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**

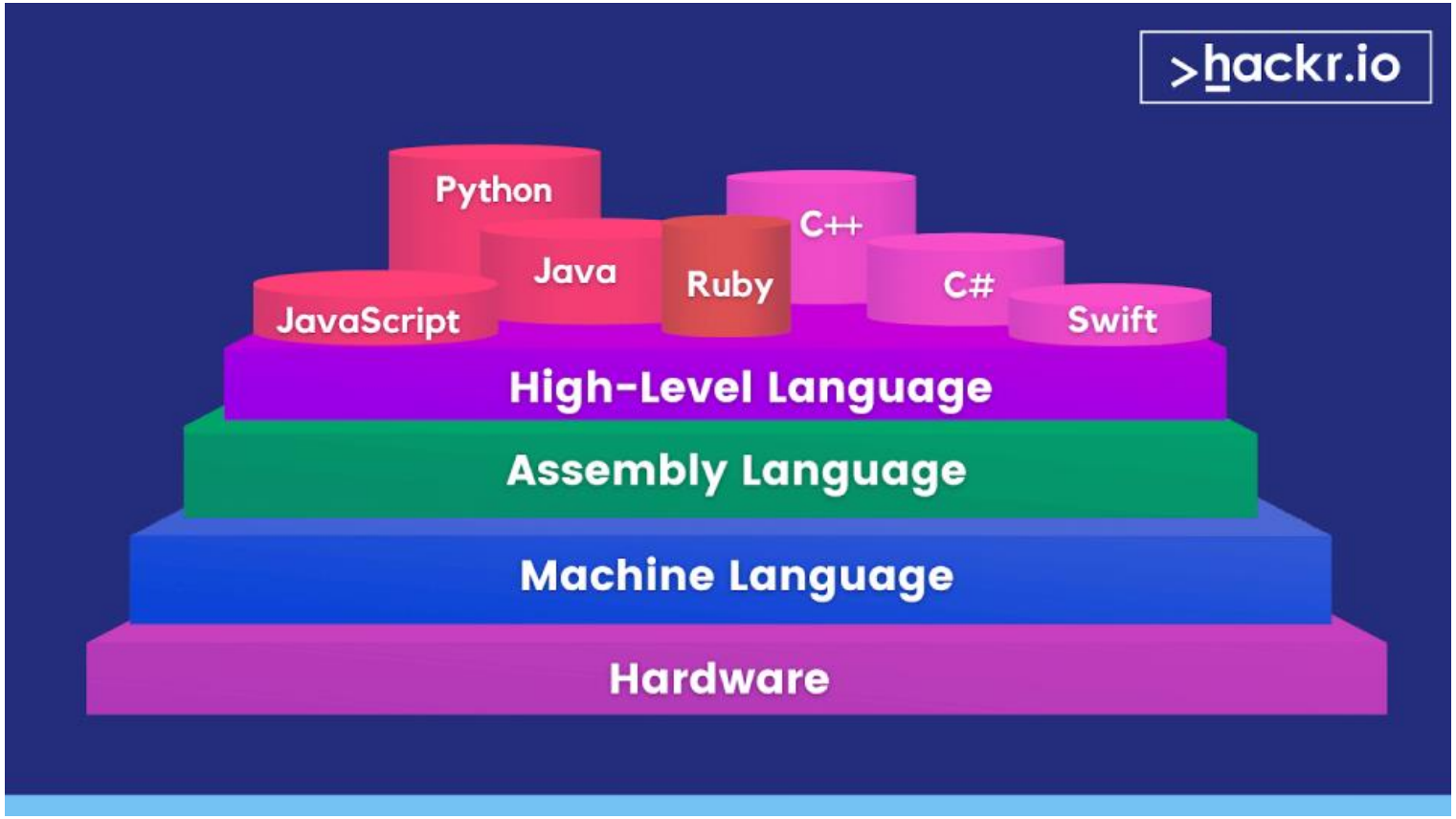
Onhexgroup.ir

انواع زبانهای برنامه نویسی

- زبانهای سطح پایین
  - نسل اول : زبان ماشین
  - نسل دوم : اسمبلی
- زبانهای سطح بالا
  - مانند سی ، سی شارپ ، پایتون ، گولنگ و ...
- از لحاظ مدیریت حافظه زبانهای سطح میانی ، مانند سی هم تعریف میکنن
- سطح پایین ، سطح بالا یه تعریف نسبی هست

Youtube: Onhexgroup

انواع زبانهای برنامه نویسی



Onhexgroup.ir

انواع زبانهای برنامه نویسی سطح بالا

- زبانهای برنامه نویسی مفسری
- زبانهای برنامه نویسی کامپایلری
- زبانهای برنامه نویسی هم مفسری هم کامپایلری

Telegram: onhex_ir

زبانهای برنامه نویسی مفسری

- نمونه :
  - پایتون ، روبی ، جاوااسکریپت، Lua ، پاورشل و ...
- توسط مفسر یا Interpreter تبدیل میشه
- دستورات خط به خط خوانده و به زبان ماشین تبدیل میشه (بلافاصله)
- در هر بار اجرا روند خط به خط خوندن انجام میشه (کند)
- برای اجرا باید اون مفسر باشه
- کد قابل مشاهده هستش
- توسعه ، نگهداری و دیباگشون ساده هست

Youtube: Onhexgroup

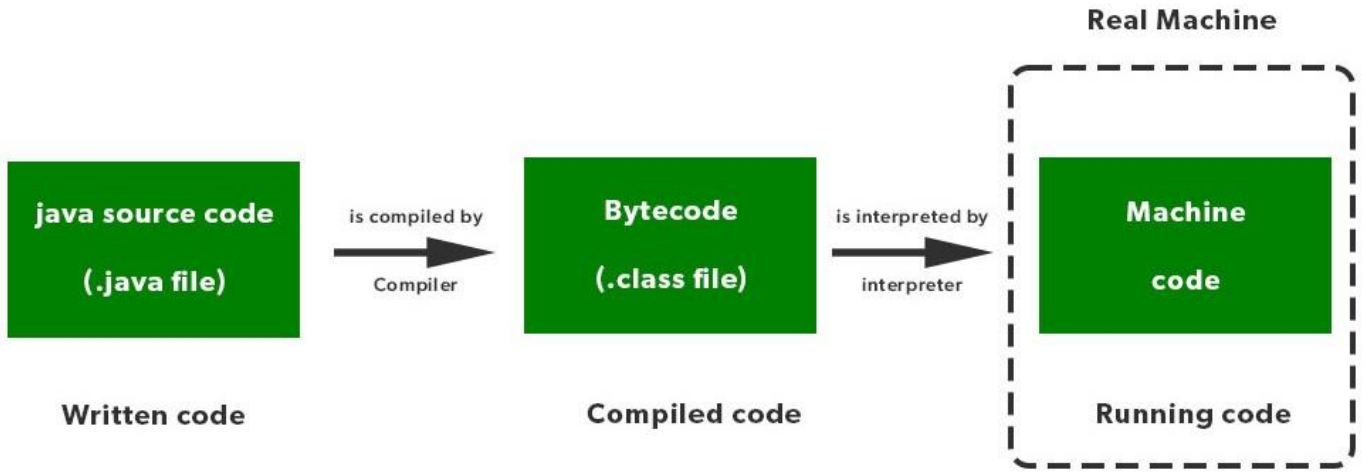
زبانهای برنامه نویسی کامپایلری

- نمونه :
- سی ، سی شارپ ، گولنگ و ...
- توسط ابزاری بنام کامپایلر تبدیل میشن.
- دستورات بصورت کامل بررسی و به یک فایل قابل اجرا در سیستم عامل هدف تبدیل میشن.
- کدها بهینه سازی میشن.
- نیاز به کامپایلر برای اجرا نیست.
- کد قابل مشاهده نیست

Onhexgroup.ir

زبانهای برنامه نویسی هم مفسری هم کامپایلری

- جاوا
- کدها در ابتدا به بایت کد تبدیل میشه و در زمان اجرا ماشین مجازی جاوا (JVM) اونارو تبدیل به زبان ماشین میکنه.



Telegram: onhex_ir

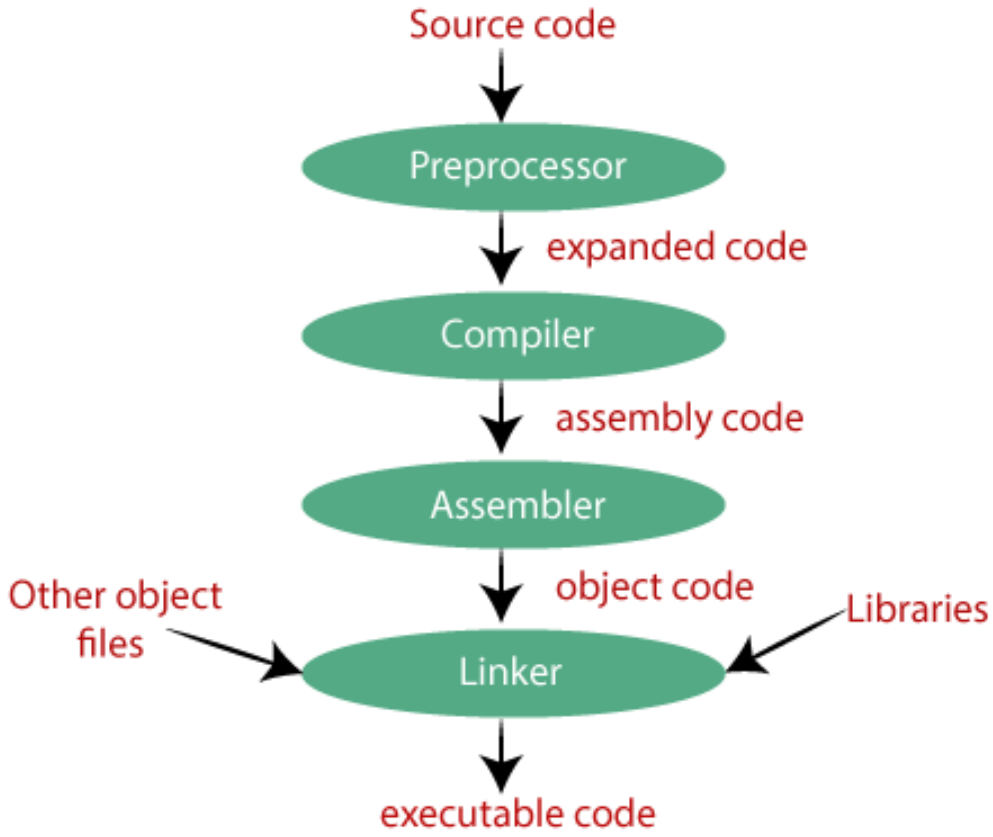
اساس این دوره

- 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++)

Onhexgroup.ir

نحوه ی کار کامپایلرها

- مراحل تبدیل کد سی به فایل اجرایی :



Onhexgroup.ir

Preprocessor

- قبل از کامپایل اطلاعات مرتبط با دستورات پیش پردازنده رو به کد اضافه میکنه.
- دستورات پیش پردازنده، دستوراتی هستن که با # شروع میشن. مانند : include , error, define , ...
- ورودی این مرحله فایل **.c** و خروجی اون **.i**
- دستور این مرحله :

```
cl /P /EP code.c
```

Telegram: onhex_ir

Compiler

- تبدیل کد تولید شده از Preprocessor به کد های اسمبلی
- ورودی این مرحله فایل i. و خروجی اون asm.
- دستور این مرحله :

```
cl /c /Facode.asm /Tccode.i
```

Onhexgroup.ir

Assembler

- تبدیل فایل اسمبلی به Object File
- فایل Obj حاوی کد ماشین یا object code هستش اما معمولا بصورت مستقیم اجرا نمیشه
- ورودی این مرحله فایل asm. و خروجی اون obj.
- دستور این مرحله :

```
ml.exe /c /coff /Zi /Fl /Fo code.obj
code.asm
```

Onhexgroup.ir

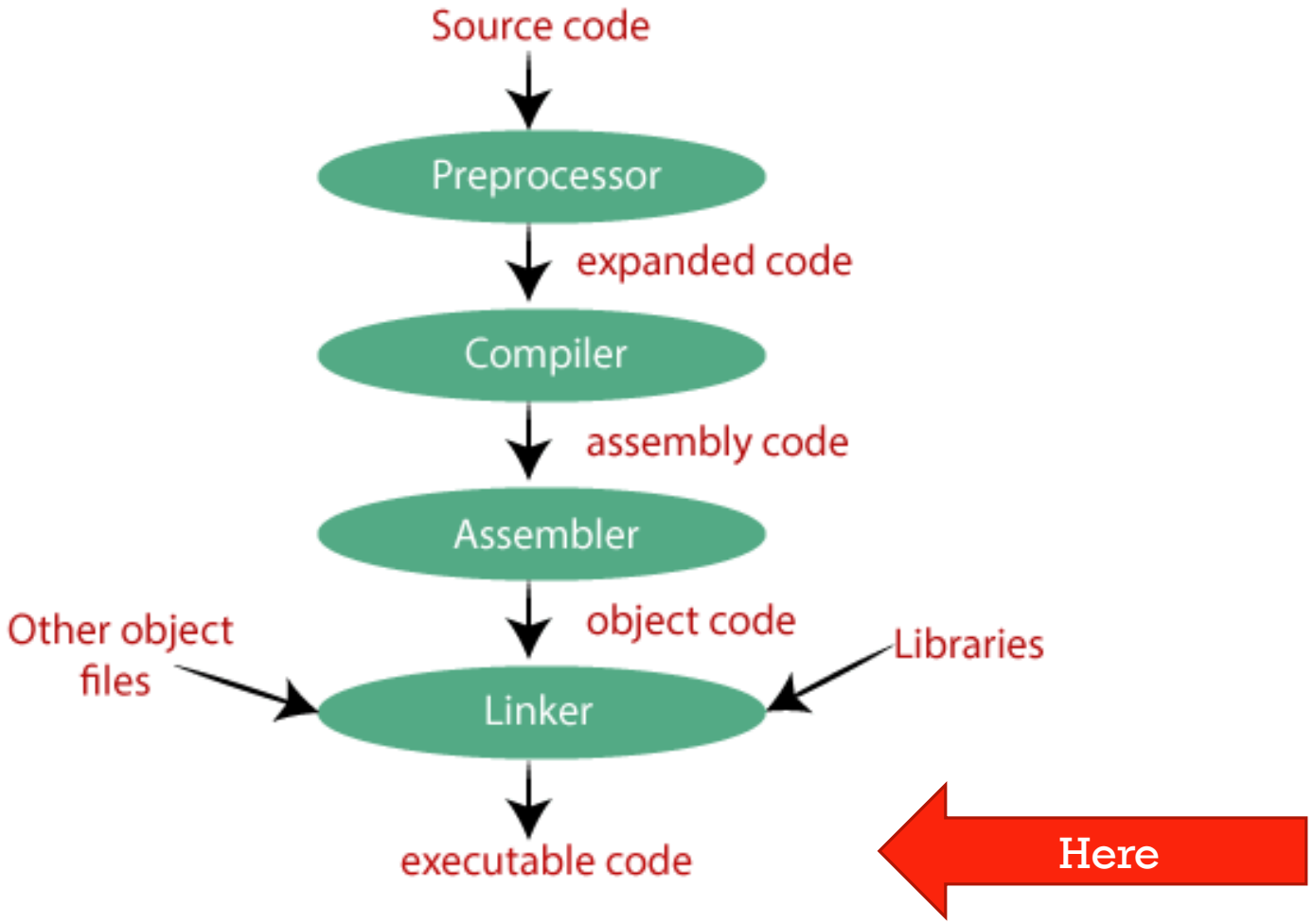
Linker

- همه فایلهای مورد نیاز به برنامه رو لینک کرده و خروجی نهایی که فایل اجرایی هست میده
- ورودی این مرحله فایل obj. و خروجی اون exe.
- دستور این مرحله :

Link code.obj

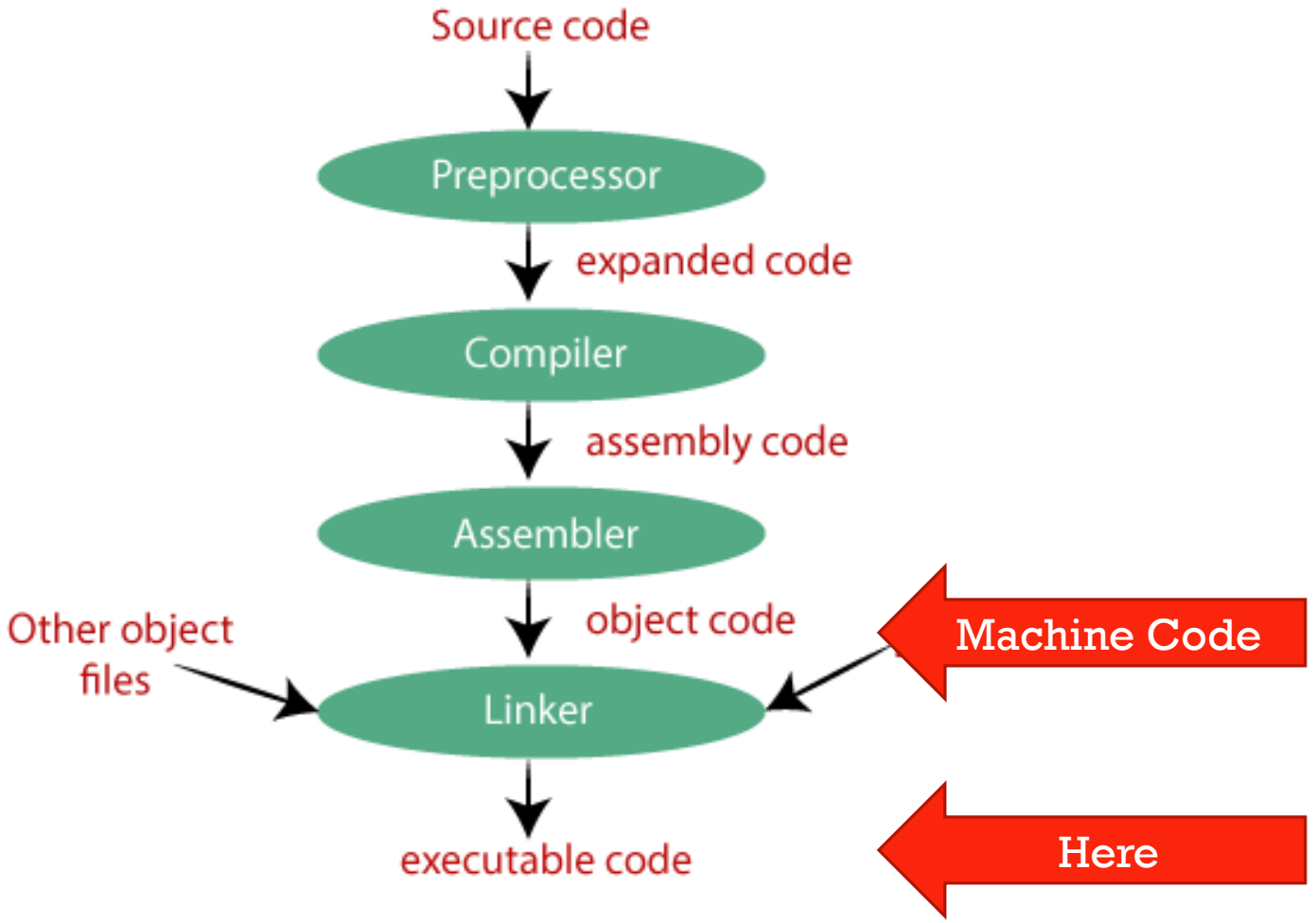
Onhexgroup.ir

اهمیت یادگیری اسمبلی



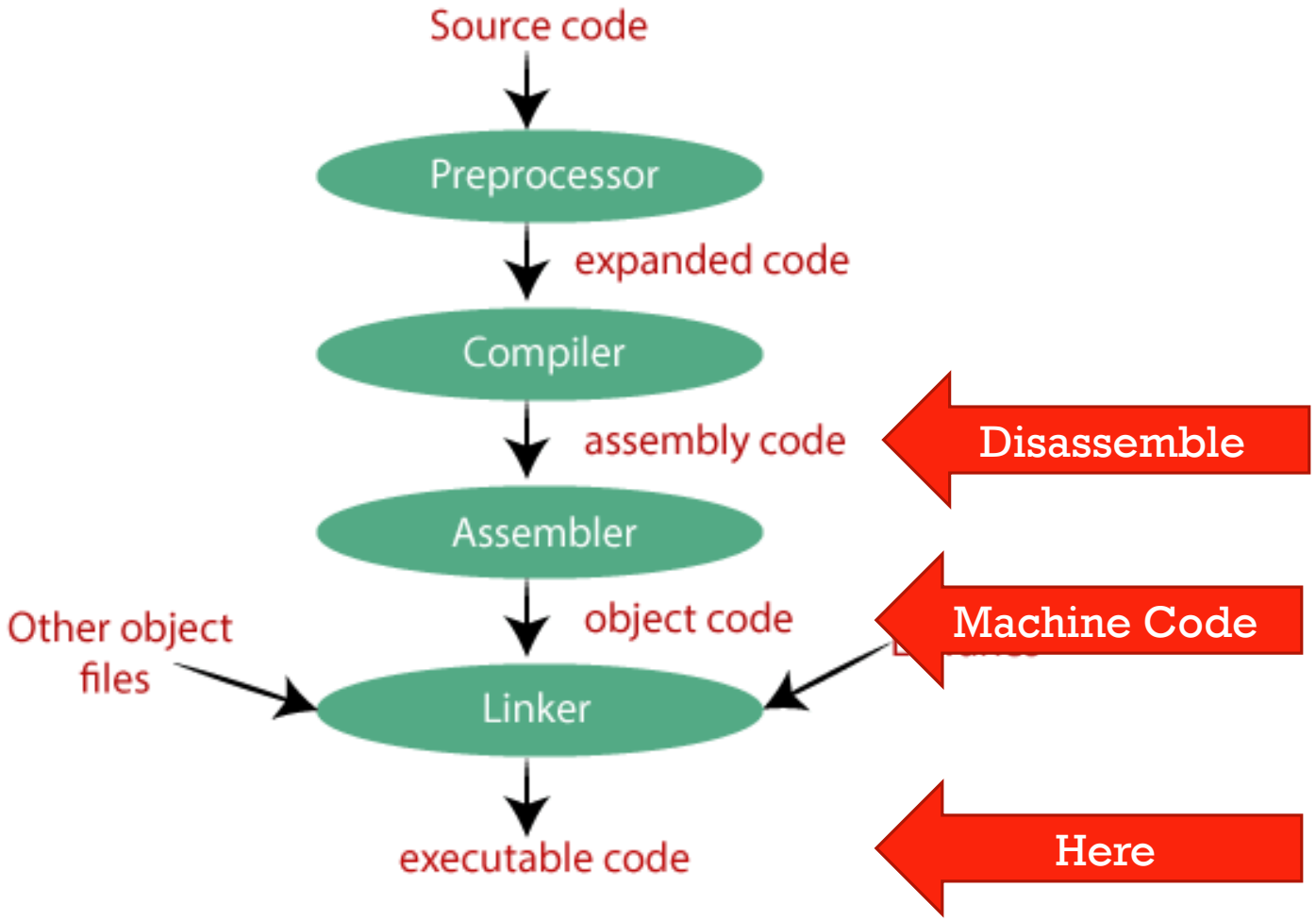
Onhexgroup.ir

اهمیت یادگیری اسمبلی



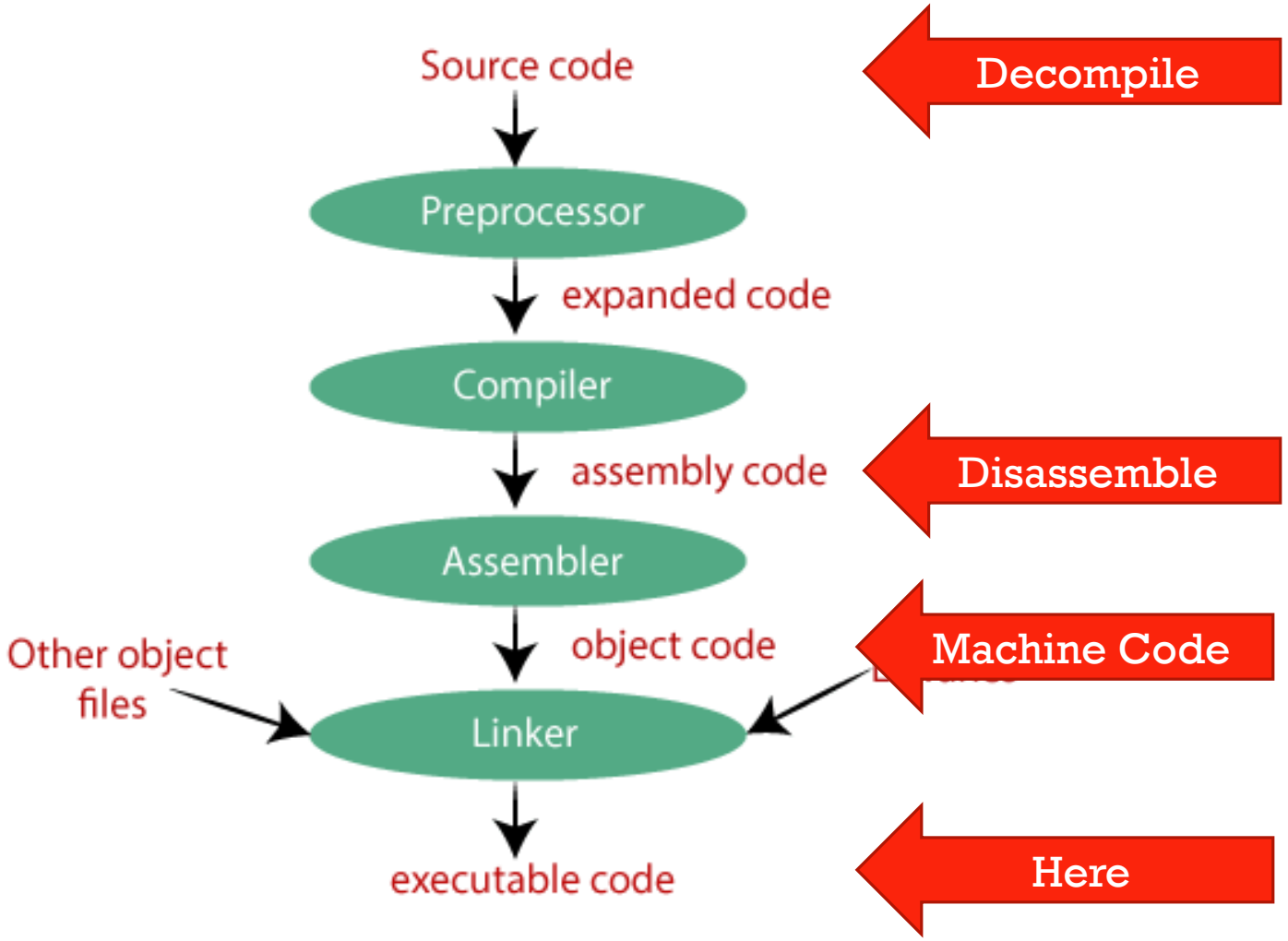
Onhexgroup.ir

اهمیت یادگیری اسمبلی



Onhexgroup.ir

اهمیت یادگیری اسمبلی



Onhexgroup.ir

منابع

- https://learn.microsoft.com/en-us/cpp/build/walkthrough-compile-a-c-program-on-the-command-line?view=msvc-170
- https://www.studytonight.com/c/c-compilation-process.php
- https://en.wikipedia.org/wiki/Object_file
- https://www.chakray.com/programming-languages-types-and-features/