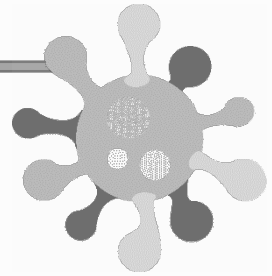
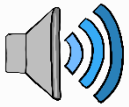
Exercice: endianness



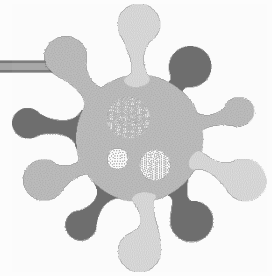
Vérifiez l'endianness de votre machine avec le programme testEndianness.c (voir les slides du cours).

Visualisez l'affiche d'une zone mémoire comme un tableau et comme un nombre à l'aide du programme myArray.c. Expliquez la difference et analysez comment le programme fonctionne.

	3	2	1	0		
EBP-C	D	C	B	A	->	0x44434241
EBP-8	H	G	F	E	->	0x48474645
EBP-4	L	K	J	I	->	0x00004a49



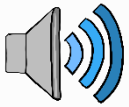
Exercice: reverse statique



Trouvez le mot de passe dans le fichier **reverse1** et **reverse2** à l'aide de Ghidra.

Manipuler le binaire **jump** dans Ghidra pour que l'outil affiche le code C le plus proche possible du code source **jump.c**.

Google pour trouver comment avoir le même code



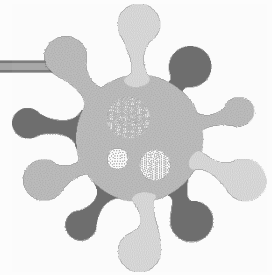
Exercice: analyse de la stack

Trouvez le mot de passe et le serial dans **jumpMania**, **functions1** et **functions2** à l'aide de Ghidra… et illustrez l'utilisation de la pile

Functions - 24 items

Label	Location	Function Signature	Fu...
_init	0804830c	int _init(EVP_PKEY_CTX * ctx)	35
FUN_08048330	08048330	undefined FUN_08048330()	12
puts	08048340	thunk int puts(char * __s)	6
strlen	08048350	thunk size_t strlen(char * __s)	6
__libc_start_main	08048360	thunk undefined __libc_start_main()	6
__isoc99_scanf	08048370	thunk undefined __isoc99_scanf()	6
__gmon_start__	08048380	thunk undefined __gmon_start__()	6
_start	08048390	undefined _start()	51
__i686.get_pc_thunk....	080483c3	undefined __i686.get_pc_thunk.bx()	4
_dl_relocate_static_pie	080483d0	undefined _dl_relocate_static_pie()	2
__x86.get_pc_thunk.bx	080483e0	undefined __x86.get_pc_thunk.bx()	4
deregister_tm_clones	080483f0	undefined deregister_tm_clones()	41
register_tm_clones	08048430	undefined register_tm_clones()	54
__do_global_dtors_aux	08048470	undefined __do_global_dtors_aux()	31
frame_dummy	080484a0	undefined frame_dummy()	6
main	080484a6	undefined main(undefined1 param_1)	288
__libc_csu_init	080485d0	undefined __libc_csu_init(undefined4 param_1, ...	93
__libc_csu_fini	08048630	undefined __libc_csu_fini()	2
_fini	08048634	undefined _fini()	20
puts	0804b000	thunk int puts(char * __s)	1
__gmon_start__	0804b004	thunk undefined __gmon_start__()	1
strlen	0804b008	thunk size_t strlen(char * __s)	1
__libc_start_main	0804b00c	thunk undefined __libc_start_main()	1
__isoc99_scanf	0804b010	thunk undefined __isoc99_scanf()	1

Exercice: reverse dynamique



Trouver le mot de passe dans le binaire **gdb**:

- commencer par une analyse statique dans ghidra et trouver où l'analyse dynamique deviant necessaire
- utiliser le debugger GDB pour révéler les caractères du mot de passe l'un après l'autre
- **gdb_test** est une version simplifiée pour "se faire la main"