# **Assembly programming**

Cheat sheets

© Government of Canada

This document is the property of the Government of Canada. It shall not be altered, distributed beyond its intended audience, produced, reproduced or published, in whole or in any substantial part thereof, without the express permission of CSE.





# NASM assembler instruction quick reference

Instruction	Description
db	Data byte is used when declaring variables
dw	Data word is used when declaring variables
dd	Data double is used when declaring variables
dq	Data quad is used when declaring variables
align XX	Can be used before just about anything to force alignement on XX bytes
extern X	Used to indicate that a function is external to the file
global	Makes a symbol available to the linked (ex: global main)
section	Start a new section (ex: section .text)

# NASM command line quick reference

Option	Description
-f	Choose a format. Use "-f elf" for 32 bits and "-f elf64" for 64 bits.
-0	Use to select a name for the output file. Ex: "-o outFileName"



## Clang command line quick reference

Option	Description
-m32	Used on 64 bits system to cross compile to 32 bits.
-0	Use to select a name for the output file. Ex: "-o outFileName"



# **GDB** general command quick reference

Command	Description
break	Set a breakpoint on a label. Ex: "break main". If no label information is available, you can use an address as: "break *0x040000"
nexti	Use to single step to the next instruction no matter what that instruction is.
info reg	Display all registers information. This can also be used as: "info reg eax" to display info for specific registers.
set disassembly- flavor intel	Switch the disassembly syntax from AT&T to intel.
layout asm	Set a split view with auto follow of ASM code (fun).

## **GDB** data inspection quick reference

"x /FormatSize address" is used for data inspection.

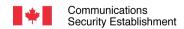
The format is defined as a number followed by a type. The number indicates how many "size" are to be printed in a specific format.

Frequent format: x (hexadecimal), c (char), a (address), f (float)

Possible sizes are: b (byte), h (halfword), w(word), g (giant) <- this is 8 bytes

#### Examples:

- x /4xb 0x20 (prints 4 bytes in hexadecimal from address 0x20)
- x /4xw \$esp (prints 4 words in hexadecimal from esp)





## **GNU** assembler (ARM) quick reference

Instruction	Description
.byte	Data byte is used when declaring variables
.hword (.2byte)	Data half word (16 bits) is used when declaring variables
.word (.4byte)	Data word (32 bits) is used when declaring variables
.8byte	8 bytes is used when declaring variables
.align XX	Can be used before just about anything to force alignement on XX bytes
.extern X	Used to indicate that a function is external to the file
.global	Makes a symbol available to the linked (ex: .global main)
.section	Start a new section (ex: .section .text)
.asciz	Zero terminated string

