

УДК 004.4
ББК 32.97
Г93

Йо Ван Гуй

Г93 Программирование на ассемблере x64 для начинающих / пер. с англ. А. В. Снастина. – М.: ДМК Пресс, 2021. – 332 с.: ил.

ISBN 978-5-97060-929-3

Цель этой книги – показать, как используются инструкции языка ассемблера, и научить читателей программировать на нем – начиная с создания самых простых программ и заканчивая использованием расширенной системы команд Advanced Vector Extensions (AVX). Для изучения практической части потребуются знания основы программирования на каком-либо языке высокого уровня, например С.

Теоретический материал сведен к необходимому минимуму: немного информации о двоичных числах, краткое описание логических операторов и кое-что об основах линейной алгебры. Исходный ассемблерный код представлен в виде завершенных программ, которые читатель может протестировать на своем компьютере и поэкспериментировать с ними. Рассматриваются инструментальные средства, которыми можно воспользоваться, и потенциальные проблемы при использовании этих инструментов.

Основная часть книги содержит информацию о применении ассемблера в ОС Linux; несколько заключительных глав описывают работу в Windows.

Книга предназначена для программистов на языках высокого уровня, а также для системных инженеров и инженеров по обеспечению безопасности, работающих в области исследования вредоносного программного обеспечения.

УДК 004.4
ББК 32.97

First published in English under the title Beginning x64 Assembly Programming; From Novice to AVX Professional by Jo Van Hoey, edition: 1

Copyright © Jo Van Hoey, 2019 *

This edition has been translated and published under licence from APress Media, LLC, part of Springer Nature. APress Media, LLC, part of Springer Nature takes no responsibility and shall not be made liable for the accuracy of the translation.

Все права защищены. Любая часть этой книги не может быть воспроизведена в какой бы то ни было форме и какими бы то ни было средствами без письменного разрешения владельцев авторских прав.

ISBN (англ.) 978-1-4842-5075-4
ISBN (рус.) 978-5-97060-929-3

© 2019 by Jo Van Hoey
© Оформление, издание, перевод, ДМК Пресс, 2021

Оглавление

| | |
|---|----|
| Об авторе | 12 |
| О техническом рецензенте | 13 |
| Предисловие от издательства | 14 |
| Введение | 15 |
| Прежде чем начать | 17 |
| Глава 1. Самая первая программа | 19 |
| Редактирование, ассемблирование, связывание и запуск (или отладка)..... | 20 |
| Структура программы на ассемблере | 25 |
| Раздел section .data | 25 |
| Раздел section .bss..... | 26 |
| Раздел section .txt..... | 27 |
| Резюме..... | 29 |
| Глава 2. Двоичные и шестнадцатеричные числа и регистры | 30 |
| Краткий вводный курс по двоичным числам..... | 30 |
| Целые числа | 31 |
| Числа с плавающей точкой | 32 |
| Краткий вводный курс по регистрам..... | 32 |
| Регистры общего назначения | 33 |
| Регистр счетчика команд (rip) | 34 |
| Регистр флагов | 34 |
| Регистры xmm и ymm | 35 |
| Резюме..... | 35 |
| Глава 3. Анализ программ с помощью отладчика: GDB | 36 |
| Начало отладки | 36 |
| Двигаемся дальше | 42 |
| Некоторые дополнительные команды отладчика GDB | 44 |
| Немного улучшенная версия программы hello, world | 45 |
| Резюме..... | 47 |

| | |
|--|----|
| Глава 4. Следующая программа: Alive and Kicking | 48 |
| Анализ программы alive | 49 |
| Вывод | 53 |
| Резюме | 56 |
| Глава 5. Ассемблер основан на логике | 57 |
| Логический оператор NOT | 57 |
| Логический оператор OR | 57 |
| Логический оператор XOR | 58 |
| Логический оператор AND | 58 |
| Резюме | 59 |
| Глава 6. Отладчик Data Display Debugger | 60 |
| Работа с отладчиком DDD | 60 |
| Резюме | 63 |
| Глава 7. Переходы и циклы | 64 |
| Установка SimpleASM | 64 |
| Использование SASM | 64 |
| Резюме | 72 |
| Глава 8. Память | 73 |
| Обследование памяти | 73 |
| Резюме | 80 |
| Глава 9. Целочисленная арифметика | 81 |
| Основы использования целочисленной арифметики | 81 |
| Изучение арифметических инструкций | 84 |
| Резюме | 87 |
| Глава 10. Стек | 88 |
| Изучение работы стека | 88 |
| Наблюдение за стеком | 91 |
| Резюме | 93 |
| Глава 11. Арифметика с плавающей точкой | 94 |
| Сравнение чисел с обычной и двойной точностью | 94 |
| Кодирование с применением чисел с плавающей точкой | 96 |
| Резюме | 98 |
| Глава 12. Функции | 99 |
| Создание простой функции | 99 |

| | |
|---|------------|
| Еще о функциях | 100 |
| Резюме..... | 102 |
| Глава 13. Выравнивание стека и фрейм стека | 103 |
| Выравнивание стека..... | 103 |
| Более подробно о фреймах стека | 105 |
| Резюме..... | 106 |
| Глава 14. Внешние функции | 107 |
| Создание и связывание функций..... | 107 |
| Расширенная версия makefile..... | 110 |
| Резюме..... | 111 |
| Глава 15. Соглашения о вызовах функций..... | 112 |
| Аргументы функций..... | 113 |
| Схема стека | 116 |
| Сохранение регистров..... | 118 |
| Резюме..... | 120 |
| Глава 16. Операции с битами | 121 |
| Основные положения..... | 121 |
| Арифметика | 126 |
| Резюме..... | 129 |
| Глава 17. Работа с битами | 130 |
| Другие способы изменения битов..... | 130 |
| Переменная bitflags..... | 132 |
| Резюме..... | 133 |
| Глава 18. Макрокоманды | 134 |
| Создание макроса..... | 134 |
| Использование objdump..... | 136 |
| Резюме..... | 137 |
| Глава 19. Ввод и вывод в консоли | 138 |
| Использование средств ввода/вывода | 138 |
| Обработка переполнений | 140 |
| Резюме..... | 143 |
| Глава 20. Файловый ввод/вывод | 144 |
| Использование системных вызовов..... | 144 |
| Обработка файла | 145 |

| | |
|--|------------|
| Условное ассемблирование | 152 |
| Инструкции для обработки файлов..... | 152 |
| Резюме..... | 153 |
| Глава 21. Командная строка | 154 |
| Доступ к аргументам командной строки..... | 154 |
| Отладка программы с аргументами командной строки | 155 |
| Резюме..... | 157 |
| Глава 22. Использование ассемблера в коде С..... | 158 |
| Создание файла исходного кода на языке С..... | 158 |
| Создание файла исходного кода на ассемблере | 160 |
| Резюме..... | 163 |
| Глава 23. Встроенный ассемблер..... | 164 |
| Простой встроенный ассемблерный код | 164 |
| Расширенный встроенный ассемблерный код..... | 166 |
| Резюме..... | 169 |
| Глава 24. Строки | 170 |
| Обработка строк | 170 |
| Сравнение и сканирование строк | 174 |
| Резюме..... | 178 |
| Глава 25. Предъявите ваш идентификатор | 179 |
| Использование инструкции <code>cuid</code> | 179 |
| Использование инструкции <code>test</code> | 181 |
| Резюме..... | 183 |
| Глава 26. SIMD..... | 184 |
| Скалярные данные и упакованные данные..... | 184 |
| Невыровненные и выровненные данные | 186 |
| Резюме..... | 187 |
| Глава 27. Работа с битами регистра <code>mxcsr</code> | 189 |
| Анализ программы..... | 194 |
| Резюме..... | 196 |
| Глава 28. Выравнивание для SSE..... | 197 |
| Пример без выравнивания | 197 |
| Пример с выравниванием..... | 200 |
| Резюме..... | 203 |

| | |
|--|-----|
| Глава 29. SSE-инструкции для работы с упакованными целыми числами | 204 |
| SSE-инструкции для работы с целыми числами | 204 |
| Анализ исходного кода | 206 |
| Резюме | 206 |
| Глава 30. Обработка строк средствами SSE | 207 |
| Управляющий байт <code>imm8</code> | 208 |
| Использование управляющего байта <code>imm8</code> | 209 |
| Биты 0 и 1 | 209 |
| Биты 2 и 3 | 209 |
| Биты 4 и 5 | 210 |
| Бит 6 | 211 |
| Зарезервированный бит 7 | 211 |
| Флаги | 211 |
| Резюме | 212 |
| Глава 31. Поиск символа в строке | 213 |
| Определение длины строки | 213 |
| Поиск в строках | 216 |
| Резюме | 219 |
| Глава 32. Сравнение строк | 220 |
| Строки с неявно заданной длиной | 220 |
| Строки с явно заданной длиной | 222 |
| Резюме | 226 |
| Глава 33. Перемешиваем данные | 227 |
| Основные принципы операций перемешивания | 227 |
| Перемешивание в случайном порядке | 231 |
| Перемешивание в обратном порядке | 233 |
| Перемешивание вращением | 234 |
| Перемешивание байтов | 234 |
| Резюме | 236 |
| Глава 34. SSE-инструкции: маски строк | 237 |
| Поиск символов | 237 |
| Поиск символов из заданного диапазона | 243 |
| Поиск подстроки | 246 |
| Резюме | 249 |

| | |
|--|-----|
| Глава 35. AVX | 250 |
| Проверка поддержки AVX | 250 |
| Пример программы с использованием AVX | 252 |
| Резюме | 256 |
| Глава 36. Операции с матрицами с использованием AVX | 257 |
| Пример исходного кода для операций с матрицами | 257 |
| Вывод матрицы: <code>printm4x4</code> | 264 |
| Умножение матриц: <code>multi4x4</code> | 265 |
| Обращение матрицы: <code>inverse4x4</code> | 268 |
| Теорема Гамильтона–Кэли | 268 |
| Алгоритм Фаддеева–Леве́рье | 268 |
| Исходный код | 269 |
| Резюме | 273 |
| Глава 37. Транспонирование матриц | 274 |
| Пример исходного кода для транспонирования матриц | 274 |
| Версия с использованием неупакованных данных | 277 |
| Версия с применением перемешивания | 282 |
| Резюме | 285 |
| Глава 38. Оптимизация производительности | 286 |
| Производительность вычисления транспонированной матрицы | 286 |
| Производительность вычисления следа матрицы | 292 |
| Резюме | 297 |
| Глава 39. Приветствуем мир Windows | 298 |
| Начинаем изучение | 298 |
| Пишем код в Windows | 300 |
| Отладка | 302 |
| Системные вызовы | 302 |
| Резюме | 303 |
| Глава 40. Использование Windows API | 304 |
| Вывод в консоли | 304 |
| Создание окон Windows | 307 |
| Резюме | 308 |
| Глава 41. Функции в Windows | 309 |
| Использование более четырех аргументов функции | 309 |
| Обработка значений с плавающей точкой | 314 |
| Резюме | 316 |

| | |
|---|------------|
| Глава 42. Функции с переменным числом аргументов | 317 |
| Функции с переменным числом аргументов в Windows | 317 |
| Обработка смешанных значений | 319 |
| Резюме..... | 320 |
| Глава 43. Работа с файлами в Windows..... | 321 |
| Резюме..... | 324 |
| Послесловие. Что дальше? | 325 |
| Предметный указатель | 326 |