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

دستورات منطقی

- از دستورات منطقی یا بولی برای انجام عملیات منطقی یا بولی روی بیت ها استفاده می کنیم.
- عملیات بولی براساس منطق بولی است.
- منطق بولی سیستم استدلالی هستش که از ۰ و ۱ ها استفاده میکنه و از **NOT** و **OR** و **AND** تشکیل شده.
  - صفر : نادرست
  - یک: درست

Youtube: Onhexgroup

دستورات منطقی

- دستورات منطقی در اسمبلی:
  - **NOT**
  - **OR**
  - **XOR**
  - **AND**
  - **TEST**

Twitter: Onhexgroup

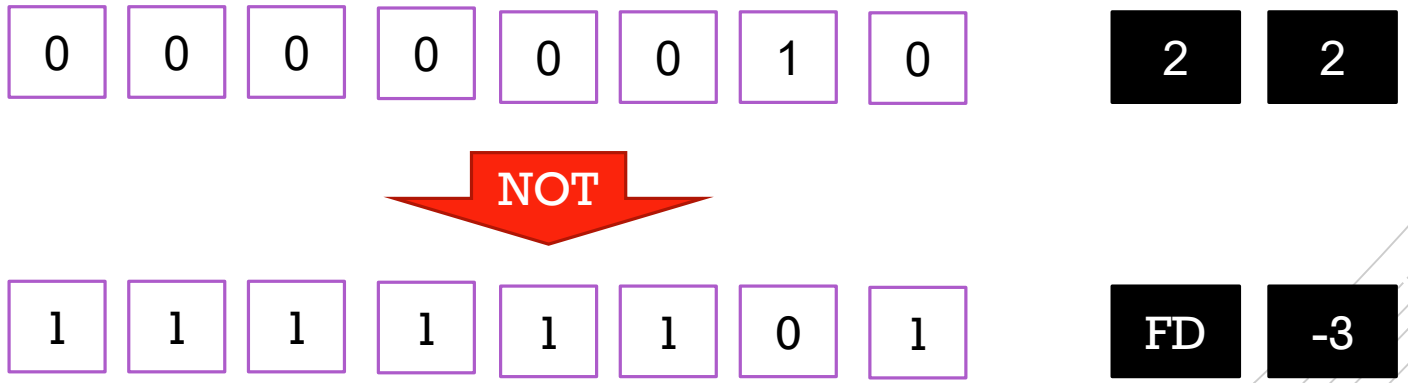
دستور NOT

- مقدار بیت دریافتی را معکوس میکند:
  - اگه صفر بدیم: ۱ میکنه
  - اگه یک بدیم: ۰ میکنه
- شکل کلی دستور:

NOT OP

- روی فلگها تاثیری نداره
- فرم **RM**:

NOT R/M



Onhexgroup.ir

دستور OR

- مفهومش: فرقی نمیکنه – هر کدوم شد.
- عملکردش:

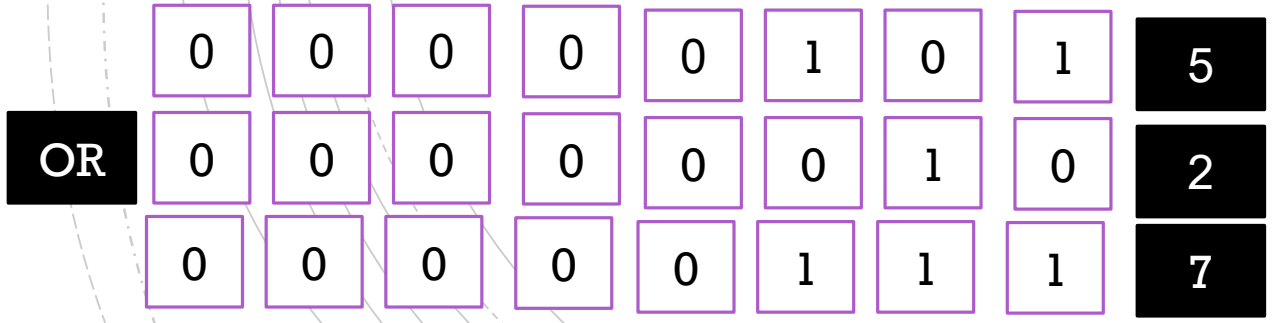
OR OP1,OP2

OP1=OP1 OR OP2

- روی فلگهای **OF** و **CF** و **SF** و **ZF** و **PF** تاثیر میزاره.

OR R/M,R/M/IMM

OP 1	OP 2	OP1 OR OP2
0	0	0
0	1	1
1	0	1
1	1	1

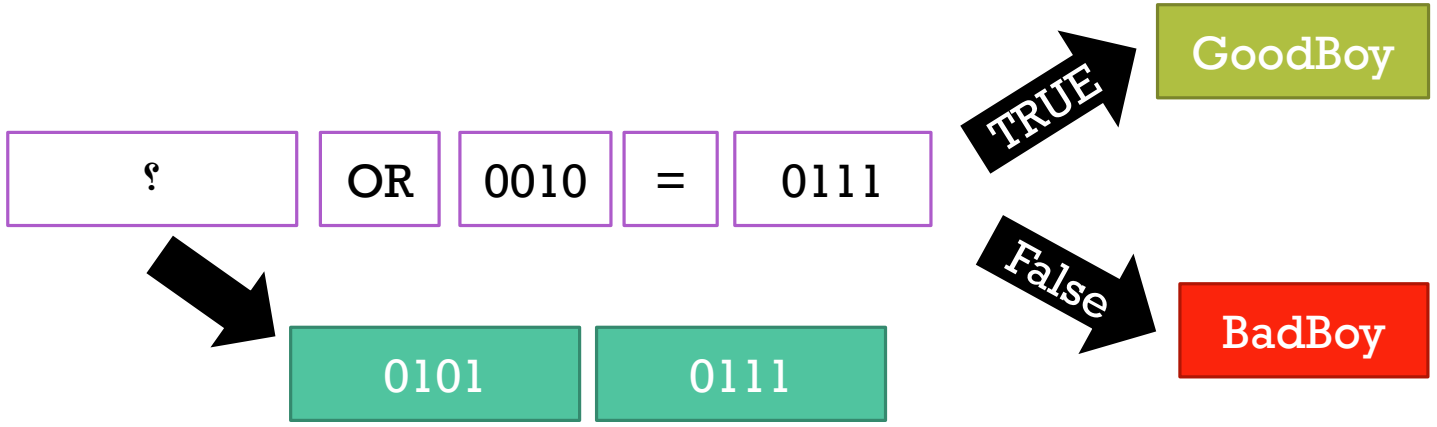


Telegram: onhex_ir

دستور OR

OP 1	OP 2	OP1 OR OP2
0	0	0
0	1	1
1	0	1
1	1	1

- نکته ۱: اگه بخواییم بیتی رو یک کنیم با یک **OR** میکنیم.
- نکته ۲: اگه بخواییم بیتی بدون تغییر بمونه با صفر **OR** میکینم.



5	OR	2	=	7
7	OR	2	=	7

- نکته ۱: اگه بخواییم بیتی رو یک کنیم با یک **OR** میکنیم.
- نکته ۲: اگه بخواییم بیتی بدون تغییر بمونه با صفر **OR** میکینم.

OP 1	OP 2	OP1 OR OP2
0	0	0
0	1	1
1	0	1
1	1	1

Github: Onhexgroup

دستور OR

a	61	0	1	1	0	0	0	0	1
A	41	0	1	0	0	0	0	0	1
b	62	0	1	1	0	0	0	1	0
B	42	0	1	0	0	0	0	1	0

کاراکتر بزرگ → کاراکتر کوچک

کاراکتر بزرگ **OR** 00100000 (20h / 32) → کاراکتر کوچک

Twitter: Onhexgroup

دستور XOR

- عملکردش:

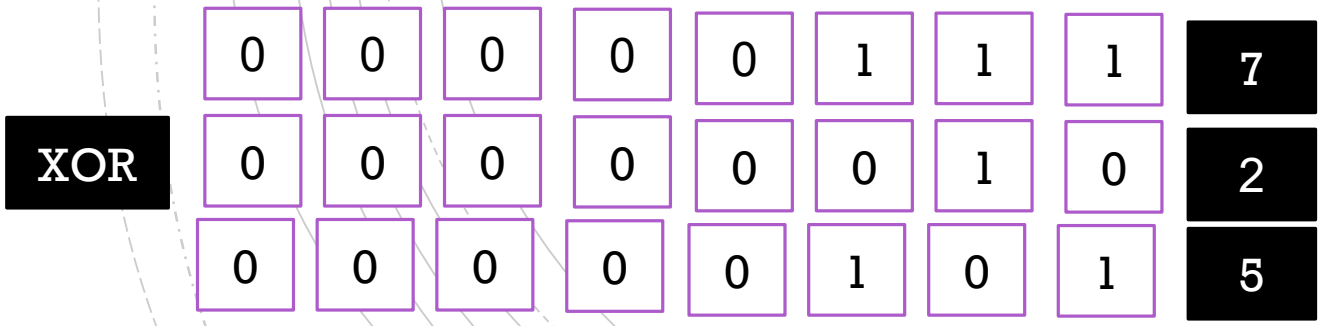
XOR OP1,OP2

OP1=OP1 XOR OP2

- روی فلگهای **OF** و **CF** و **SF** و **ZF** و **PF** تاثیر میزاره.

XOR R/M,R/M/IMM

OP 1	OP 2	OP1 XOR OP2
0	0	0
0	1	1
1	0	1
1	1	0

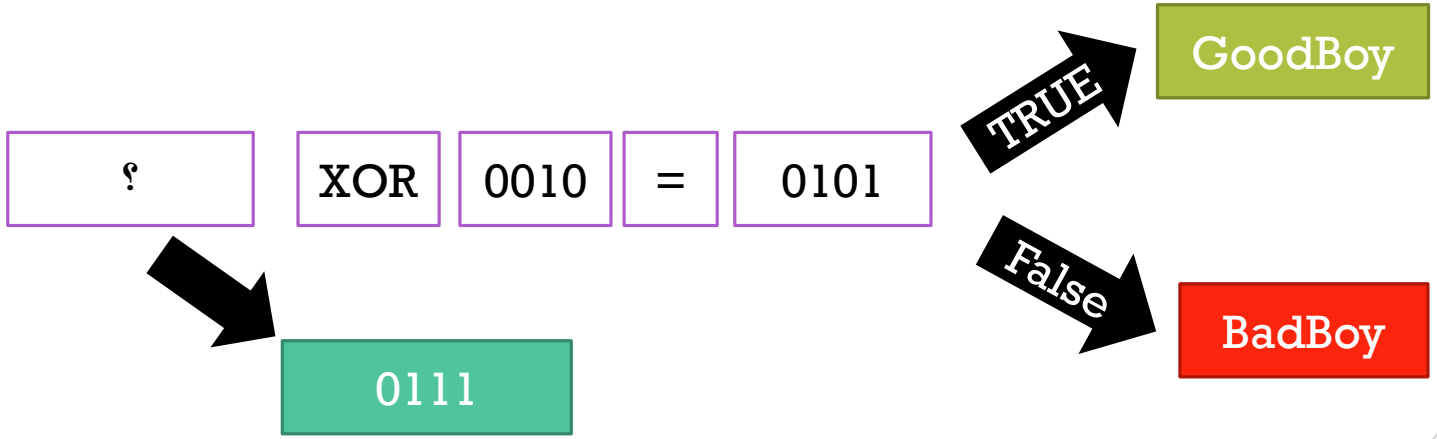


Onhexgroup.ir

دستور XOR

OP 1	OP 2	OP1 XOR OP2
0	0	0
0	1	1
1	0	1
1	1	0

- نکته ۱: اگه بخواییم بیتی رو معکوس کنیم، با یک **XOR** میکنیم.
- نکته ۲: اگه بخواییم بیتی بدون تغییر بمونه با صفر **XOR** میکینم.



7 XOR 2 = 5

Telegram: onhex_ir

دستور AND

- هم این هم اون – هر دو
- عملکردش:

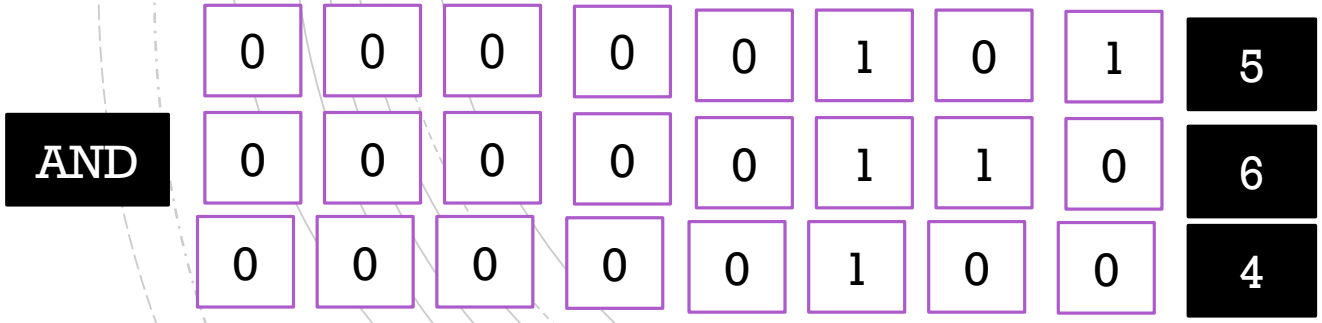
AND OP1,OP2

OP1=OP1 AND OP2

- روی فلگهای **OF** و **CF** و **SF** و **ZF** و **PF** تاثیر میزاره.

AND R/M,R/M/IMM

OP 1	OP 2	OP1 AND OP2
0	0	0
0	1	0
1	0	0
1	1	1

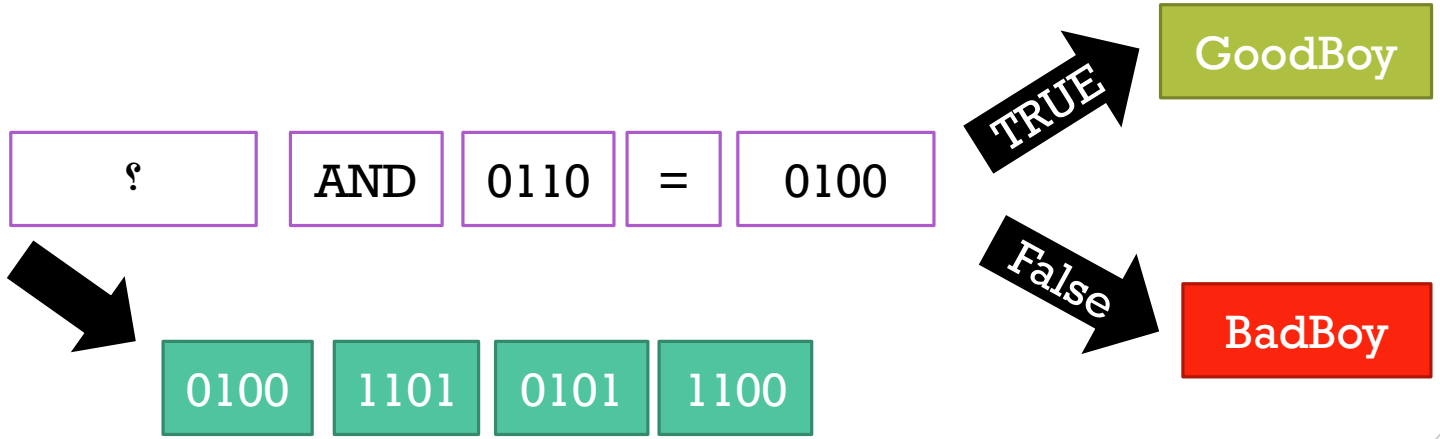


Youtube: Onhexgroup

دستور AND

- نکته ۱: اگه بخواییم بیتی رو صفر کنیم، با صفر **AND** میکنیم.
- نکته ۲: اگه بخواییم بیتی بدون تغییر باشه با یک **AND** میکنیم.

OP 1	OP 2	OP1 AND OP2
0	0	0
0	1	0
1	0	0
1	1	1



4 AND 6 = 4

13 AND 6 = 4

5 AND 6 = 4

12 AND 6 = 4

دستور AND

GitHub: Onhexgroup

OP 1	OP 2	OP1 AND OP2
0	0	0
0	1	0
1	0	0
1	1	1

- نکته ۱: اگه بخواییم بیتی رو صفر کنیم، با صفر **AND** میکنیم.
- نکته ۲: اگه بخواییم بیتی بدون تغییر باشه با یک **AND** میکنیم.

a	61	0	1	1	0	0	0	0	1
A	41	0	1	0	0	0	0	0	1
b	62	0	1	1	0	0	0	1	0
B	42	0	1	0	0	0	0	1	0

کاراکتر کوچک → کاراکتر بزرگ

کاراکتر کوچک **AND** **11011111** (**DFh** / **223**) → کاراکتر بزرگ

Onhexgroup.ir

دستور TEST

- مانند دستور **AND** است و فقط روی فلگها تاثیر میذاره.
- عملکردش:

TEST OP1,OP2

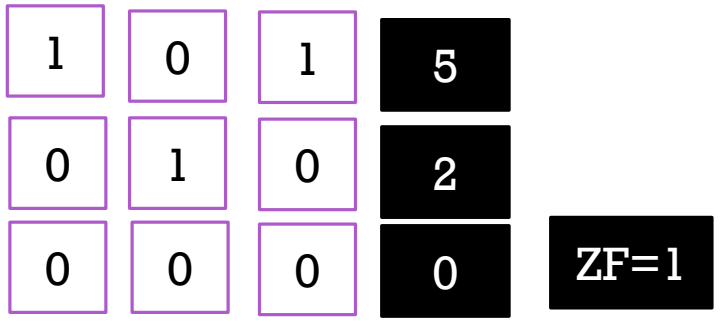
OP1 AND OP2

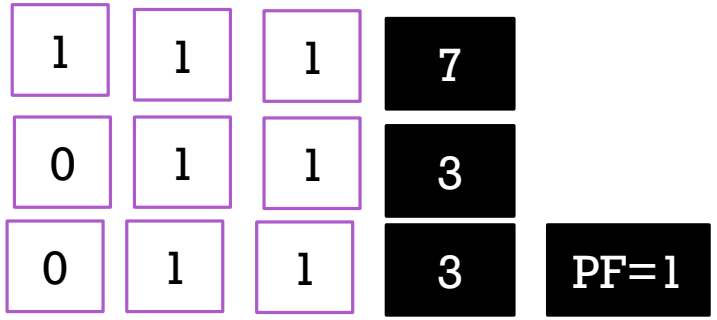
- روی فلگهای **OF** و **CF** و **SF** و **ZF** و **PF** تاثیر میزاره.

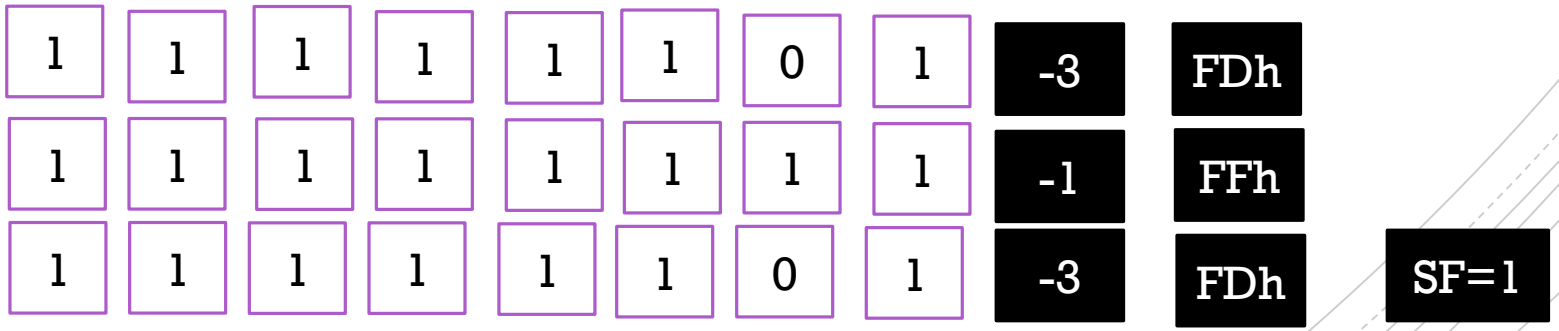
TEST R/M,R/M/IMM

Twitter: Onhexgroup

دستور TEST







Youtube: Onhexgroup

دستور CMP

- دو مقدار را با هم مقایسه میکند. (بزرگتر-مساوی-کوچکتر)
- مشابه دستور **SUB** است و فقط روی فلگها تاثیر میزاره.
- عملکردش:

CMP OP1,OP2

OP1 - OP2

- روی فلگهای **CF, OF, SF, ZF, AF, PF** تاثیر میزاره.

CMP R/M,R/M/IMM

مثال	ZF	CF	جواب
5>2	0	0	OP1> OP2
2=2	1	0	Op1 = op 2
2<5	0	1	Op1 < op2

Telegram: onhex_ir

درصد

ONHEXGROUP

62%

NOP 10%	PUSH 15%	CALL 8%	LEA 5%
MOV 27%	INT3 5%	ADD 3%	JNZ 2%
POP 3%	JMP 2%	XOR 2%	XADD 1%
CMP 3%	JG 1%	DEC 1%	JZ 2%
TEST 3%	RET 2%	SUB 2%	OTHRES 5%