

УДК 003.26
ББК 32.81
М66

Митани Масааки, Сато Синъити
М66 Занимательная информатика. Криптография. Манга / Митани Масааки, Сато Синъити (авторы), Хиноки Идэро (худож.); пер. с яп. Клионского А. Б., научн. ред. Д. М. Белявский. – М.: ДМК Пресс, 2019. – 238 с.: ил. – (Серия «Образовательная манга»). – Доп. тит. л. яп.

ISBN 978-5-97060-603-2

Из музея искусств один за другим дерзко крадут ценные произведения, а преступник каждый раз оставляет зашифрованные сообщения. Проницательный инспектор Мэгуро, его сестра – математик Рика, – и эрудированная журналистка Ёнэда Рио бросают вызов дерзкому похитителю, но для этого им требуется разгадать загадку шифра. Книга познакомит читателя с общими понятиями криптологии и лежащими в её основе интересными математическими закономерностями, а также с тем, как криптография используется в нашей повседневной жизни.

УДК 003.26
ББК 32.81

Original Japanese edition
Manga de waku Ango (The Manga Guide to Cryptology)
By Mitani Masaaki and Sato Shinichi (Authors), Hinoki Idero (Illustrator) and
Verte Corp. (Producer)
Japan language edition copyright © 2007 by Verte Corp. and Mitani Masaaki
Russian language edition copyright © 2019 by ДМК Пресс

Все права защищены. Никакая часть этого издания не может быть воспроизведена в любой форме или любыми средствами, электронными или механическими, включая фотографирование, ксерокопирование или иные средства копирования или сохранения информации, без письменного разрешения издательства.

СОДЕРЖАНИЕ

ПРОЛОГ	1
--------------	---

Глава 1

ОСНОВЫ КРИПТОГРАФИИ	15
---------------------------	----

1-1 Основные понятия криптографии	16
---	----

• Термины криптографии	20
------------------------------	----

• Связь между ключами E_k и D_k	21
---	----

1-2 Классические шифры	24
------------------------------	----

• Шифр Цезаря	24
---------------------	----

• Шифр одноалфавитной замены	25
------------------------------------	----

• Шифр многоалфавитной замены (шифр Виженера).....	26
--	----

• Шифр перестановки	27
---------------------------	----

1-3 Стойкость шифра	28
---------------------------	----

• Число ключей шифра многоалфавитной замены.....	32
--	----

• Число ключей шифра перестановки	32
---	----

• Возможность криптоанализа	35
-----------------------------------	----

• Совершенно стойкий шифр.....	35
--------------------------------	----

• Типы криптостойкости	37
------------------------------	----

Глава 2

ОДНОКЛЮЧЕВОЙ ШИФР	45
-------------------------	----

2-1 Двоичные числа и сложение по модулю 2	46
---	----

2-2 Что такое одноключевой шифр?	57
--	----

• Особенности одноключевого шифра	62
---	----

2-3 Устройство потокового шифра	63
---------------------------------------	----

2-4 Устройство блочного шифра	66
-------------------------------------	----

• Режим сцепления блоков шифртекста (CBC)	69
---	----

2-5 Устройство шифра DES	70
--------------------------------	----

• Основы строения сети Фейстеля.....	71
--------------------------------------	----

• Инволюция.....	72
------------------	----

• Генерирование ключей шифрования DES	75
• Устройство нелинейной функции f шифра DES	76
• Обобщённая модель шифрования и расшифрования DES	77
2-6 Шифры 3-DES и AES	78
• Общие сведения о шифре AES	83
Пример использования упрощённого DES	87
• Преобразование в двоичные данные	87
• Генерирование шифртекста DES	87
• Расшифрование шифртекста DES	95
• Генерирование ключей шифрования DES	100
• Генерирование ключей расшифрования DES	104

Глава 3

ШИФР С ОТКРЫТЫМ КЛЮЧОМ

3-1 Основы шифра с открытым ключом	108
• Основные разновидности шифра с открытым ключом	117
• Односторонние функции	118
• Рождение шифра RSA	121
3-2 Простые числа и факторизация	122
• Тест на простоту	131
3-3 Модульная арифметика	136
• Сложение по модулю и вычитание по модулю	139
• Умножение по модулю и деление по модулю	148
3-4 Малая теорема Ферма и теорема Эйлера	154
• Ферма - отец теории чисел	155
• Тест Ферма и псевдопростые числа	157
• Теорема Эйлера	158
• Математик Эйлер	159
• Функция Эйлера от произведения двух простых чисел	160
3-5 Устройство шифра RSA	163
• Шифрование и расшифрование RSA	165
• Метод генерирования ключей RSA	167

• Генерирование открытого и секретного ключей А.....	169
• Генерирование шифртекста RSA	171
• Расшифрование RSA	173
3-6 Шифр с открытым ключом и задача дискретного логарифмирования.....	175
• Задача дискретного логарифмирования	176
• Шифрование и расшифрование Эль-Гамала.....	178
Расширенный алгоритм Евклида	183

Глава 4

КАК ИСПОЛЬЗУЮТ ШИФР НА ПРАКТИКЕ?..... 187

4-1 Гибридные криптосистемы	188
4-2 Хеш-функция и код аутентификации сообщения	192
• Подмена данных	192
• Защита от подмены.....	194
• Хеш-функция	195
• Спуфинг.....	196
• Защита от спуфинга.....	197
• Устройство имитовставки.....	198
• Отказ.....	199
• Два недостатка имитовставки	201
4-3 Цифровая подпись	202
• Защита от отказа.....	202
• Устройство цифровой подписи	203
• Атака посредника.....	205
• Защита от атаки посредника	206
• Сертификат и удостоверяющий центр	206
4-4 Инфраструктура открытых ключей (ИОК).....	208
Доказательство с нулевым разглашением	219
Разъяснение некоторых терминов	225
Список использованной литературы	227
Предметный указатель	228