

Бабенко, Л. К.

Криптографическая защита информации: симметричное шифрование: учеб. пособие для вузов / Л. К. Бабенко, Е. А. Ищукова. — М.: Издательство Юрайт, 2017. — 220 с. — Серия : Университеты России.

Содержание

Введение.....	8
1. Основные операции, используемые в современных криптографических системах.....	13
2. Основные схемы построения симметричных алгоритмов шифрования.....	23
3. Стандарты шифрования данных.....	26
3.1. Бывший стандарт шифрования данных США - DES.....	26
3.2. Стандарт шифрования ГОСТ 28147-89.....	36
3.3. Стандарт AES.....	46
3.4. Проект нового стандарта шифрования данных ГОСТ - алгоритм «Кузнечик».....	59
4. Учебные алгоритмы шифрования.....	73
4.1. Учебный алгоритм шифрования УАШ.....	73
4.1.1. Предпосылки создания.....	73
4.1.2. Общий вид учебного алгоритма шифрования.....	73
4.1.3. Функция F	75
4.1.4. Использование раундовых подключей.....	78
4.1.5. Использование одного и того же алгоритма для шифрования и расшифрования данных.....	79
4.1.6. Пример шифрования данных с использованием УАШ.....	84
4.2. Упрощенный алгоритм шифрования DES (S-DES).....	92
4.2.1. Вычисление ключей S-DES.....	93
4.2.2. Шифрование S-DES.....	95
4.2.3. Пример шифрования данных с использованием алгоритма S-DES.....	98
4.3. Алгоритм шифрования SAES.....	105
4.3.1. Математическое обоснование алгоритма.....	105
4.3.2. Описание алгоритма SAES.....	106
4.3.3. Алгоритм выработки подключей.....	119
4.3.4. Пример преобразования данных с помощью алгоритма SAES.....	119
5. Режимы шифрования для симметричных блочных шифров.....	123

5.1. Основные режимы работы блочных шифров.	123
5.1.1. Режим электронной кодовой книги (<i>Electronic codebook, ECB</i>).	123
5.1.2. Режим сцепления блоков (<i>Cipher block chaining, CBC</i>)	126
5.1.3. Режим обратной связи по выходу (<i>Output-Feedback, OFB</i>)	128
5.1.4. Режим обратной связи по шифру (<i>Cipher-Feedback, CFB</i>)	130
5.2. Специальные режимы работы алгоритма DES.	131
5.2.1. Двойной DES.	131
5.2.2. Тройной DES с двумя ключами.	133
5.3. Специальные режимы для нового стандарта шифрования ГОСТ.	135
5.3.1. Вспомогательные операции.	136
5.3.2. Режим простой замены (<i>ECB - ГОСТ</i>).	138
5.3.3. Режим гаммирования (<i>CTR - ГОСТ</i>).	140
5.3.4. Режим гаммирования с обратной связью по выходу (<i>OFB - ГОСТ</i>).	142
5.3.5. Режим простой замены с зацеплением (<i>CBC - ГОСТ</i>).	145
5.3.6. Режим гаммирования с обратной связью по шифр-тексту (<i>CFB - ГОСТ</i>).	147
5.3.7. Режим выработки имитовставки (<i>MAC - ГОСТ</i>).	150
6. Поточные шифры.	154
6.1. Регистры сдвига с обратной линейной связью.	156
6.2. Алгоритм A5/1.	159
6.3. Усеченная модель алгоритма A5/U.	164
7. Малоресурсная криптография.	167
7.1. Алгоритм шифрования CLEFIA.	168
7.2. Алгоритм шифрования Present.	172
7.3. Алгоритм шифрования Trivium.	174
8. Анализ симметричных алгоритмов шифрования.	177
8.1. Метод полного перебора.	180
8.2. Метод встречи посередине.	183
8.3. Линейный криптоанализ.	183

8.4. Дифференциальный криптоанализ.....	188
8.5. Алгебраический анализ.....	193
8.6. Анализ стандарта AES.....	196
8.7. Слайдовая атака.....	199
8.8. Парадокс дней рождений и его роль в задачах криптоанализа.....	203
Контрольные вопросы.....	207
Задачи для самостоятельного решения.....	210
Библиографический список.....	219