Introdução à Programação em Baixo Nível [REVISÃO]

Engenharia de Computação
UFC QUIXADÁ

Programa em C

```
#include <stdio.h>
int main(void)  {
    int a = 5;
    int b = 7;
    int c;
    c = a + b;
    return 0;
  }
```

Em NASM

```
%include "io.inc"

section .data
a dd 5
b dd 7

section .bss
c resd 1

section .text
global CMAIN
CMAIN:
        mov EAX, [a]
        add EAX, [b]
        mov [c], EAX
        xor eax, eax
        ret
```

Programação em Assembly

Instruções Manipulam:

- Unidade Lógico Aritmética (ULA)
- Unidade de Controle (UC)
- Interrupções
  - Vetor de Interrupção
    - Chamadas de Sistema
    - Memória Externa
- Co-processadores Intel de ponto flutuante (x87)
- Conjunto estendido de instruções vetoriais (SSE, MMX, AVX, . . .)

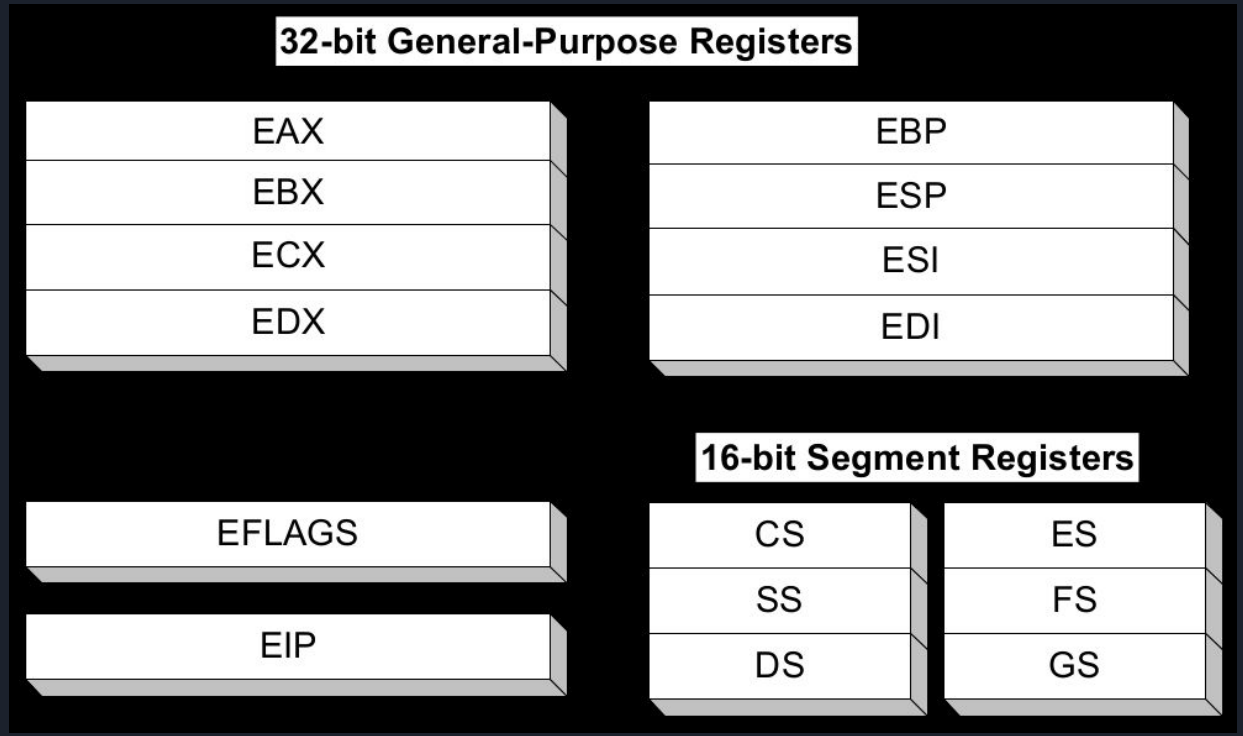
Armazenando Dados

Locais de Armazenamento durante a execução de um programa

- Memória Externa
- Memória Interna
- Registradores
  - Implícitos
  - Explícitos

Registradores x86

Registradores Explícitos de Propósito Geral



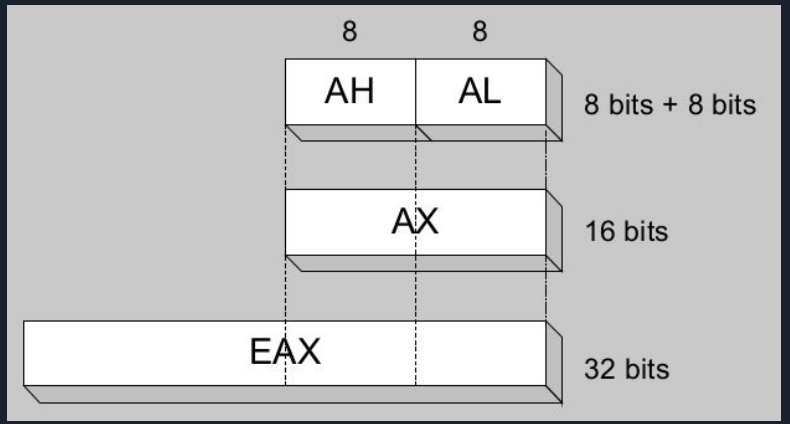
Entendendo o OFFSET

Considere o segmento DS (Segmento de Dados)

```
section .data
a dd 5
b dd 7
c dd 3
d dd 8
```

Acessando Partes de Registradores

- Usando nome de 8-bit, nome de 16-bit, ou nome de 32-bit
- Aplicáveis a EAX, EBX, ECX e EDX



32-bit	16-bit	8-bit (high)	8-bit (low)
EAX	AX	AH	AL
EBX	BX	BH	BL
ECX	CX	CH	CL
EDX	DX	DH	DL

Registradores de Índice e Base

- Alguns registradores possuem somente nome de 16-bit para sua metade menor

32-bit	16-bit
ESI	SI
EDI	DI
EBP	BP
ESP	SP

Registradores de Uso Especializado

- **Propósito Geral**
  - EAX - acumulador (accumulator)
  - ECX - contador de laço (loop counter)
  - ESP - ponteiro de pilha (stack pointer)
  - ESI, EDI - registrador de índice (index registers)
  - EBP - ponteiro de frame estendido (extended frame pointer-stack)
- **Segmento**
  - CS - segmento de código (code segment)
  - DS - segmento de dados (data segment)
  - SS - segmento de pilha (stack segment)
  - ES, FS, GS - segmento adicional (additional segments)
- EIP - ponteiro de instrução (instruction pointer)
- EFLAGS
  - Flags de status e controle
  - cada flag é um único bit binário

Flags de Status

- Carry
  - operação aritmética sem sinal fora de faixa (out of range)
- Overflow
  - operação aritmética com sinal fora de faixa (out of range)
- Sign
  - o resultado é negativo
- Zero
  - o resultado é zero
- Auxiliary Carry
  - carry do bit 3 ao bit 4
- Parity
  - soma de 1 bit e um número par

Registradores de ponto flutuante, MMX, XMM

- Oito registradores de dados ponto flutuante de 80-bit na unidade de ponto flutuante (Float Point Unit- FPU)
  - ST(0), ST(1), . . . , ST(7)
  - arranjados em uma pilha
  - usado por todos operações aritméticas de ponto flutuante
- Oito registradores 64-bit MMX
  - Utiliza os mesmos registradores da FPU
- Oito registradores 128-bit XMM para operações SIMD (single instruction multiple data)
  - XMM0, XMM1, . . . , XMM7
- O AVX utiliza dezesseis registradores YMM de 256bits
  - YMM0, YMM1, . . . , YMM15