

## МАТЕМАТИЧЕСКИЕ ОСНОВЫ КРИПТОЛОГИИ

**Харин Ю. С. и др. Математические основы криптологии:** Учеб. пособие / Ю. С. Харин, В. И. Берник, Г. В. Матвеев. — Мн.: БГУ, 1999. -319 с: ил.

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

Данное пособие является первым отечественным учебным пособием по новому актуальному направлению прикладной математики — математические методы защиты информации.



Изложены математические основы криптографической защиты информации в компьютерных сетях и системах связи. Исследованы математические модели симметричных и несимметричных криптосистем, а также методы их анализа. Описаны методы генерации и тестирования случайных и псевдослучайных последовательностей. Представлены математические подходы к решению проблем аутентификации. Изложены протоколы функционирования сетевых криптосистем.

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

<b>Предисловие</b>	7
Основные обозначения	10
<b>Глава 1. Введение в криптологию</b>	11
Задачи и упражнения к главе 1	18
<b>Глава 2. Арифметические основы</b>	19
2.1 Алгоритм деления с остатком	19
2.2 Наибольший общий делитель	20
2.3 Взаимно простые числа	21
2.4 Наименьшее общее кратное	22
2.5 Простые числа	22
2.6 Сравнения	24
2.7 Классы вычетов	25

2.8	Функция Эйлера	26
2.9	Сравнения первой степени	27
2.10	Система сравнений первой степени	28
2.11	Первообразные корни	29
2.12	Существование первообразных корней	31
2.13	Индексы по модулям $p^k, 2p^k$	32
2.14	Символ Лежандра	33
2.15	Квадратичный закон взаимности	34
2.16	Символ Якоби	35
	Задачи и упражнения к главе 2	37
	<b>Глава 3. Алгебраические основы</b>	41
3.1	Понятие группы	41
3.2.	Подгруппы групп	43
3.3	Циклические группы	45
3.4	Гомоморфизмы групп	47
3.5	Группы подстановок	48
3.6	Действие группы на множестве	51
3.7	Кольца и поля	52
3.8	Подкольца	54
3.9	Гомоморфизмы колец	56
3.10	Евклидовы кольца	57
3.11	Простые и максимальные идеалы	59
3.12	Конечные расширения полей	60
3.13	Поле разложения	63
3.14	Конечные поля	64
3.15	Порядки неприводимых многочленов	65
3.16	Линейные рекуррентные последовательности	66
3.17	Последовательности максимального периода	68
	Задачи и упражнения к главе 3	69
	<b>Глава 4. Вероятностно-статистические модели сообщений и их энтропийные свойства</b>	77
4.1	Источники дискретных сообщений и их вероятностные модели	77
4.2	Функционал энтропии и его свойства	79
4.3	Условная энтропия и ее свойства	83
4.4	Удельная энтропия стационарной символьной последовательности	89
4.5	Энтропийные характеристики марковских последовательностей	95
4.6	Источники непрерывных сообщений и их энтропийные свойства	100
4.7	Оптимизация функционала энтропии на классе вероятностных распределений	111
	Задачи и упражнения к главе 4	116
	<b>Глава 5. Методы теории информации в криптологии</b>	119

5.1 Асимптотические свойства стационарного источника дискретных сообщений	119
5.2 Энтропийная устойчивость случайных символьных последовательностей	125
5.3 Количество информации по Шеннону и его свойства	131
5.4 Шенноновские модели криптосистем	138
5.5 Теоретико-информационные оценки стойкости симметричных криптосистем	144
Задачи и упражнения к главе 5	150
<b>Глава 6. Генерирование случайных и псевдослучайных последовательностей</b>	<b>153</b>
6.1 Принципы генерирования случайных и псевдослучайных последовательностей	153
6.2 Статистические методы тестирования	163
6.3 Классификация методов генерирования псевдослучайных последовательностей	170
6.4 Конгруэнтные генераторы	171
6.5 Генераторы, использующие рекурренту в конечном поле	179
6.6 Генераторы, использующие регистр сдвига	181
6.7 Генераторы Фибоначчи	182
6.8 Составные генераторы	184
Задачи и упражнения к главе 6	188
<b>Глава 7. Математические модели стандартных симметричных криптосистем</b>	<b>193</b>
7.1 Математическая модель криптосистемы DES	194
7.2 Математическая модель криптосистемы IDEA	200
7.3 Математическая модель криптосистемы GOST	204
Задачи и упражнения к главе 7	206
<b>Глава 8. Математические методы криптоанализа</b>	<b>207</b>
8.1 Задачи и принципы криптоанализа	207
8.2 Метод "опробования" и его вычислительная сложность	210
8.3 Методы криптоанализа на основе теории статистических решений	214
8.4 Разностный криптоанализ	227
8.5 Линейный криптоанализ	232
Задачи и упражнения к главе 8	241
<b>Глава 9. Криптосистемы с открытым ключом</b>	<b>243</b>
9.1 Описание RSA -криптосистемы	243
9.2 Возможные атаки на криптосистему RSA	246
9.3 О стойкости RSA против метода повторного шифрования	247
9.4 О поиске секретного ключа $d$ и факторизации модуля $N$	249
9.5 Биты в RSA -криптосистеме	250

9.6 Система Рабина	252
9.7 Рюкзачный метод шифрования	253
9.8 Стойкость рюкзачного шифра	254
<b>9.9 Тесты на простоту и методы факторизации</b>	256
9.10 Разделение секрета	259
Задачи и упражнения к главе 9	261
<b>Глава 10. Электронная цифровая подпись</b>	263
10.1 Обобщённая модель ЭЦП	264
10.2 Схема ЭЦП Рабина	266
10.3 Схема Диффи-Лампорта	267
10.4 Вероятностная схема подписи. Рабина	268
10.5 Стандарт ЭЦП DSS	270
10.6 Схема ЭЦП Эль-Гамала	273
10.7 Арифметические свойства российского стандарта цифровой подписи	274
10.8 Эквивалентность задач фальсификации подписи в DSS схеме Эль-Гамала	2
10.9 ЭЦП и хэш-функции	81
10.10. Алгоритмы генерации простых чисел	283
Задачи и упражнения к главе 10	285
<b>Глава 11. Протоколы управления криптографическими ключами</b>	292
11.1. Протоколы генерации ключей	295
11.2. Протоколы взаимной аутентификации	296
11.3. Протоколы прямого обмена ключами	297
11.4. Протоколы распределения сеансовых ключей с использованием центра распределения ключей	300
<b>Приложение А. Таблицы</b>	301
<b>Приложение Б. Описание ППП "КриптоЛаборатория"</b>	305
<b>Литература</b>	307
	309