Введение в теорию итерированных шифров

А.Г. Ростовцев, Е.Б. Маховенко

Содержание

ВВЕДЕНИЕ
ГЛАВА 1. КРИПТОГРАФИЯ И ЗАЩИТА ИНФОРМАЦИИ
1.1. Основные понятия и определения
1.2. Исчисление атак
1.2.1. Алгоритм и исчисление
1.2.2. Множества возможностей нарушителя
Упражнения к главе 1
Литература к главе 1

ГЛАВА 2. ОБЩИЕ СВЕДЕНИЯ ОБ ИТЕРИРОВАННЫХ КРИПТОАЛГОРИТМАХ
2.1. Основные понятия классической криптографии
2.2. Некоторые положения теории секретности Шеннона
2.3. Булевы функции и булевы формулы
2.4. Кольцо многочленов Жегалкина и аффинные подстановки
2.4.1. Разложение на множители в кольце Gn
2.4.2. Симметрические функции кольца Gn
2.4.3. Кольцо дифференциальных операторов кольца Gn
2.4.4. Аффинные булевы функции
2.4.5. Эндоморфизмы кольца Gn
2.4.6. Многочлены Жегалкина как функции на поверхности единичного куба
2.5. Аффинно эквивалентные булевы функции и подстановки
2.6. Задача вскрытия ключа и математические задачи
2.6.1. Задача вскрытия ключа и NP-полные задачи
2.6.2. Задача о выполнимости

2.6.3. Задачи выбора, распознавания, поиска
2.7. Нестандартные вычислительные модели
2.7.1. Молекулярный компьютер
2.7.2. Квантовый компьютер
2.8. Требования к шифрам
2.9. Шифры замены и перестановки
2.9.1. Моноалфавитная замена
2.9.2. Полиалфавитная замена
2.10. Типовые операции, используемые при построении блочных шифров
2.11. Описание итерированных шифров в терминах булевых функций
Упражнения к главе 2
Литература к главе 2

ГЛАВА 3. АЛГЕБРАИЧЕСКИЕ МЕТОДЫ КРИПТОАНАЛИЗА
3.1. Метод обобщения и редукции. Метод гомоморфизмов
3.2. Замкнутые и чистые шифры
3.2.1. Вскрытие ключей замкнутых и чистых шифров
3.2.2. Проверка шифра на замкнутость и чистоту
3.3. Решеточный криптоанализ
3.3.1. Решеточно продолженные булевы функции и решеточные многочлены
3.3.2. Метод криптоанализа
3.4. Метод арифметического продолжения булевых функций
3.5. Анализ шифров с малым порядком нелинейности
3.6. Криптоанализ на основе рационального продолжения многочленов Жегалкина
3.6.1. Теоретические основы
3.6.2. Метод криптоанализа
3.7. Криптоанализ на основе 2-адического продолжения многочленов Жегалкина
3.7.1. Теоретические основы
3.7.2. Метод криптоанализа
3.8. Максимизация числа совпавших разрядов промежуточных текстов
3.9. Анализ с использованием сжимающих гомоморфизмов
3.10. Поиск коллизий хэш-функции
3.11. Компромисс время/память
3.12. Сочетание перебора и вычисления ключа
3.13. Отбраковка классов ключей
3.14. Задачи, к которым сводится задача вскрытия ключа
Упражнения к главе 3
Литература к главе 3

ГЛАВА 4. СТАТИСТИЧЕСКИЕ МЕТОДЫ КРИПТОАНАЛИЗА
4.1. Некоторые определения
4.2. Дифференциальный криптоанализ
4.2.1. Конечные приращения
4.2.2. Метод криптоанализа
4.2.3. Анализ с помощью усеченных дифференциалов
4.2.4. Анализ с помощью дифференциалов высших порядков
4.2.5. Атака "бумеранг"
4.3. Криптоанализ на основе списка ключей и связанных ключей
4.4. Линейный криптоанализ
4.5. Анализ степенных шифров методом сдвига
4.6. Генерация экстремальных подстановок для шифров
4.6.1. Экстремальные подстановки

4.6.2. Булевы функции для экстремальных подстановок
4.6.3. Примеры экстремальных подстановок
Упражнения к главе 4
Литература к главе 4

ГЛАВА 5. ПРИМЕНЕНИЕ ИТЕРИРОВАННЫХ ШИФРОВ И ХЭШ-ФУНКЦИЙ
5.1. Режимы шифрования
5.1.1. Режим простой замены
5.1.2. Режим гаммирования
5.1.3. Режим гаммирования с обратной связью
5.1.4. Режим сцепления блоков. Выработка имитовставки
5.2. Некоторые вопросы применения шифров
5.3. DES
5.4. FEAL
5.5. IDEA
5.6. ГОСТ 28147-89
5.6.1. Стойкость ГОСТ 28147-89
5.6.2.. Стойкость ГОСТ 28147-89 при наличии у нарушителя лабораторных возможностей
5.7. RC5
5.8. Blowfish
5.9. SAFER
5.10. RIJNDAEL (AES)
5.11. MD5
5.12. ГОСТ Р 34.11-94
Упражнения к главе 5
Литература к главе 5

ОТВЕТЫ И УКАЗАНИЯ К УПРАЖНЕНИЯМ

УКАЗАТЕЛЬ