

УДК 681.322
ББК 32.97я7

Кирпичников А. П.

Криптографические методы защиты компьютерной информации : учебное пособие / А. П. Кирпичников, З. М. Хайбуллина; М-во образ. и науки России, Казан. нац. исслед. технол. ун-т. – Казань : Изд-во КНИТУ, 2016. – 100 с.

ISBN 978-5-7882-2052-9

Описаны классические методы симметричного шифрования данных от первых систем шифрования Спарты, Древней Греции и Рима до методов шифрования Вижинера и Вернама. Рассмотрены шифры перестановки, простой и сложной замены. Отдельный раздел посвящен шифрованию методом гаммирования, который является результатом развития метода Вернама и широко используется в настоящее время.

Предназначено для студентов, обучающихся по направлениям 01.03.02 «Прикладная математика и информатика», 02.03.03 «Математическое обеспечение и администрирование информационных систем», 09.03.01 «Информатика и вычислительная техника».

Подготовлено на кафедре интеллектуальных систем и управления информационными ресурсами.

Печатается по решению редакционно-издательского совета Казанского национального исследовательского технологического университета

Рецензенты: д-р техн. наук, проф. *К. Х Гильфанов*
д-р техн. наук, проф. *Л. М. Шарнин*

ISBN 978-5-7882-2052-9 © Кирпичников А. П., Хайбуллина З. М., 2016
© Казанский национальный исследовательский технологический университет, 2016

СОДЕРЖАНИЕ

ВВЕДЕНИЕ	3
1. ОСНОВНЫЕ ПОНЯТИЯ И ОПРЕДЕЛЕНИЯ	6
1.1. Шифры перестановки	11
1.1.1. Шифрующие таблицы	11
1.1.2. Применение магических квадратов	14
1.2. Шифры простой замены	15
1.2.1. Система шифрования Цезаря	16
1.2.2. Аффинная система подстановок Цезаря	20
1.2.3. Система Цезаря с ключевым словом	21
1.2.4. Шифрующие таблицы Трисемуса	23
1.2.5. Биграммный шифр Плейфейра	24
1.2.6. Криптосистема Хилла	26
1.3. Шифры сложной замены	31
1.3.1. Система шифрования Вижинера	32
1.3.2. Шифр «двойной квадрат» Уитстона	35
1.3.3. Одноразовая система шифрования	37
1.3.4. Шифрование методом Вернама	39
1.4. Шифрование методом гаммирования	41
1.4.1. Методы генерации псевдослучайных последовательностей чисел.....	42
2. КОНЦЕПЦИЯ КРИПТОСИСТЕМЫ С ОТКРЫТЫМ КЛЮЧОМ	53
2.1. Однонаправленные функции	55

2.2. Криптосистема шифрования данных RSA.....	57
2.2.1. Процедуры шифрования и расшифрования в криптосистеме RSA.....	60
2.2.2. Безопасность и быстродействие криптосистемы RSA	63
2.3. Схема шифрования Полига-Хеллмана.....	66
2.4. Схема шифрования Эль Гамала	66
2.5. Комбинированный метод шифрования	68
3. ПРОБЛЕМА АУТЕНТИФИКАЦИИ ДАННЫХ И ЭЛЕКТРОННАЯ ПОДПИСЬ	71
3.1. Однонаправленные хэш-функции	73
3.1.1. Однонаправленные хэш-функции на основе симметричных блочных алгоритмов	74
3.1.2. Отечественный стандарт хэш-функции	77
3.2. Алгоритмы электронной цифровой подписи	78
3.2.1. Алгоритм цифровой подписи RSA	78
3.2.2. Алгоритм цифровой подписи Эль Гамала (EGSA)	82
3.2.3. Алгоритм цифровой подписи DSA	85
3.2.4. Отечественный стандарт цифровой подписи	88
3.3.. Цифровые подписи с дополнительными функциональными свойствами	90
3.3.1. Схемы слепой подписи	90
3.3.2. Схемы неоспоримой подписи	92
Литература	97