ŋqdqɏəɎ bɆ dədɆbɎɜə d ɕɔɑbɔɏ Ɉqddɏqɏè

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
«Оренбургский государственный университет»

Кафедра вычислительной техники

А.И. Сердюк, О.Н. Яркова

КРИПТОГРАФИЯ. РАЗРАБОТКА ПРИЛОЖЕНИЙ ДЛЯ ШИФРОВАНИЯ ИНФОРМАЦИИ

Рекомендовано к изданию Редакционно-издательским советом федерального государственного бюджетного образовательного учреждения высшего профессионального образования «Оренбургский государственный университет» в качестве методических указаний для студентов, обучающихся по программам высшего профессионального образования по специальности 090104.65 Комплексная защита объектов информатизации, 230101.65 Вычислительные машины, комплексы, системы и сети, направлению подготовки 090900.62 Информационная безопасность, профиль «Комплексная защита объектов информатизации»

Оренбург
2012

ŋqdqɏəɎ bɆ dədɆbɎɜə d ɕɔɑbɔɏ Ɉqddɏqɏè

УДК 004.056.5:003.26(076.5)
ББК 32.973.2я7+32.811я7
С 32

Рецензент - доктор технических наук, профессор Т.З. Аралбаев

Сердюк, А.И.
С 32 Криптография. Разработка приложений для шифрования информации: методические указания / А.И. Сердюк, О.Н. Яркова; Оренбургский гос. ун-т. – Оренбург: ОГУ, 2012. – 98 с.

Методические указания содержат теоретический материал и задания к лабораторным работам, посвященным разработке компьютерных программ на основе конкретных шифрсистем. В качестве среды программирования использована интегрированная среда Delphi 7.

Методические указания предназначены студентам специальностей 090104.65 Комплексная защита объектов информатизации, 230101.65 Вычислительные машины, комплексы, системы и сети, направлению подготовки 090900.62 Информационная безопасность профиль «Комплексная защита объектов информатизации», изучающим дисциплины «Математические основы криптологии», «Криптографические методы и средства обеспечения информационной безопасности» и родственные дисциплины, а так же для научных работников и инженеров, занятых вопросами создания и внедрения компьютерно управляемых комплексов оборудования.

УДК 004.056.5:003.26(076.5)
ББК 32.973.2я7+32.811я7

© Сердюк А.И., 2012
Яркова О.Н., 2012
© ОГУ, 2012

Содержание

Введение 5
1 Символы и их коды. Системы исчисления 7
1.1 Лабораторная работа Символы и их коды. 7
1.1.1 Дополнительное задание. 9
1.1.2 Контрольные вопросы. 9
1.2 Системы исчисления. 9
1.2.1 Непозиционные и позиционные системы исчисления. 10
1.2.2 Обозначение чисел в нестандартной системе исчисления. 11
1.2.3 Алгоритмы перевода чисел из одной позиционной системы исчисление в другую. 12
1.2.4 Лабораторная работа Системы исчисления. 14
1.2.4.1 Дополнительное задание. 17
1.2.4.2 Контрольные вопросы. 17
1.3 Представление результатов шифрования в бинарном исчислении. 18
1.3.1 Лабораторная работа Разложение и конвертирование текстового сообщения. 19
1.3.1.1 Дополнительное задание. 21
1.3.1.2 Контрольные вопросы. 22
1.4 Частотный анализ символов. 22
1.4.1 Общие сведения. 22
1.4.2 Лабораторная работа Частотный анализ символов. 23
1.4.2.1 Дополнительное задание. 28
1.4.2.2 Контрольные вопросы. 28
2 Классические шифры. 30
2.1 Шифр Цезаря. 30
2.1.1 Лабораторная работа Шифр Цезаря. 30
2.1.2 Дополнительное задание. 32

ŋqdqȺeɎ bɆ dədɆbɎзə d ɕɔɑbɔȺ ɈqddɎqȺè

2.1.3 Контрольные вопросы 32
2.2 Одноалфавитный шифр простой замены. 33
2.3 Процедура криптоанализа шифра простой замены. 34
2.3.1 Лабораторная работа Шифр простой замены. Процедура криптоанализа шифра простой замены. 34
2.3.1.1 Контрольные вопросы 41
2.4 Многоалфавитный шифр. Матрица Вижинера. 42
2.4.1 Общие сведения. 42
2.4.2 Лабораторная работа Шифры многоалфавитной замены. 44
2.4.2.1 Дополнительное задание 48
2.4.2.2 Контрольные вопросы 48
2.5 Шифр перестановки - решетка Кардано. 48
2.5.1 Лабораторная работа Шифр перестановки. 50
2.5.1.1 Дополнительное задание. 54
2.5.1.2 Контрольные вопросы 54
3 Основы шифрования с открытым ключом. 56
3.1 Алгоритм Эратосфена формирования простых чисел 56
3.1.1 Лабораторная работа Простые числа. 56
3.1.1.1 Дополнительные задания. 58
3.1.1.2 Контрольные вопросы 59
3.2 Основы теории чисел. 59
3.2.1 Лабораторная работа Каноническое разложение числа. 62
3.2.1.1 Дополнительные задания. 63
3.2.1.2 Контрольные вопросы. 64
3.3 Модульная арифметика (арифметика вычетов) 64
3.3.1 Сравнения. 64
3.3.2 Лабораторная работа Модульная арифметика. 68
3.3.2.1 Дополнительное задание. 74
3.3.2.2 Контрольные вопросы. 74
3.4 Шифрсистема RSA. 75

ŋqdqȺeɎ bɆ dədɆbɎзə d ɕɔɑbɔȺ ɈqddɎqȺè

ŋqdqɏeɎ bɆ dədɆbɎɜə d ɕɔɑbɔɏ Ɉqddɏqɏè

3.4.2 Лабораторная работа Шифр-система RSA. 80

3.4.2.1 Дополнительное задание. 84

3.4.2.2 Контрольные вопросы 84

3.5 Стойкость системы RSA. Многопользовательский вариант RSA. 84

3.5.1 Лабораторная работа Многопользовательский вариант RSA 87

3.5.1.1 Контрольные вопросы 90

3.6 Цифровая подпись. 91

3.6.1 Общие сведения. 91

3.6.2 Алгоритм цифровой подписи Эль-Гамаля. 91

3.6.3 Лабораторная работа Цифровая подпись Эль-Гамаля. 93

3.6.3.1 Контрольные вопросы 96

Список использованных источников. 97

ŋqdqɏeɎ bɆ dədɆbɎɜə d ɕɔɑbɔɏ Ɉqddɏqɏè