

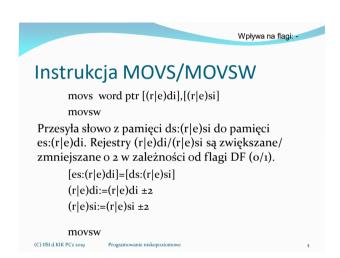
Operacje na łańcuchach

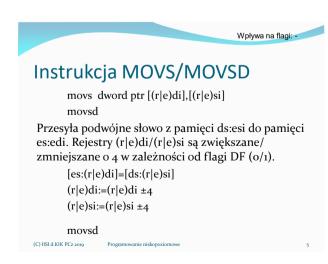
- MOVS/MOVSB/MOVSW/MOVSD/MOVSQ Prześlij łańcuch/bajtów/słów/podwójnych słów/poczwórnych słów
- CMPS/CMPSB/CMPSW/CMPSD/CMPSQ Porównaj łańcuchy/bajtów/słów/podwójnych słów/poczwórnych słów
- SCAS/SCASB/SCASW/SCASD/SCASQ Skanuj łańcuch/bajtów/słów/podwójnych słów/poczwórnych słów
- LODS/LODSB/LODSW/LODSD/LODSQ Ładuj łańcuch/bajtów/słów/podwójnych słów/poczwórnych słów
- STOS/STOSB/STOSW/STOSD/STOSQ Zapamiętaj
- łańcuch/bajtów/słów/podwójnych słów/poczwórnych słów
 REP Powtarzaj dopóki ECX nie jest zerem
- REPE/REPZ Powtarzaj dopóki equal/zero
- KEI E/ KEI E I Owtai zaj dopoki equal/zero
- REPNE/REPNZ Powtarzaj dopóki not equal/not zero

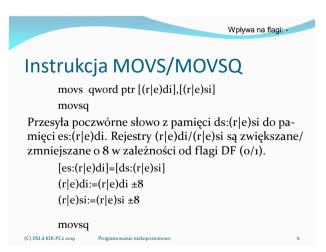
(C) IISI d.KIK PCz 2019

rogramowanie niskopoziomow

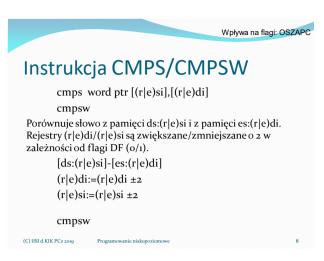
Instrukcja MOVS/MOVSB movs byte ptr [(r|e)di],[(r|e)si] movsb Przesyła bajt z pamięci ds:(r|e)si do pamięci es:(r|e)di. Rejestry (r|e)di/(r|e)si są zwiększane/zmniejszane o 1 w zależności od flagi DF (o/1). [(r|e)s:edi]=[ds:(r|e)si] (r|e)di:=(r|e)di ±1 (r|e)si:=(r|e)si ±1 movsb











Instrukcja CMPS/CMPSD

cmps dword ptr [(r|e)si],[(r|e)di]
cmpsd

Porównuje podwójne słowo z pamięci ds:(r|e)si i z pamięci es:(r|e)di. Rejestry (r|e)di/(r|e)si są zwiększane/zmniejszane o 4 w zależności od flagi DF (o/1).

[ds:(r|e)si]-[es:(r|e)di]
(r|e)di:=(r|e)di ±4
(r|e)si:=(r|e)si ±4

cmpsd



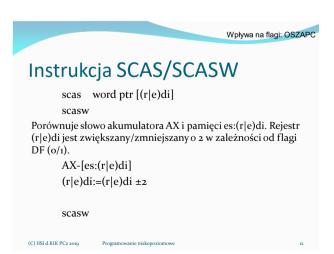
Instrukcja SCAS/SCASB

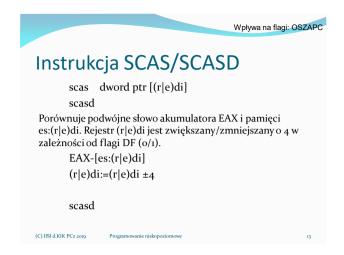
scas byte ptr [(r|e)di]
scasb

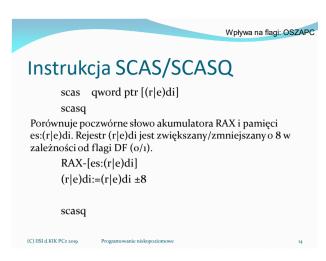
Porównuje bajt akumulatora AL i pamięci es:(r|e)di. Rejestr (r|e)di jest zwiększany/zmniejszany o 1 w zależności od flagi DF (o/1).

AL-[es:(r|e)di]
(r|e)di:=(r|e)di ±1

scasb





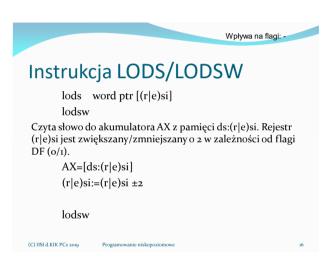


Instrukcja LODS/LODSB

lods byte ptr [(r|e)si]
lodsb

Czyta bajt do akumulatora AL z pamięci ds:(r|e)si. Rejestr
(r|e)si jest zwiększany/zmniejszany o 1 w zależności od flagi DF
(o/1).

AL=[ds:(r|e)si]
(r|e)si:=(r|e)si ±1
lodsb



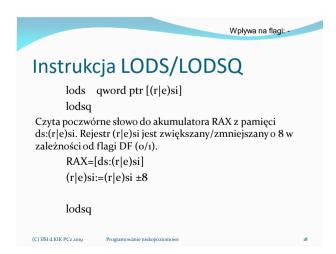
Instrukcja LODS/LODSD

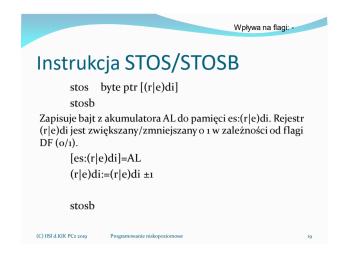
lods dword ptr [(r|e)si]
lodsd

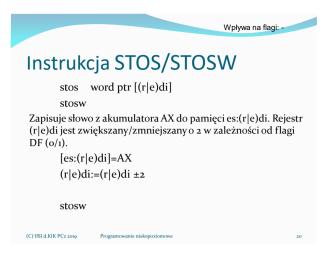
Czyta podwójne słowo do akumulatora EAX z pamięci ds:(r|e)si.
Rejestr (r|e)si jest zwiększany/zmniejszany o 4 w zależności od flagi DF (o/1).

EAX=[ds:(r|e)si]
(r|e)si:=(r|e)si ±4

lodsd







Instrukcja STOS/STOSD

stos dword ptr [(r|e)di]
stosd

Zapisuje podwójne słowo z akumulatora EAX do pamięci
es:(r|e)di. Rejestr (r|e)di jest zwiększany/zmniejszany o 4 w
zależności od flagi DF (o/1).
[es:(r|e)di]=EAX
(r|e)di:=(r|e)di ±4

stosd

Instrukcja STOS/STOSQ

stos qword ptr [(r|e)di]
stosq

Zapisuje poczwórne słowo z akumulatora RAX do pamięci
es:(r|e)di. Rejestr (r|e)di jest zwiększany/zmniejszany o 8 w
zależności od flagi DF (o/1).
[es:(r|e)di]=RAX
(r|e)di:=(r|e)di ±8

stosq

(C) ISI d.KIK PCz 2019 Programowanie niskopoziomowe 2 2

Prefiks REP REPNZ/REPNE REPZ/REPE Powoduje powtórzenie (R|E)CX razy następującej po nim instrukcji łańcuchowej, jeśli spełniony jest warunek (repnz powtarza dopóty ZF=o,jeśli ZF=1 powtarzanie jest przerywane itd.). Jeżeli (R|E)CX=o, to

instrukcja nie zostanie wykonana.

Prefiks REP

REPNZ/REPNE

REPZ/REPE

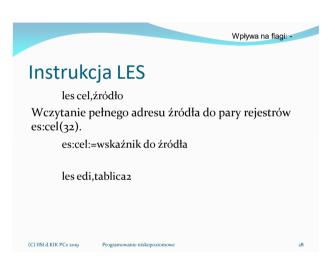
rep movsb
rep lodsd
rep stosq
repww cmpsw
repww scasb

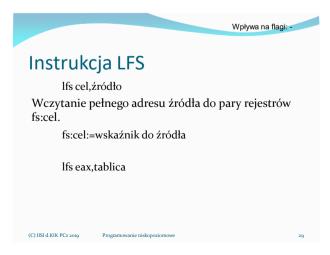
(C) IISI d.KIK PCz 2019

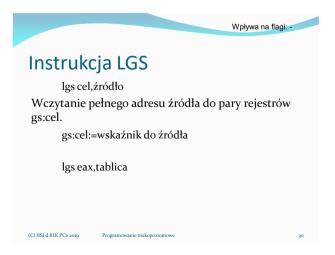


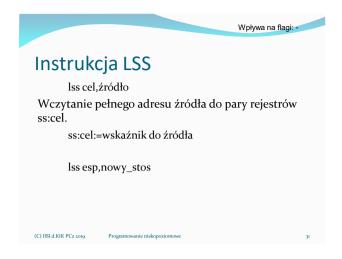
Operacje na rejestrach segmentowych LDS Załadowanie pełnego wskaźnika z użyciem DS LES Załadowanie pełnego wskaźnika z użyciem ES LFS Załadowanie pełnego wskaźnika z użyciem FS LGS Załadowanie pełnego wskaźnika z użyciem GS LSS Załadowanie pełnego wskaźnika z użyciem SS







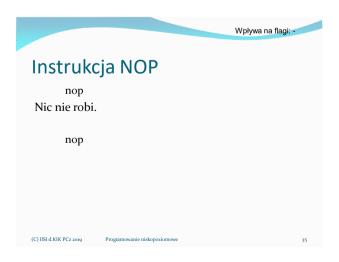


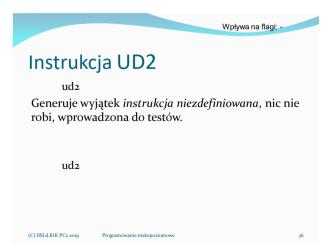


Inne operacje LOCK Powoduje niepodzielne wykonanie następnej instrukcji • LEA Ładowanie adresu efektywnego NOP Nie wykonuje żadnego działania • UD2 Instrukcja niezdefiniowana Tłumaczenie w oparciu o tablicę XLAT/XLATB translacji MOVBE Przesłanie po zamianie kolejności bajtów CPUID Identyfikacja procesora (C) IISI d.KIK PCz 2019

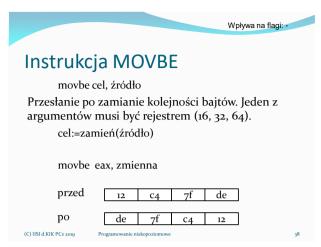












2019



