دوره مهندسی معکوس نرم افزار

- Site: OnHexGroup.ir
- Youtube: @onhexgroup
- Telegram: onhex_ir
- Twitter: @onhexgroup
- Github: onhexgroup

نسخه ی ۳۲ و ۶۴ بیتی

پلتفرم: ویندوز

ارائه دهنده : **OnhexGroup**

Onhexgroup.ir

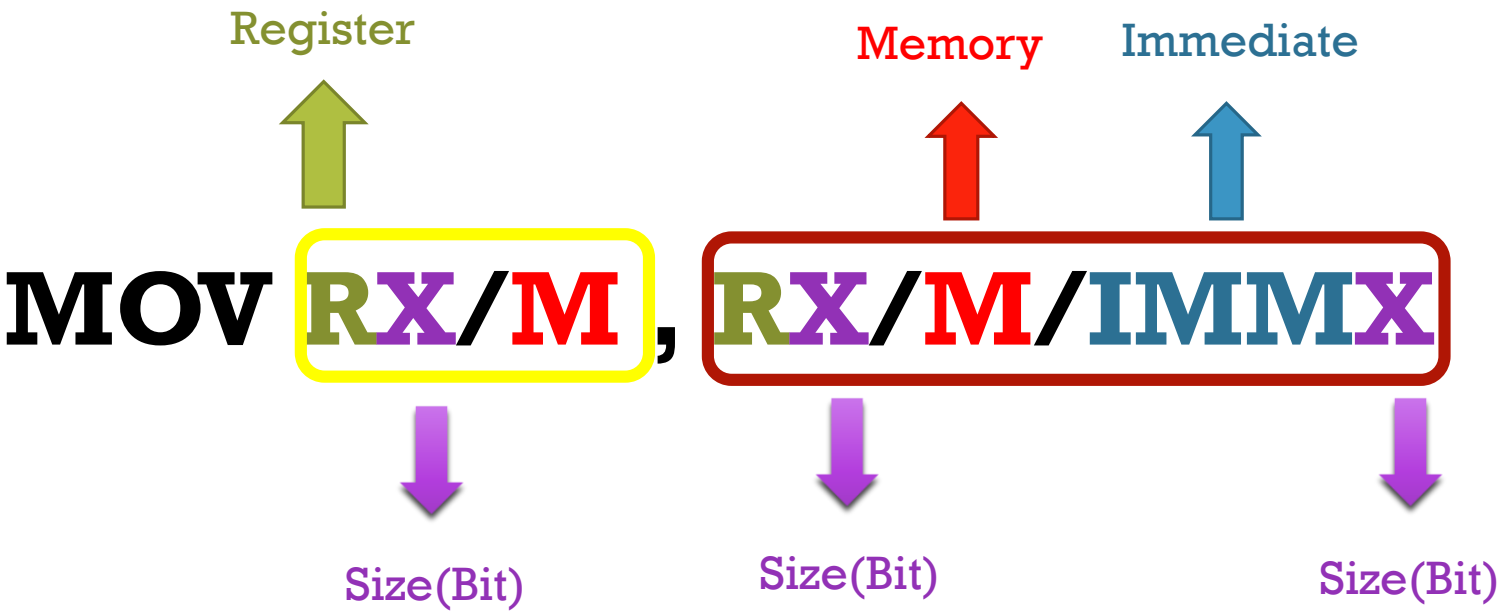
دستور MOV

- برای انتقال اطلاعات از مبدا به مقصد استفاده میشه
- اطلاعات در حقیقت کپی میشه
- روی فلگها تاثیر نمیزاره.

MOV Dest, Source

Telegram: onhex_ir

دستور MOV



Youtube: onhexgroup

شکل دستور MOV

MOV RX/M, RX/M/IMMX

MOV al,11h

R8= al,ah,bl,...

R16= ax,bx,...

R32= eax,ebx,....

R64=rax,rbx,...

IMM8, IMM16, IMM32, IMM64

Github: onhexgroup

شکل دستور MOV

MOV RX/M, RX/M/IMMX

MOV al,bl

R8= al,ah,bl,...

R16= ax,bx,...

R32= eax,ebx,....

R64=rax,rbx,...

Twitter: onhexgroup

شکل دستور MOV

MOV RX/M, RX/M/IMMX

MOV [eax],11h

IMM8, IMM16,...

Onhexgroup.ir

شکل دستور MOV

MOV RX/M, RX/M/IMMX

MOV rax,[rbx]

R8= al,ah,bl,...

R16= ax,bx,...

R32= eax,ebx,....

R64=rax,rbx,...

Onhexgroup.ir

شکل دستور MOV

MOV RX/M, RX/M/IMMX

MOV [rax],rbx

R8= al,ah,bl,...

R16= ax,bx,...

R32= eax,ebx,....

R64=rax,rbx,...

Youtube: onhexgroup

نکات مهم MOV

- با این دستور نمیتوانیم یک حافظه را به حافظه دیگه منتقل کنیم.

✖ **MOV M,M**

- مقصد هرگز نمیتواند یک عدد صریح باشد.

✖ **MOV imm,r/m/imm**

- مقصد نمیتواند رجیستر اشاره گر آدرس باشد

✖ **MOV RIP/EIP,r/m/imm**

Github: onhexgroup

نکات مهم MOV

- مقدار صریح اگه با حروف شروع بشه باید اولش ۰ بزاریم:

✘ **MOV r/m,ah**

✓ **MOV r/m,0ah**

- سایز مقصد باید برابر یا بزرگتر از مبدا باشد.

MOV r/m,r/m/imm

Twitter: onhexgroup

نکات مهم MOV

- نمیتونیم یک مقدار صریح رو در رجیسترهای سگمنت بریزیم

✗ **MOV CS,11h**

- اندازه مقصد و مبدا یکسان است. بایت به بایت، کلمه به کلمه و ..

✗ **MOV ax, bl**

✗ **MOV ax, [x] (x=1 byte)**

✓ **MOV rax,11h**

✓ **MOV rax,[rbx]**

✓ **MOV [rax],1122h**

Youtube: onhexgroup

دستور Lea

- همانند دستور **MOV** برای انتقال داده است، اما آدرس را انتقال میدهد.

Lea Dest, Source

Site: onhexgroup.ir

دستور Lea

Lea RX, M

R16= ax,bx,...

R32= eax,ebx,....

R64=rax,rbx,...

Telegram: onhex_ir

نکات دستور Lea

- دستور زیر مجاز نیست:

lea [mybyte],[rcx]

- دستور **Lea** سایز کمتری نسبت به **Mov** داره.
- دستور زیر معادل هستن (طبق شرایطی):

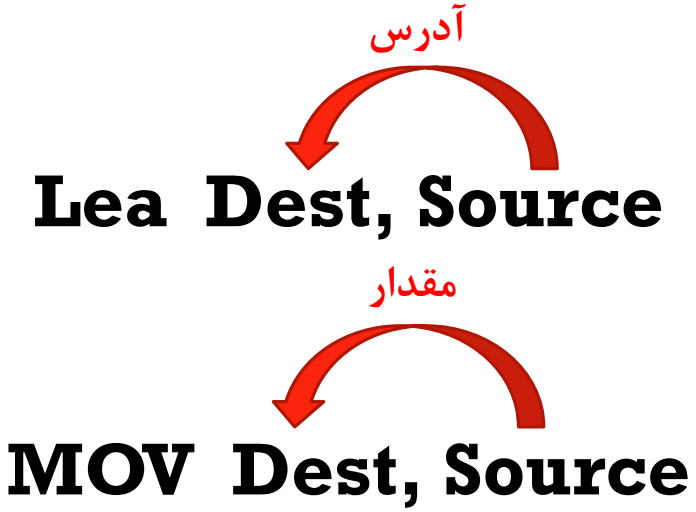
lea rax,[mybyte]

mov rbx,offset[mybyte]

Site: onhexgroup.ir

نکات طلایی برای LEA,Mov

- در کل باید مفهوم انتقال رو بدونیم:



Github: onhexgroup

درصد