

А.В. БАБАШ

МОНОГРАФИЯ

ДЕШИФРОВАНИЕ КЛАССИЧЕСКИХ ШИФРОВ

Теоретическая и практическая стойкость шифров

Дешифрование шифров тотальным методом

Дешифрование шифров методом эквивалентных ключей

Дешифрование шифров гаммирования

Дешифрование дисковых шифраторов
на основе развития атаки «человек посередине»

Дешифрование шифрующих автоматов
с помощью их приближенных моделей

KNORUS

BOOK.ru

ЧИТАТЬ ONLINE



А.В. Бабаш

ДЕШИФРОВАНИЕ КЛАССИЧЕСКИХ ШИФРОВ

Монография



КНОРУС • МОСКВА • 2024

УДК 004.056.55
ББК 32+32.811.4
Б12

Рецензенты:

П.Б. Хорев, Национальный исследовательский университет «МЭИ», канд. техн. наук, доц.,

А.М. Чеповский, Российский университет дружбы народов (РУДН), Высшая школа экономики (НИУ ВШЭ), д-р техн. наук, проф.

Автор

А.В. Бабаш, Российский экономический университет имени Г.В. Плеханова

Бабаш, Александр Владимирович.

Б12 Дешифрование классических шифров : монография / А.В. Бабаш. — Москва : КНОРУС, 2024. — 176 с.

ISBN 978-5-406-11995-2

Большинство разделов написаны в автономном стиле. Для изучения материалов необходимо знать простейшие обозначения математики, в частности простейшие вероятностные понятия и обозначения.

Материал монографии сосредоточен на новых методах дешифрования классических шифров: шифр случайного гаммирования и его частный случай — шифр Вернама; шифр Виженера; шифр простой замены; шифр перестановки; шифр Джефферсона; шифр Тук-тук; шифр IA; дисковые шифраторы, блочные шифры как шифры простой замены с большой мощностью алфавита.

Для студентов специалитета и аспирантов, обучающихся по профилю «Защита информации», а также специалистов по защите информации.

Ключевые слова: шифр случайного гаммирования; шифр простой замены; шифр перестановки; шифр Джефферсона; шифр Тук-тук; дисковые шифраторы; блочные шифры.

УДК 004.056.55
ББК 32+32.811.4

Бабаш Александр Владимирович

**ДЕШИФРОВАНИЕ
КЛАССИЧЕСКИХ ШИФРОВ**

Изд. № 678836. Подписано в печать 13.07.2023. Формат 60×90/16.

Гарнитура «Newton». Печать офсетная.

Усл. печ. л. 11,0. Уч.-изд. л. 10,2.

ООО «Издательство «КноРус».

117218, г. Москва, ул. Кедрова, д. 14, корп. 2.

Тел.: +7 (495) 741-46-28.

E-mail: welcome@knorus.ru www.knorus.ru

ISBN 978-5-406-11995-2

© Бабаш А. В., 2024

© ООО «Издательство «КноРус», 2024

Содержание

Введение	4
Глава 1. Теоретическая и практическая стойкость шифров	8
1.1. О теоретической стойкости шифров	8
1.2. О практической стойкости шифров	9
Глава 2. Дешифрование шифров тотальным методом	12
2.1. Упрощенный тотальный метод	12
2.2. Полный тотальный метод дешифрования шифров	13
2.3. Опробование в тотальном методе	14
2.4. Расчет трудоемкости тотального метода	16
2.5. Частные случаи расчета трудоемкости тотального метода	18
2.6. Расчет надежности тотального метода	20
Глава 3. Дешифрование шифров методом эквивалентных ключей	22
Глава 4. Дешифрование шифров гаммирования	28
4.1. О дешифровании шифра Виженера как частной модификации шифра случайного гаммирования	28
4.2. Методы дешифрования шифра Виженера. Краткий путеводитель	33
Глава 5. О границах зашумления текстов при сохранении их содержания	34
5.1. Первый подход к границам зашумления текстов [6]	34
5.2. Второй подход к границам зашумления текстов [9]	43
Глава 6. Дешифрование шифра случайного гаммирования методами d-слабых ключей Виженера	56
6.1. Утверждения о недешифруемости шифра случайного гаммирования (ШСГ). В разделе использованы материалы работ [5, 6, 74, 76, 80]	57
6.2. d-слабые ключи шифра случайного гаммирования. Используем введенные ранее обозначения для ШСГ	60
6.3. Критерии определения d-слабого ключа ШСГ	62
6.4. Атаки на шифр случайного гаммирования с помощью d-слабых ключей Виженера	65
Глава 7. Что же понимать под дешифруемостью и недешифруемостью ШСГ	73
Глава 8. Дешифрование шифра случайного гаммирования методом Монте-Карло и методом Q-слабых ключей	78
Глава 9. О шифрах RC4, IA, IBAA	89
9.1. О периодичности функционирования генераторов псевдослучайных чисел RC4, IA, IBAA	89
9.2. Метод дешифрования шифра IA [100]	91
Глава 10. Дешифрование шифра Тук-тук	97
Глава 11. Дешифрование шифра Джефферсона	101
Глава 12. Дешифрование шифра простой замены	105
Глава 13. Дешифрование шифра перестановки	116
Глава 14. Дешифрование дисковых шифраторов на основе развития атаки «человек посредине»	124
Глава 15. Определение ключей блочных шифров, построенных на идее Фейстеля дифференциальным методом	134
Глава 16. Дешифрование шифрующих автоматов с помощью их приближенных моделей	150
Литература	154