

**Харин Ю. С. Компьютерный практикум по математическим методам защиты информации:** Учеб. пособие / К). С. Харин. С. В. Агиевич. - Мн.: БГУ, 2001. - 190 с.: ил.



**ISBN 985-445-217-4**

Данное учебное пособие является первым отечественным компьютерным практикумом по новому актуальному направлению прикладной математики - математическим методам защиты информации. Содержит свыше 200 заданий по всем основным разделам криптологии, а также модели, методы и алгоритмы, необходимые для выполнения этих заданий в рамках лабораторных занятий на компьютере. Приводится описание оригинального пакета прикладных программ «КриптоЛаборатория», поддерживающего компьютерный практикум.

Для студентов бакалаврского и магистерского уровней, аспирантов, обучающихся по математическим и инженерно-техническим специальностям, слушателей факультетов переподготовки и повышения квалификации, а также для специалистов в области прикладной математики, информатики и электроники, желающих познакомиться с математическими методами защиты информации.

### Оглавление

Предисловие	5
Основные обозначения	9
Глава 1. Статистическое тестирование случайных и псевдослучайных последовательностей	11
1.1. Равномерно распределенная случайная последовательность и ее свойства	11
1.2. Универсальный алгоритм статистического тестирования случайных и псевдослучайных последовательностей	14
1.3. Тест n -серий	19
1.4. Тест интервалов	19
1.5. Обобщенный покер-тест	21
1.6. Тест «собирателя купонов»	23
1.7. Тест перестановок	24
1.8. Тест пересекающихся n-грамм	25
1.9. Тест, основанный на рангах двоичных матриц	27
1.10. Спектральные тесты	29
1.11. Тесты случайного блуждания	33
1.12. Универсальный статистический тест Маурсра	35
1.13. Тесты на основе приращений энтропии	37
1.14. Тест, основанный на алгоритме сжатия Лемпеля - Зива	40
1.15. Тест, основанный на линейной сложности	42
1.16. Тест на основе экстремальной статистики скалярного произведения	44
1.17. Тест на основе экстремальной статистики дельта-произведения	49
Глава 2. Алгоритмы генерации псевдослучайных последовательностей	52
2.1. Классификация алгоритмов генерации	52
2.2. Линейные и мультипликативные конгруэнтные генераторы	54
2.3. Нелинейные конгруэнтные генераторы	56
2.4. Рекуррентны и конечном поле	58
2.5. Последовательности, порождаемые линейными регистрами сдвига с обратной связью ( LFSR )	60
2.6. Генераторы Фибоначчи	62
2.7. Криптостойкие генераторы на основе односторонних функций	63
2.8. Криптостойкие генераторы, основанные на проблемах теории чисел	67
2.9. Методы «улучшения» элементарных псевдослучайных последовательностей	70
2.10. Комбинирование алгоритмов генерации методом Макларсия Марсальи	72
2.11. Комбинирование LFSR -генераторов	73
2.12. Конгруэнтный генератор со случайными параметрами	76
Глава 3. Элементы симметричных криптосистем	78
3.1. Булевы векторы	78
3.2. Подстановки	79
3.3- Булевы функции	82
3.4. iS -блоки и /-"-блоки	83
3.5. Преобразование Уолша - Адамара	85
3.6. Критерий выбора булевых функций	87
3.7. Таблицы разностей	89
3.8.Нелинейность	90

3.9.Строение конечных полей	91
3.10.Перестановочные многочлены	93
Глава 4. Элементы криптосистем с открытым ключом	96
4.1. Арифметика, больших чисел	96
4.2. Кольца вычетов	99
4.3. Модулярная арифметика	100
4.4. Алгоритм Евклида	102
4.5. Квадратичные вычеты	103
4.6. Простые числа	105
4.7. Первообразные корни	108
Глава 5. Блочные криптосистемы	110
5.1. Определению	110
5.2. Блочные-итерационные криптосистемы	112
5.3. Криптосистемы Фейстеля	114
5.4. Режимы криптопреобразования	118
5.5. Криптоанализ «грубой силой»	120
5.6. Групповой криптоанализ	122
5.7. Разностный криптоанализ	124
5.8. Линейный криптоанализ	126
Глава 6. Поточные криптосистемы	129
6.1. Определение	129
6.2. Рекуррентные последовательности	130
6.3. Линейные рекуррентные последовательности	131
6.4. Оценивание параметров и распознавание ЛРП	134
6.5. Линейная сложность	136
6.6. Определение начального состояния ЛРП	137
6.7. Комбинирование последовательностей	139
6.8. Корреляционный криптоанализ	142
Глава 7. Функции хэширования	146
7.1. Определение	146
7.2. Блочнo-итерационные функции хэширования	147
7.3. Использование блочных криптосистем	148
7.4. Атака «дней рождений»	149
7.5. Криптосистемы аутентификации	151
7.6. Функция хэширования СТБ 1176.1-99	152
Глава 8. Криптосистемы с открытым ключом	157
8.1. Односторонние функции с лазейкой	157
8.2. Задача факторизации	159
8.3. Схема RSA	162
8.4. Схема Рабина	165
8.5. Задача дискретного логарифмирования	167
8.6. Схема, Эль-Гамала	169
8.7. Электронная цифровая подпись СТБ 1176.2-99	172
Глава 9. Компьютерный практикум «КриптоЛаборатория»	175
9.1. Общие сведения	175
9.2. Рабочий план «КриптоЛаборатории»	175
9.3. Инструменты «КриптоЛаборатории»	178
9.4. Задания «КриптоЛаборатории»	179
Приложение. Архив дискретных последовательностей	181
Литература	183