенций ПК.1/Э, ПК.2/Э, ПК.3/Э, ПК.6/Э, за которые отвечает дисциплина, на разных уровнях.

Общая характеристика уровней освоения компетенций.

Ниже порогового. Уровень выполнения работ не отвечает большинству основных требований, теоретическое содержание курса освоено частично, пробелы могут носить существенный характер, необходимые практические навыки работы с освоенным материалом сформированы не достаточно, большинство предусмотренных программой обучения учебных заданий не выполнены или выполнены с существенными ошибками.

Пороговый. Уровень выполнения работ отвечает большинству основных требований, теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, необходимые практические навыки работы с освоенным материалом в основном сформированы, большинство предусмотренных программой обучения учебных заданий выполнено, некоторые виды заданий выполнены с ошибками.

Базовый. Уровень выполнения работ отвечает всем основным требованиям, теоретическое содержание курса освоено полностью, без пробелов, некоторые практические навыки работы с освоенным материалом сформированы недостаточно, все предусмотренные программой обучения учебные задания выполнены, качество выполнения ни одного из них не оценено минимальным числом баллов, некоторые из выполненных заданий, возможно, содержат ошибки.

Продвинутый. Уровень выполнения работ отвечает всем требованиям, теоретическое содержание курса освоено полностью, без пробелов, необходимые практические навыки работы с освоенным материалом сформированы, все предусмотренные программой обучения учебные задания выполнены, качество их выполнения оценено числом баллов, близким к максимальному.

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новосибирский государственный технический университет»
Кафедра защиты информации

Паспорт экзамена

по дисциплине «Криптографические методы защиты информации», 6 семестр

1. Методика оценки

Экзамен проводится в устной форме, по билетам. Билет формируется по следующему правилу: первый вопрос выбирается из диапазона вопросов 1-28, задача выбирается из диапазона задач 1-10. В ходе экзамена преподаватель вправе задавать студенту дополнительные вопросы и задачи из общего перечня (п. 4).

Форма экзаменационного билета

НОВОСИБИРСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
Факультет АВТФ

Билет № _____
к экзамену по дисциплине «Криптографические методы защиты информации»

---

1. Шифры и шифрование. Основные понятия и определения
2. Зашифровать свою фамилию, имя и отчество, используя шифр Гронсфельда. В качестве ключа использовать свое имя

Утверждаю: зав. кафедрой ____ _____ должность, ФИО
(подпись)
(дата)

2. Критерии оценки

- Ответ на экзаменационный билет считается **неудовлетворительным**, если студент при ответе на вопросы не дает определений основных понятий, не способен показать причинно-следственные связи явлений, при решении задачи допускает принципиальные ошибки,
  оценка составляет *_10_ баллов.*
- Ответ на экзаменационный билет засчитывается на **пороговом** уровне, если студент при ответе на вопросы дает определение основных понятий, может показать причинно-следственные связи явлений, при решении задачи допускает непринципиальные ошибки, например, вычислительные,
  оценка составляет *__20_ баллов.*
- Ответ на экзаменационный билет (тест) билет засчитывается на **базовом** уровне, если

студент при ответе на вопросы формулирует основные понятия, законы, дает характеристику процессов, явлений, проводит анализ причин, условий, может представить качественные характеристики процессов, не допускает ошибок при решении задачи,
оценка составляет *_30_ баллов.*

- Ответ на экзаменационный билет засчитывается на **продвинутом** уровне, если студент при ответе на вопросы проводит сравнительный анализ подходов, проводит комплексный анализ, выявляет проблемы, предлагает механизмы решения, способен представить количественные характеристики определенных процессов, приводит конкретные примеры из практики, не допускает ошибок и способен обосновать выбор метода решения задачи,
оценка составляет _40_ *баллов.*

3. Шкала оценки

В общей оценке по дисциплине экзаменационные баллы учитываются в соответствии с правилами балльно-рейтинговой системы, приведенными в рабочей программе дисциплины.

4. **Вопросы и задачи к** экзамену **по дисциплине «**Криптографические методы защиты информации**»**

1	Криптографическая защита информации. Классификация шифров. Требования к средствам криптографической защиты информации.
2	Шифры и шифрование. Основные понятия и определения
3	Шифры перестановки
4	Шифры замены
5	Шифр гаммирования
6	Шифр гаммирования с обратной связью
7	Совершенные, идеально стойкие, абсолютно стойкие шифры
8	Длина ключа и стойкость шифра
9	Фундаментальные ограничения криптографических преобразований
10	Проблемы массового использования шифров. Стандартные схемы и приемы реализации массовых шифров.
11	Стандартные шифры (DES, ГОСТ, AES).
12	Стандарт шифрования DES.
13	Режимы использования шифра DES
14	Стандарт шифрования ГОСТ 28147-89
15	Стандарт шифрования AES
16	Генераторы псевдослучайных чисел в шифровании
17	Основные подходы и методики криптоанализа.
18	Криптоанализ с использованием открытого текста.
19	Криптосистемы с открытым ключем. Принцип Шеннона. Основные особенности и характеристики криптосистем с открытым ключем
29	Структура системы секретной связи при использовании симметричных шифров и шифров с открытым ключом
21	Система Диффи-Хелмана
22	Шифр RSA

23	Шифр Эль Гаммаля
24	Гибридные криптосистемы
25	Основные проблемы криптографической защиты и способы их решения
26	Применение шифров для идентификации и аутентификации субъектов и данных. Хэш-функции. Электронно-цифровая подпись. Схемы цифровой подписи.
27	Отечественные стандарт хэш-функции ГОСТ Р 34.11-94
28	Отечественные стандарт шифрования с открытым ключом и электронно-цифровой подписи ГОСТ Р 34.10-94

ЗАДАЧИ К ЭКЗАМЕНУ

1. Зашифровать свою фамилию, имя и отчество, используя шифр простой перестановки.

2. Зашифровать свою фамилию, имя и отчество, используя шифр одиночной перестановки по ключу. В качестве ключа взять свое имя.

3. Зашифровать свою фамилию, имя и отчество, используя метод Полибия.
   В качестве алфавита взять буквы, включенные в ФИО.

4. Зашифровать свою фамилию, имя и отчество, используя шифр Гронсфельда. В качестве ключа использовать свое имя.

5. Зашифровать свою фамилию, имя и отчество, используя шифр Виженера. В качестве алфавита взять буквы, включенные в ФИО, а в качестве ключа использовать свое отчество.

6. Определить длину ключа в каждом из случаев: 0101 0101 0101 0101; 0000 0000 0000 0000; FEFE FEFA FEFE FEFA. Ключи даны в 16-ричной системе.

7. Для метода RSA и $p<20$, $q<20$ сформировать ключи «d» и «e».

8. Зашифровать открытый текст 1101011001101010110101 методом гаммирования, используя ключ 1011101011. Исходная информация и ключ даны в двоичной системе.

9. Зашифровать открытый текст 1101011001101010110101 методом гаммирования с обратной связью, используя ключ 1011101011 и блок размером 4 бита. Исходная информация и ключ даны в двоичной системе.

10. Определить, сколько различных электронных документов можно представить с помощью хэш-значений длиной 16 бит и 32бита.