

# ОГЛАВЛЕНИЕ

<b>Предисловие</b> . . . . .	8
<b>Введение</b> . . . . .	10
<b>Глава 1. Устройство шифра RSA</b> . . . . .	13
<b>Глава 2. Разложение числа на простые множители</b> . . . . .	17
2.1. «Наивный» метод . . . . .	17
2.2. Метод факторных баз . . . . .	19
2.3. Оценка сложности метода факторных баз . . . . .	24
2.4. Свойства линейных систем . . . . .	30
<b>Глава 3. Метод Монтгомери</b> . . . . .	34
3.1. Еще раз о задаче и не только . . . . .	34
3.2. Метод Ланцоша. От вещественных чисел к конечным полям . . . . .	36
3.3. Блочный метод Монтгомери над $\mathbb{F}_2$ . . . . .	44
3.4. Простая параллельная реализация метода Монтгомери . . . . .	50
3.5. Немного о матрицах и аппаратном кэше . . . . .	61
3.6. Совершенствуем параллельный код . . . . .	69
3.7. Как улучшить умножение матрицы на блок? . . . . .	79
3.8. Метод «четырех русских» . . . . .	88
<b>Глава 4. Метод Видемана – Копперсмита</b> . . . . .	93
4.1. Идея Видемана . . . . .	95
4.2. Алгоритм Видемана – Копперсмита. Снова блоки . . . . .	98
4.3. Пишем параллельную реализацию . . . . .	110
<b>Вместо заключения</b> . . . . .	121
<b>Список литературы</b> . . . . .	126