دوره مهندسی معکوس نرم افزار

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

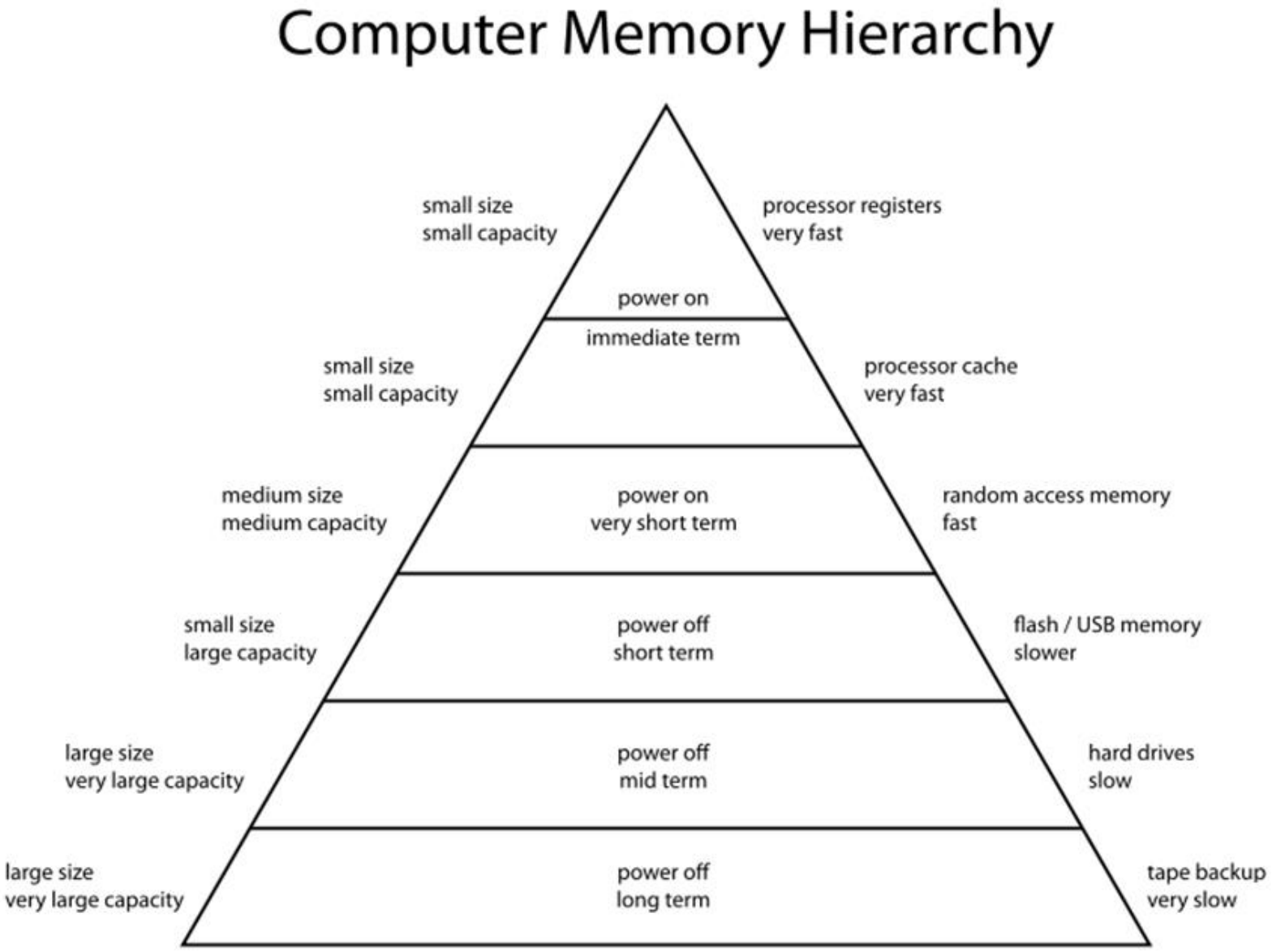
نسخه ی ۳۲ و ۶۴ بیتی

پلتفرم: ویندوز

ارائه دهنده : **OnhexGroup**

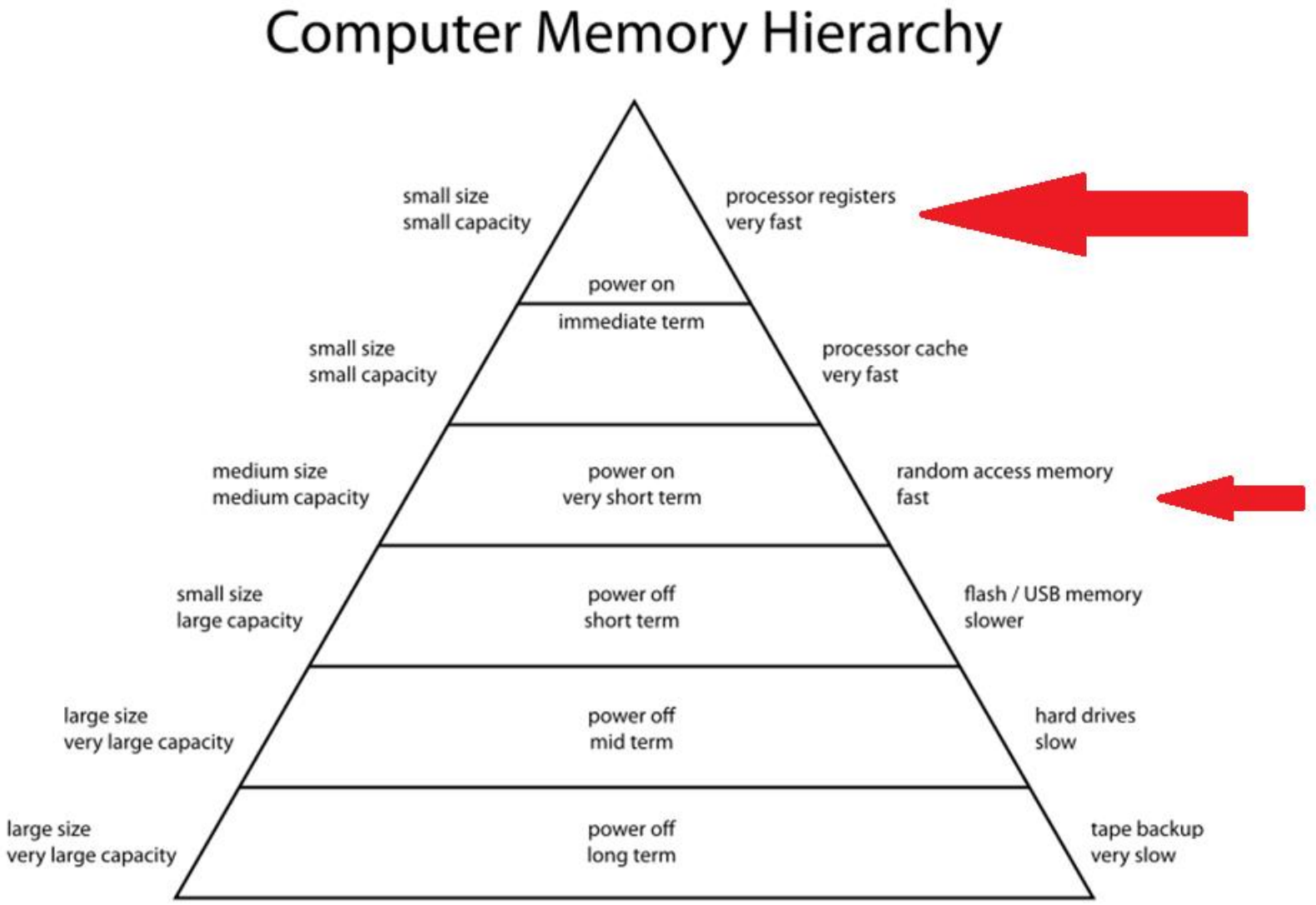
Onhexgroup.ir

سلسله مراتب حافظه



Telegram: onhex_ir

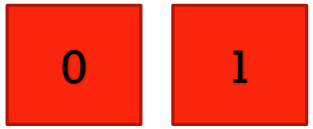
سلسله مراتب حافظه



Youtube: @onhexgroup

واحد های اندازه گیری

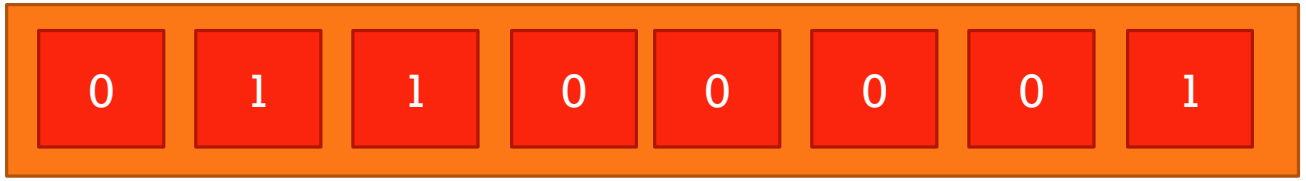
نوع	توضیحات
Bit	کوچکترین واحد. مقدارش ۰ یا ۱ هستش



Github: onhexgroup

واحد های اندازه گیری

نوع	توضیحات
Bit	کوچکترین واحد. مقدارش ۰ یا ۱ هستش
Byte	هر ۸ بیت ، یک بایت هستش.



Github: onhexgroup

آدرسها

- کوچکترین واحد قابل آدرس دهی
- در سیستم های ۳۲ بیتی 2^{32}
  - $2^{32} = 4{,}294{,}967{,}296 \sim$ 0xFFFFFFFF
- در سیستم های ۶۴ بیتی 2^{64}
  - $2^{64} = 18{,}446{,}744{,}073{,}709{,}552{,}000 \sim$ 0xFFFFFFFF`FFFFFFFF

Youtube: @onhexgroup

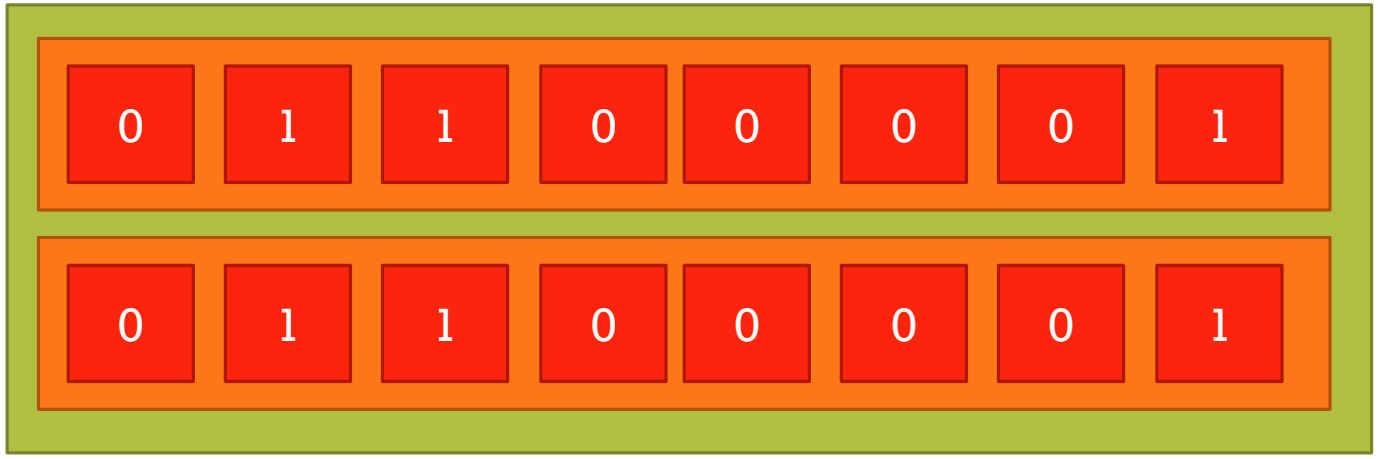
ASCII Code

Control Characters				Graphic Symbols											
Name	Dec	Binary	Hex	Symbol	Dec	Binary	Hex	Symbol	Dec	Binary	Hex	Symbol	Dec	Binary	Hex
NUL	0	0000000	00	space	32	0100000	20	@	64	1000000	40	'	96	1100000	60
SOH	1	0000001	01	!	33	0100001	21	A	65	1000001	41	a	97	1100001	61
STX	2	0000010	02	"	34	0100010	22	B	66	1000010	42	b	98	1100010	62
ETX	3	0000011	03	#	35	0100011	23	C	67	1000011	43	c	99	1100011	63
EOT	4	0000100	04	$	36	0100100	24	D	68	1000100	44	d	100	1100100	64
ENQ	5	0000101	05	%	37	0100101	25	E	69	1000101	45	e	101	1100101	65
ACK	6	0000110	06	&	38	0100110	26	F	70	1000110	46	f	102	1100110	66
BEL	7	0000111	07	'	39	0100111	27	G	71	1000111	47	g	103	1100111	67
BS	8	0001000	08	(	40	0101000	28	H	72	1001000	48	h	104	1101000	68
HT	9	0001001	09	)	41	0101001	29	I	73	1001001	49	i	105	1101001	69
LF	10	0001010	0A	*	42	0101010	2A	J	74	1001010	4A	j	106	1101010	6A
VT	11	0001011	0B	+	43	0101011	2B	K	75	1001011	4B	k	107	1101011	6B
FF	12	0001100	0C	,	44	0101100	2C	L	76	1001100	4C	l	108	1101100	6C
CR	13	0001101	0D	−	45	0101101	2D	M	77	1001101	4D	m	109	1101101	6D
SO	14	0001110	0E	.	46	0101110	2E	N	78	1001110	4E	n	110	1101110	6E
SI	15	0001111	0F	/	47	0101111	2F	O	79	1001111	4F	o	111	1101111	6F
DLE	16	0010000	10	0	48	0110000	30	P	80	1010000	50	p	112	1110000	70
DC1	17	0010001	11	1	49	0110001	31	Q	81	1010001	51	q	113	1110001	71
DC2	18	0010010	12	2	50	0110010	32	R	82	1010010	52	r	114	1110010	72
DC3	19	0010011	13	3	51	0110011	33	S	83	1010011	53	s	115	1110011	73
DC4	20	0010100	14	4	52	0110100	34	T	84	1010100	54	t	116	1110100	74
NAK	21	0010101	15	5	53	0110101	35	U	85	1010101	55	u	117	1110101	75
SYN	22	0010110	16	6	54	0110110	36	V	86	1010110	56	v	118	1110110	76
ETB	23	0010111	17	7	55	0110111	37	W	87	1010111	57	w	119	1110111	77
CAN	24	0011000	18	8	56	0111000	38	X	88	1011000	58	x	120	1111000	78
EM	25	0011001	19	9	57	0111001	39	Y	89	1011001	59	y	121	1111001	79
SUB	26	0011010	1A	:	58	0111010	3A	Z	90	1011010	5A	z	122	1111010	7A
ESC	27	0011011	1B	;	59	0111011	3B	[	91	1011011	5B	{	123	1111011	7B
FS	28	0011100	1C	<	60	0111100	3C	\	92	1011100	5C	|	124	1111100	7C
GS	29	0011101	1D	=	61	0111101	3D	]	93	1011101	5D	}	125	1111101	7D
RS	30	0011110	1E	>	62	0111110	3E	^	94	1011110	5E	~	126	1111110	7E
US	31	0011111	1F	?	63	0111111	3F	_	95	1011111	5F	Del	127	1111111	7F

Onhexgroup.ir

واحد های اندازه گیری

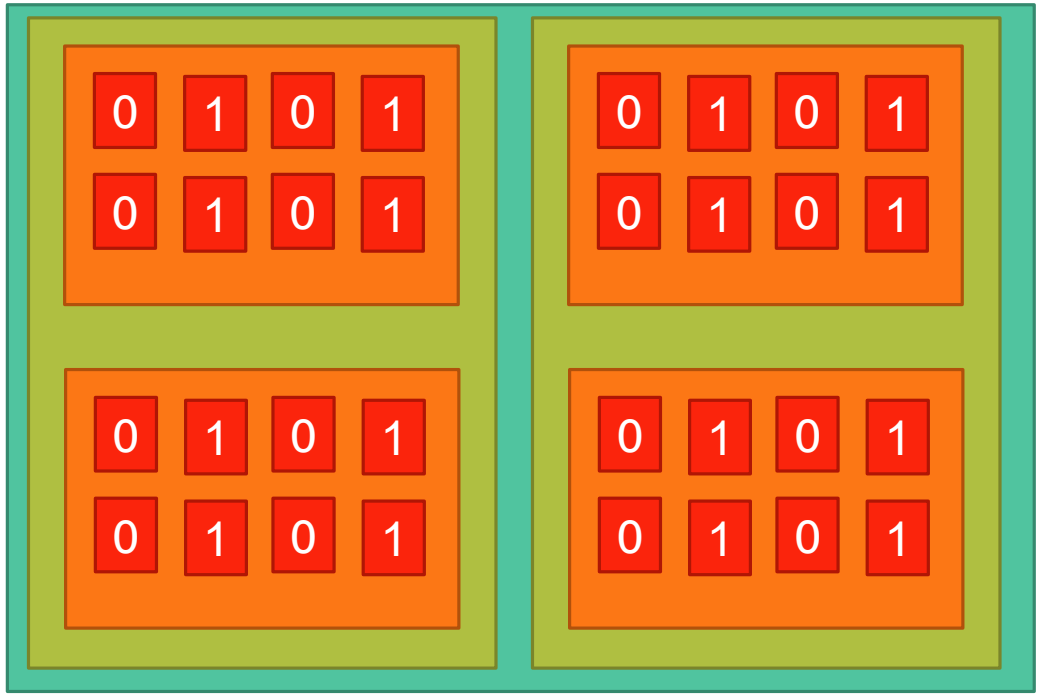
نوع	توضیحات
Bit	کوچکترین واحد. مقدارش ۰ یا ۱ هستش
Byte	هر ۸ بیت ، یک بایت هستش.
Word	هر ۱۶ بیت یا ۲ بایت یک کلمه هستش.



Onhexgroup.ir

واحد های اندازه گیری

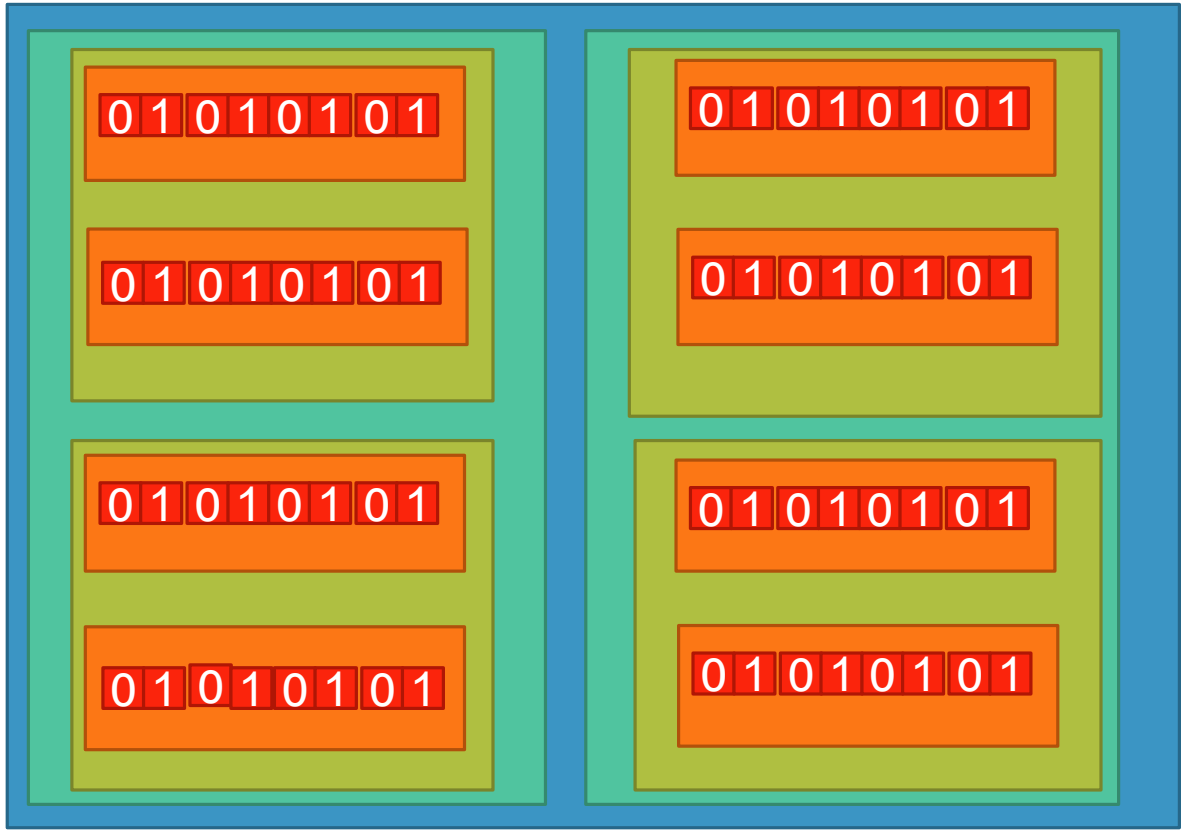
نوع	توضیحات
Bit	کوچکترین واحد. مقدارش ۰ یا ۱ هستش
Byte	هر ۸ بیت ، یک بایت هستش.
Word	هر ۱۶ بیت یا ۲ بایت یک کلمه هستش.
DWord	هر ۳۲ بیت یا ۴ بایت یا ۲ کلمه برابر یه **Dword** هستش.



Onhexgroup.ir

واحد های اندازه گیری

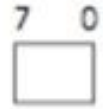
نوع	توضیحات
Bit	کوچکترین واحد. مقدارش ۰ یا ۱ هستش
Byte	هر ۸ بیت ، یک بایت هستش.
Word	هر ۱۶ بیت یا ۲ بایت یک کلمه هستش.
DWord	هر ۳۲ بیت یا ۴ بایت یا ۲ کلمه برابر یه **Dword** هستش.
QWord	هر ۶۴ بیت یا ۸ بایت یا ۴ کلمه یا دو **Dword** برابر یه **Qword** هستش.



Onhexgroup.ir

انواع داده
در زبان C

In C: char

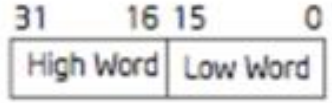


Byte

In C: short

Word

In C: int/long



DWord

In C: double/long long

QWord

Onhexgroup.ir

انواع داده

نوع	توضیحات
Bit	کوچکترین واحد. مقدارش ۰ یا ۱ هستش
Byte	در اسمبلی با عنوان **DB** شناخته میشه
Word	در اسمبلی با عنوان **DW** شناخته میشه
DWord	در اسمبلی با عنوان **DD** شناخته میشه
QWord	در اسمبلی با عنوان **DQ** شناخته میشه

Onhex_ir

Onhexgroup.ir

انواع داده

Onhex_ir

Char

o

n

h

e

x

_

i

r

Onhexgroup.ir

انواع داده

Onhex_ir

Onhexgroup.ir

انواع داده

Char	Ascii-binary
o	01101111
n	01101110
h	01101000
e	01100101
x	01111000
_	01011111
i	01101001
r	01110010

Onhex_ir

Onhexgroup.ir

انواع داده

Char	Ascii-binary	Ascii-Hex
o	01101111	6F
n	01101110	6E
h	01101000	68
e	01100101	65
x	01111000	78
_	01011111	5F
i	01101001	69
r	01110010	72

Onhex_ir

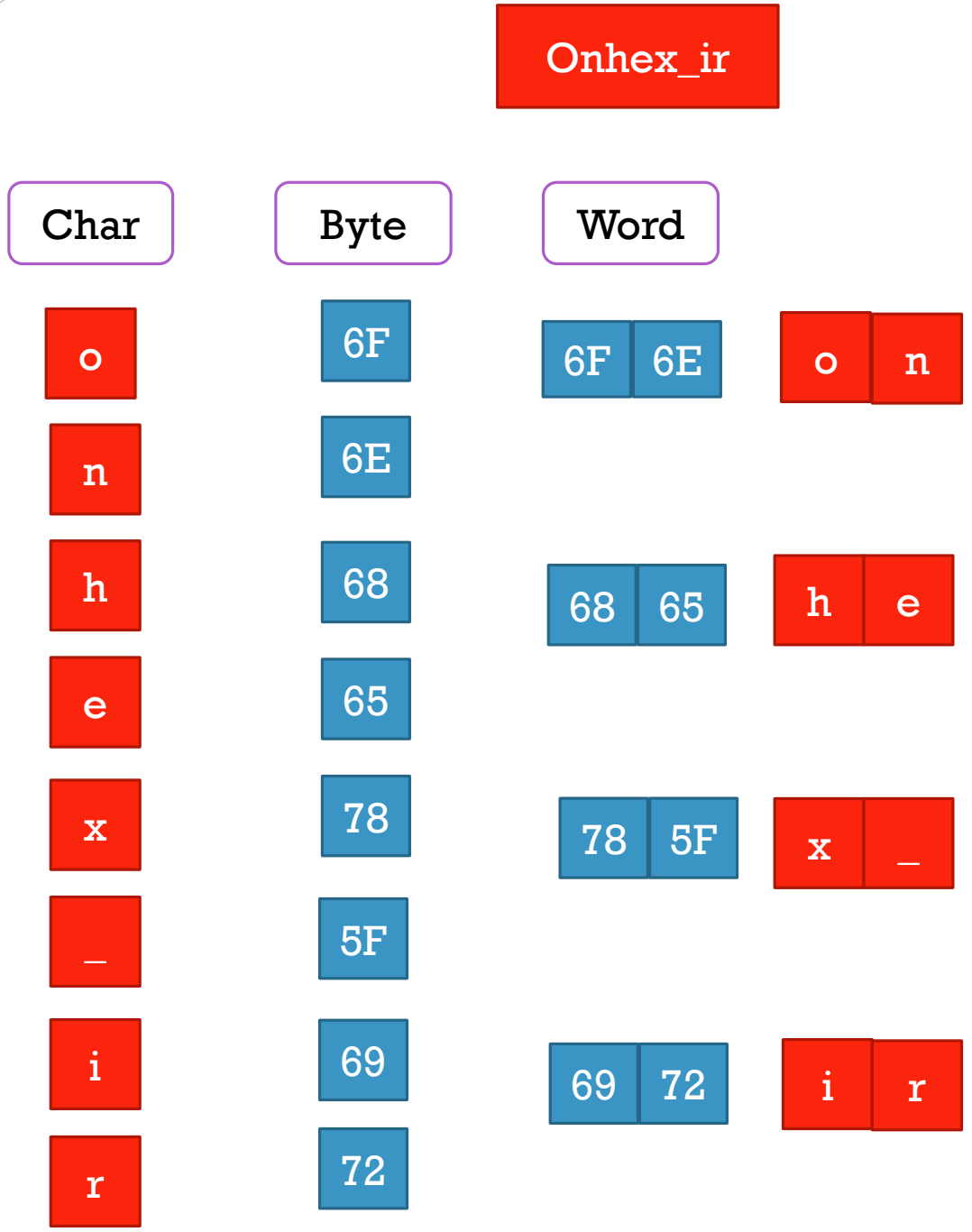
Onhexgroup.ir

انواع داده

Char	Ascii-binary	Ascii-Hex	Byte
o	01101111	6F	6F
n	01101110	6E	6E
h	01101000	68	68
e	01100101	65	65
x	01111000	78	78
_	01011111	5F	5F
i	01101001	69	69
r	01110010	72	72

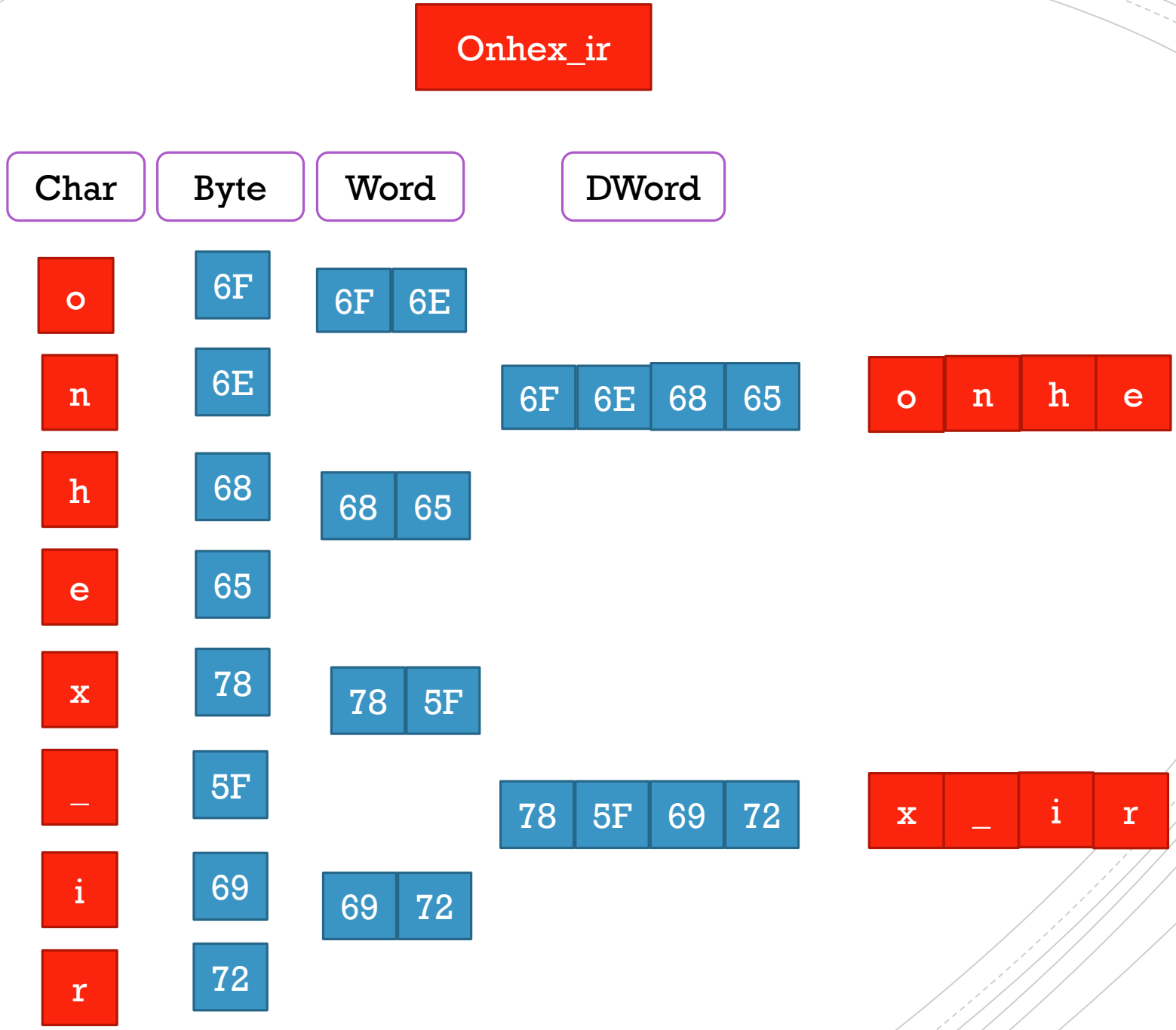
Onhexgroup.ir

انواع داده



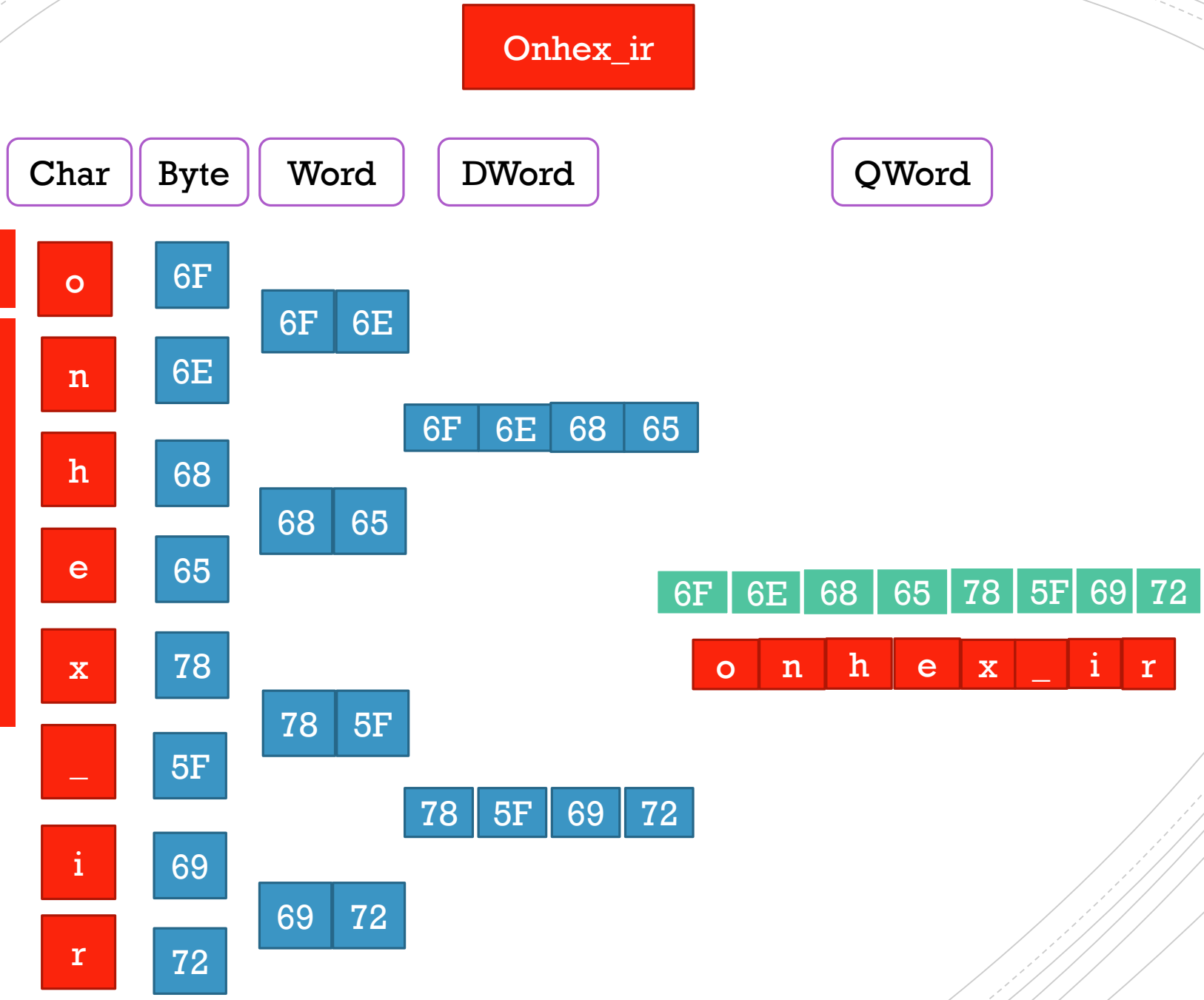
Onhexgroup.ir

انواع داده



Onhexgroup.ir

انواع داده



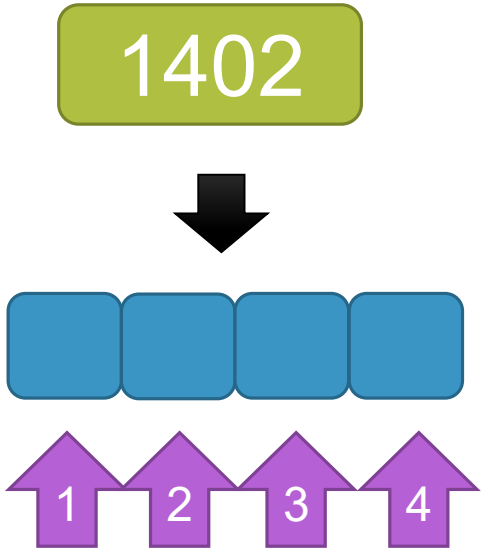
Onhexgroup.ir

Endianness

- نحوه ی چینش داده ها بصورت افقی در یه فضای آدرس پذیر (مموری)
- دو نوع :
  - **Big-Endian**
  - **Little-Endian**

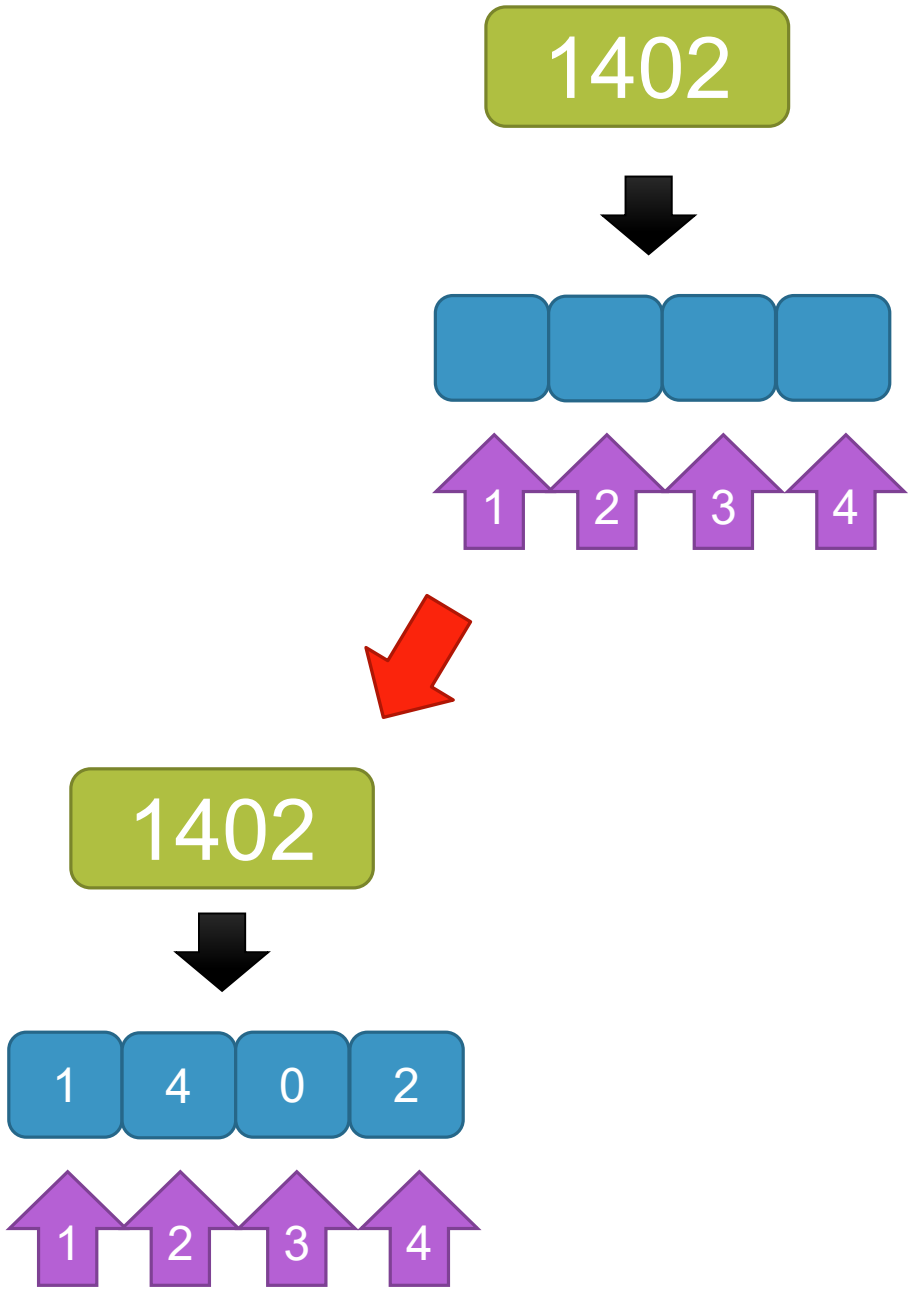
Onhexgroup.ir

Endianness



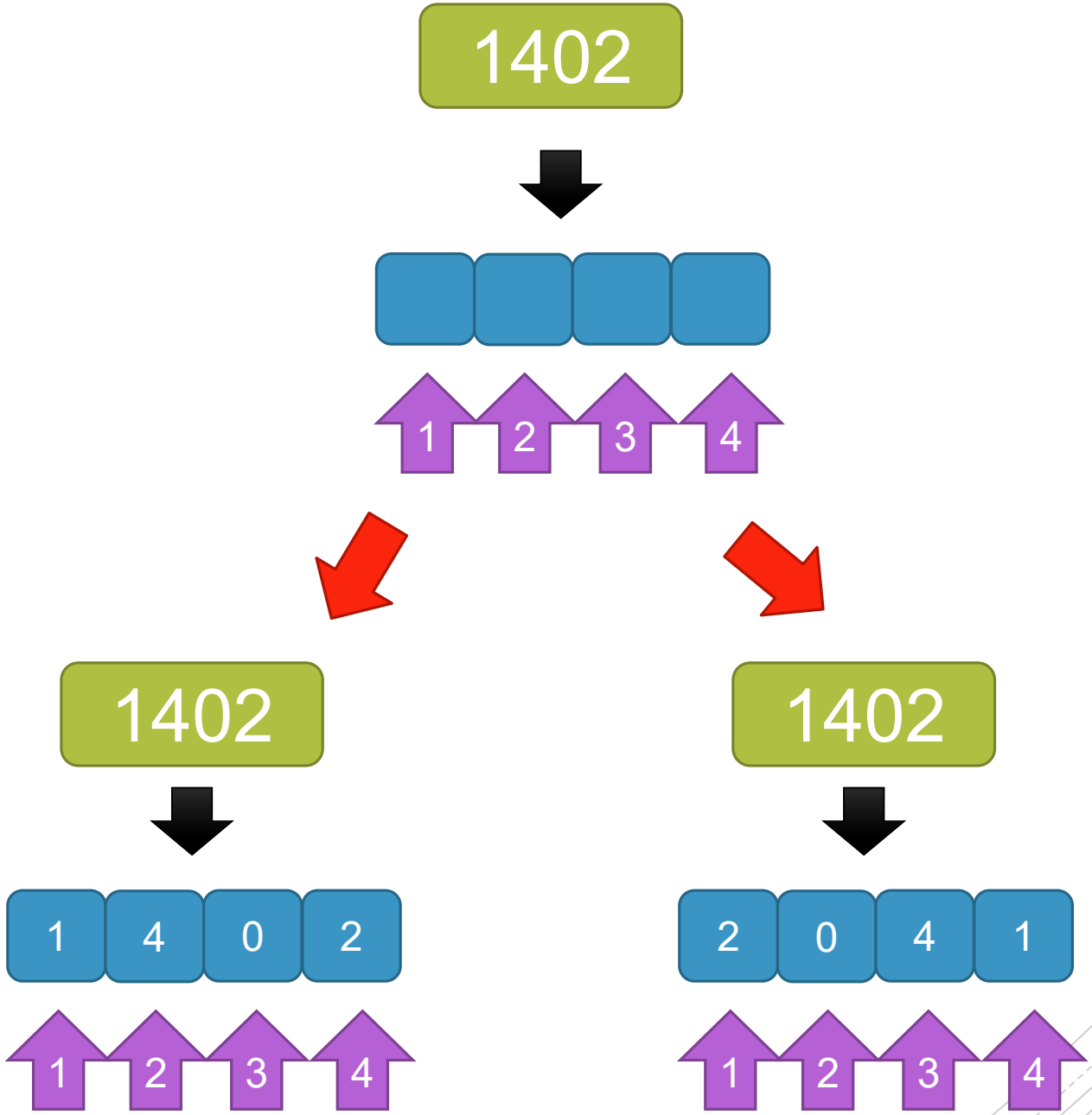
Onhexgroup.ir

Endianness



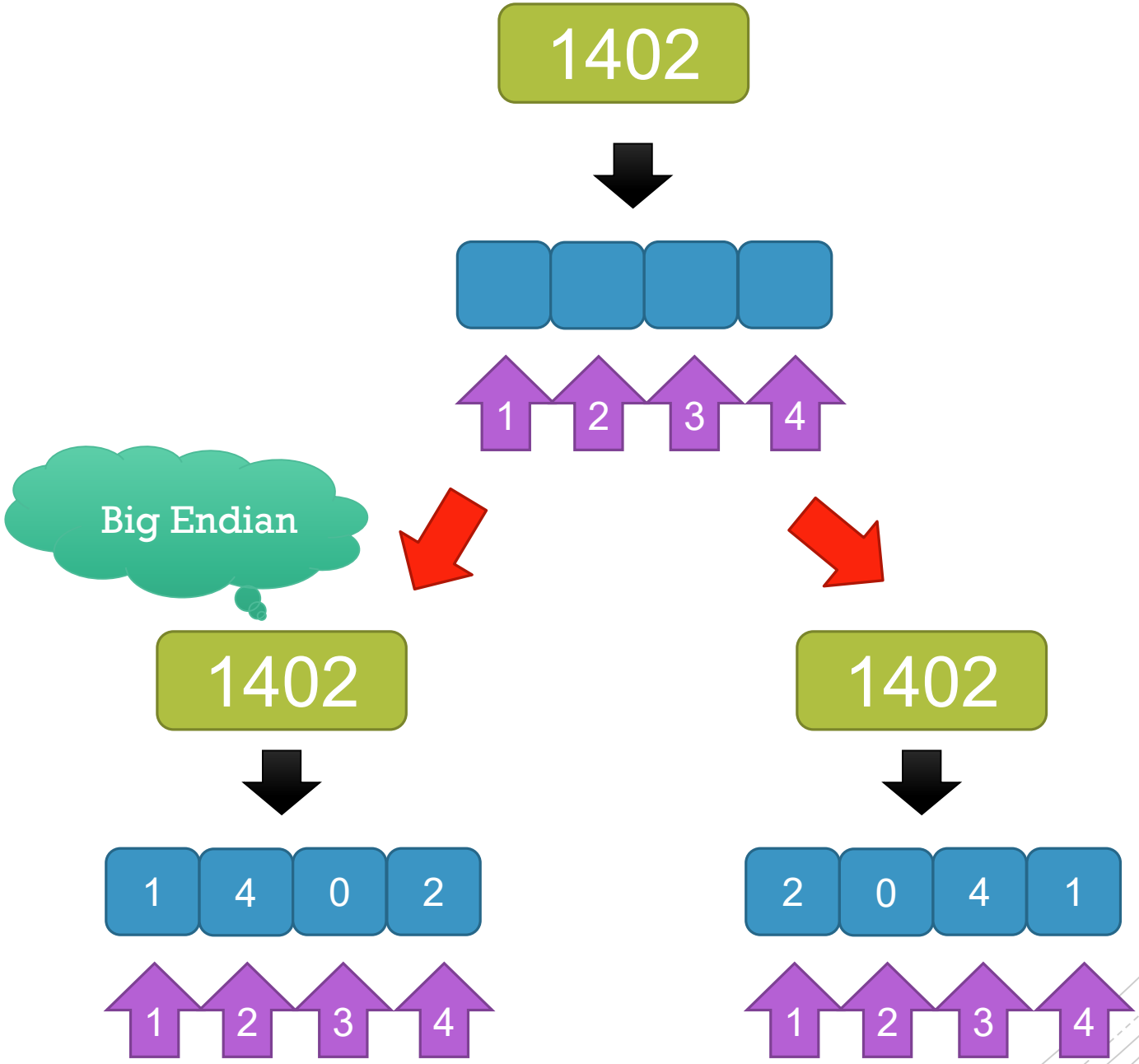
Onhexgroup.ir

Endianness



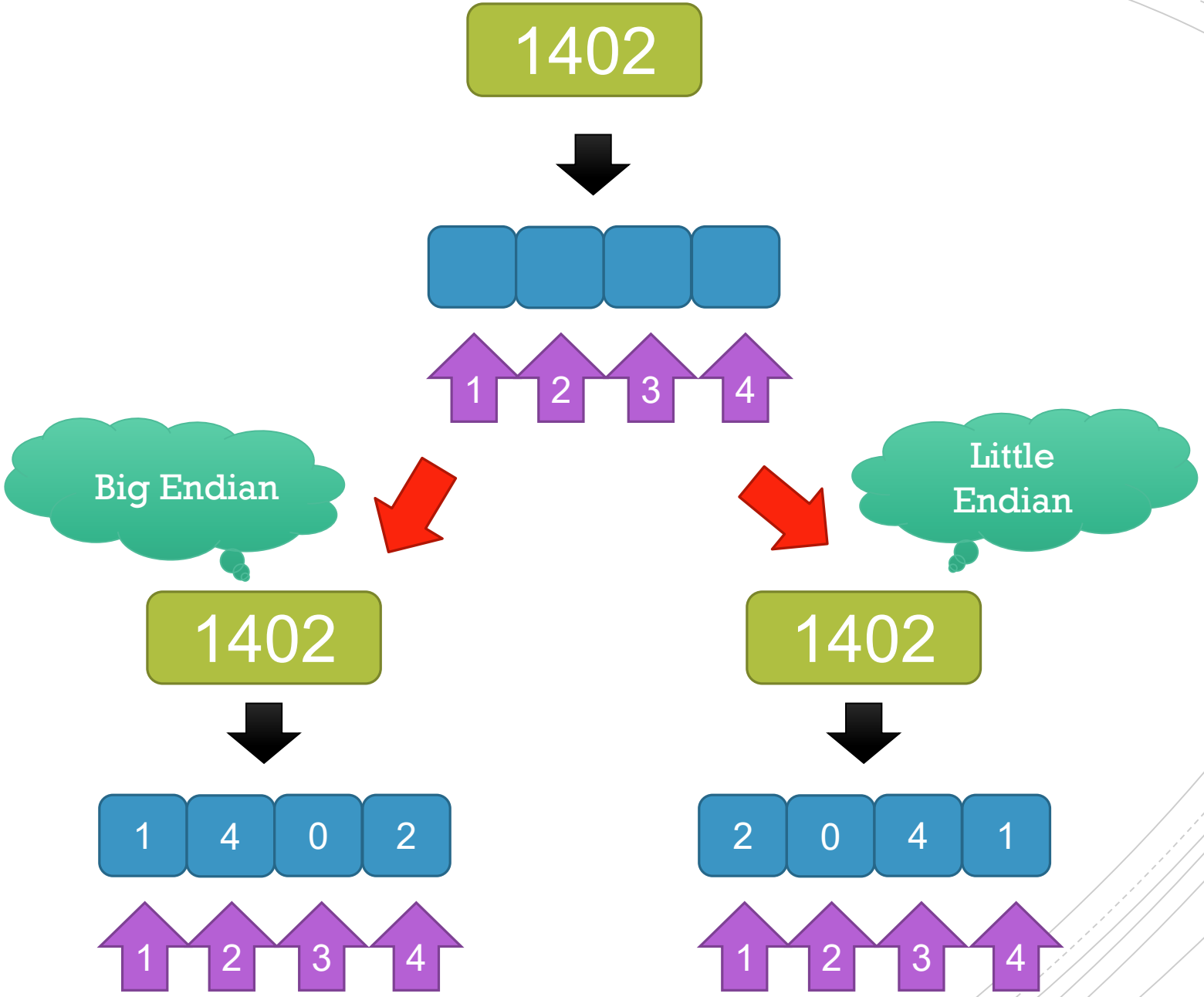
Onhexgroup.ir

Endianness



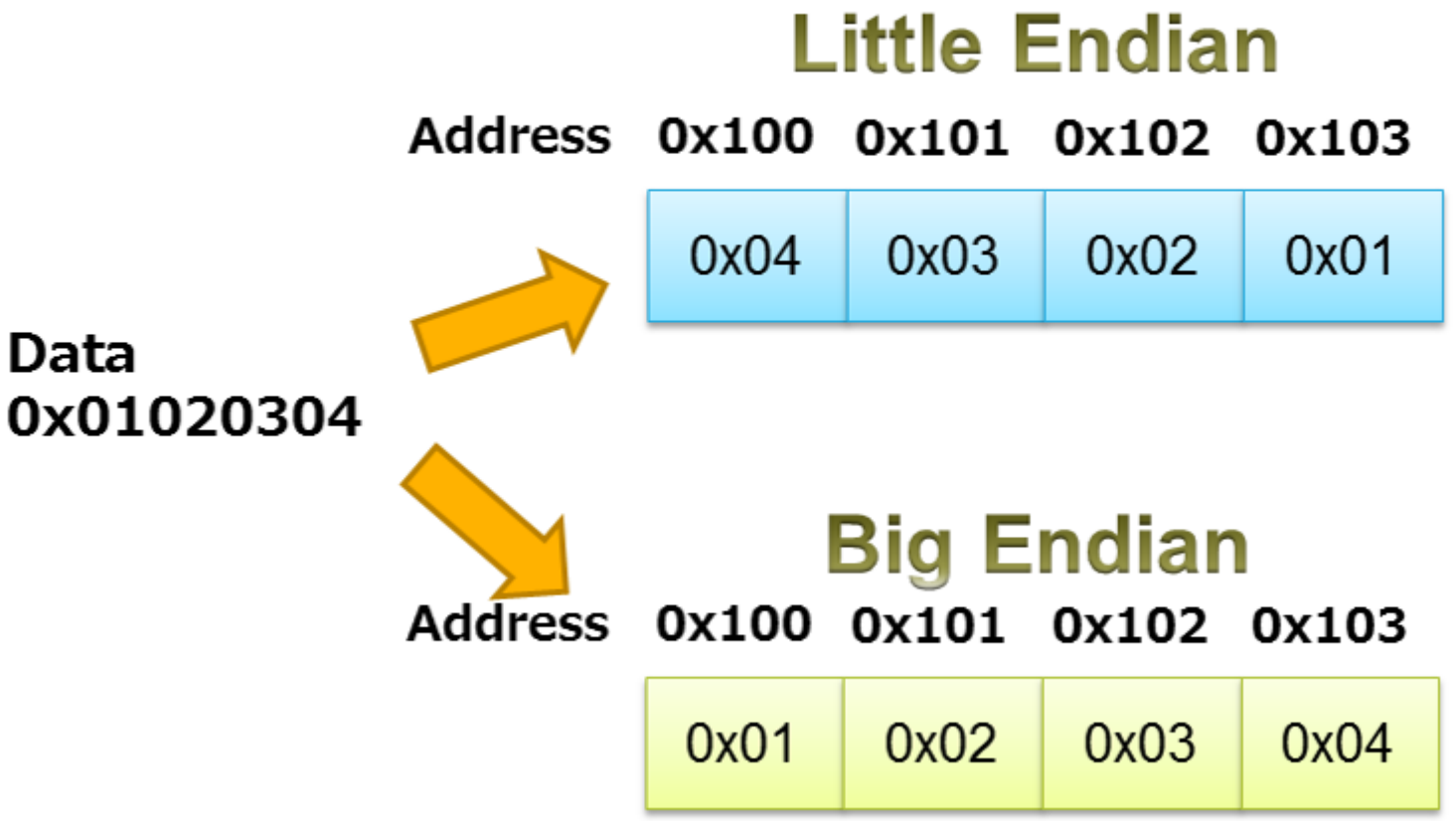
Onhexgroup.ir

Endianness



Onhexgroup.ir

Endianness



Onhexgroup.ir

Endianness

- **X86** یه معماری **Little Endian** هستش و معمولا ترافیک ارسالی در شبکه بصورت **Big Endian** هستش.
- **Endianness** برای ذخیره مقادیر در حافظه مورد استفاده قرار میگیره و نه برای رجیسترها.
- **Endianness** برای بایت ها اعمال میشه و نه بیت ها.

Onhexgroup.ir

اساس این دوره

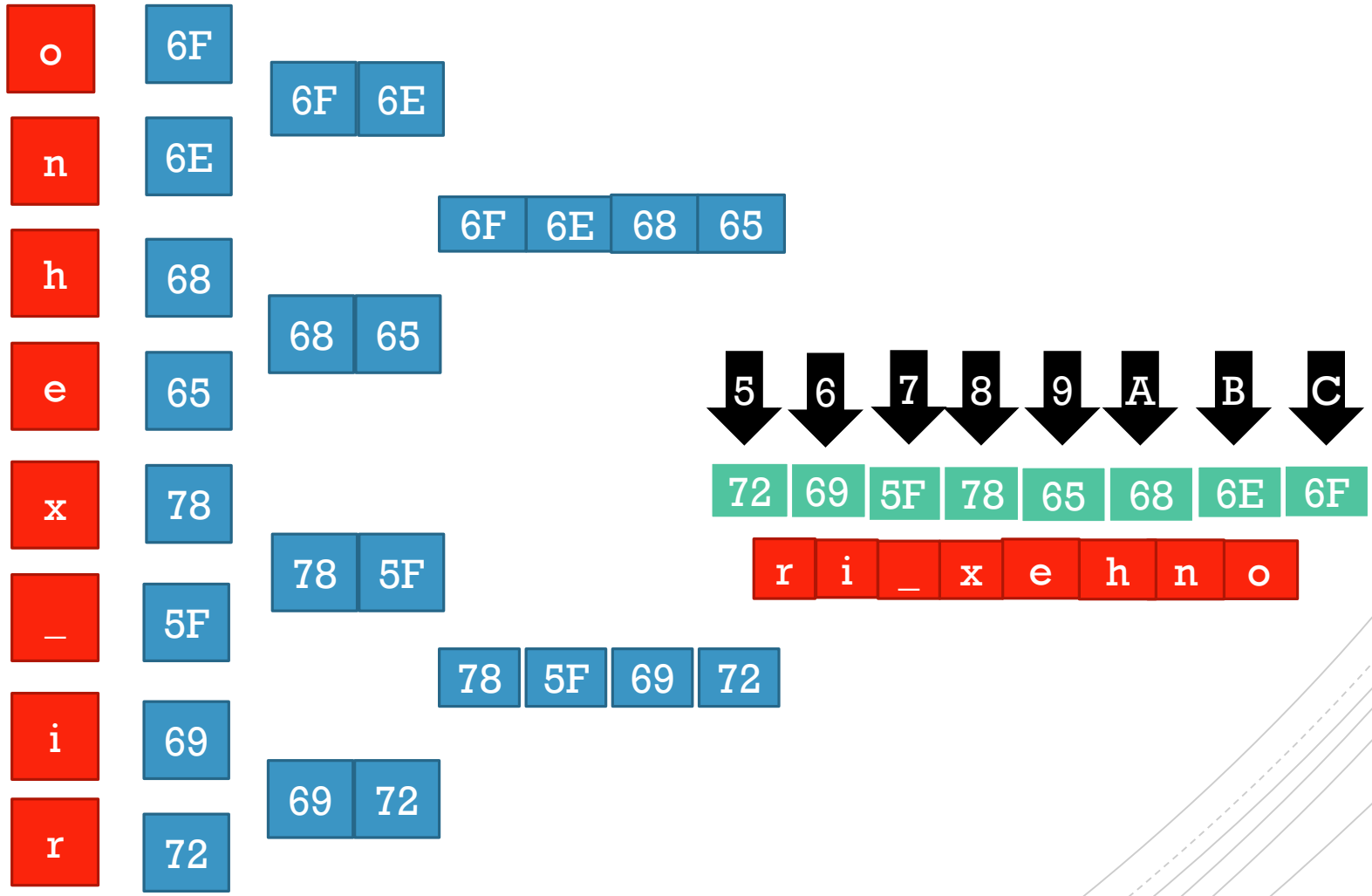
- در این دور ما موارد زیر رو پوشش میدیم:
  - پردازنده های خانواده X86
  - نسخه ی ۳۲ بیتی و ۶۴ بیتی رو پوشش میدیم.
  - در حالت Protected Mode هستیم
  - مهندسی معکوس برنامه های کامپایلری (C/C++)
  - نمایش در حافظه بصورت Little Endian خواهد بود.

Onhex_ir

Char | Byte | Word | DWord | QWord

Onhexgroup.ir

مثال



Onhexgroup.ir

منابع

- https://en.wikipedia.org/wiki/Endianness
- https://en.wikipedia.org/wiki/Memory_hierarchy
- https://www.geeksforgeeks.org/memory-hierarchy-design-and-its-characteristics/