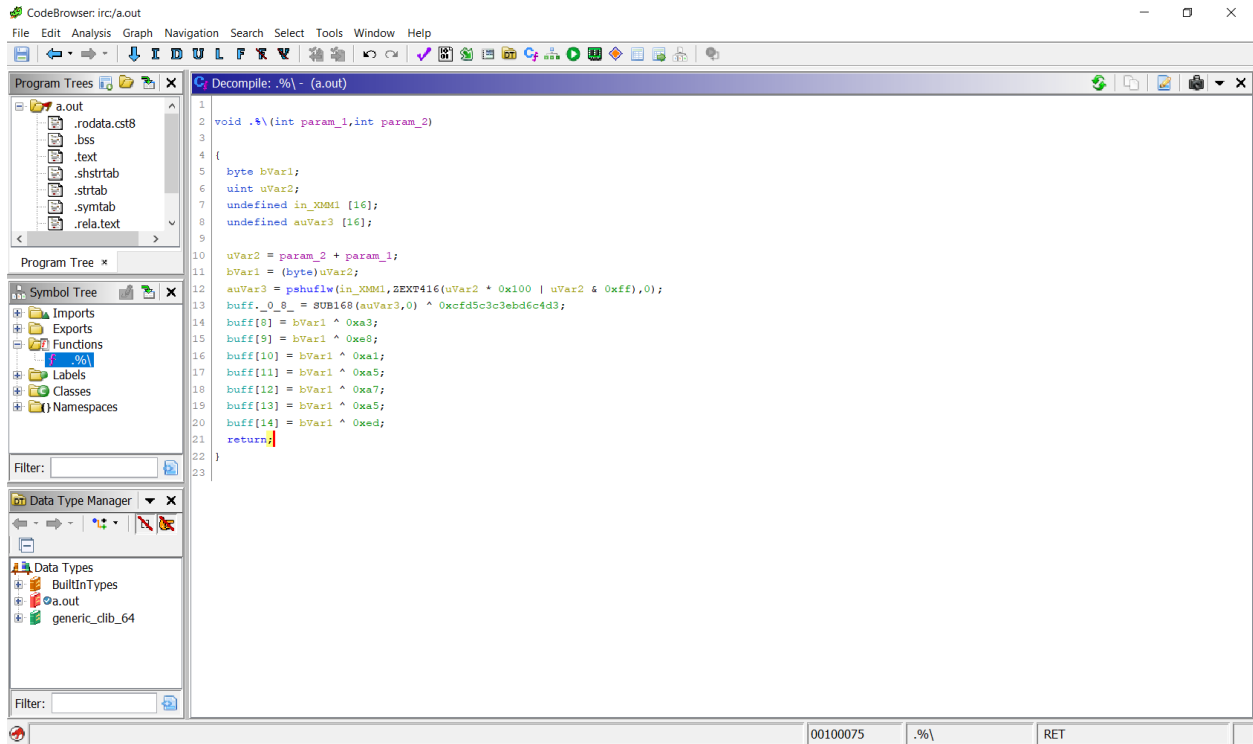


xxd -r elf.txt > a.out

ghidra a.out



Python:

```
buff = [None]*7
```

```
buff[0] = 0x90 ^ 0xa3;
```

```
buff[1] = 0x90 ^ 0xe8;
```

```
buff[2] = 0x90 ^ 0xa1;
```

```
buff[3] = 0x90 ^ 0xa5;
```

```
buff[4] = 0x90 ^ 0xa7;
```

```
buff[5] = 0x90 ^ 0xa5;
```

```
buff[6] = 0x90 ^ 0xed;
```

```
flag2 = ''.join([chr(i) for i in buff])
```

```
print flag2
```

v2 = 0x90

v3 = v2*0x100|v2&0xff

print hex(v3)

flag1 = hex(0x9090909090909090^0xcfd5c3c3ebd6c4d3)[2:-1].decode('hex')[::-1]

print flag1+flag2

The screenshot shows a MobaXterm terminal window with a file explorer on the left. The terminal output shows the execution of a Python script 'dec.py' which processes a hex string and outputs a flag. The flag is 'CTF{SSE_3x1575}'. The terminal also shows the execution of 'strings a.out' and 'python dec.py' commands.

```
buff
.syntab
.strtab
.shstrtab
.rela.text
.data
.bss
.rodata.cst8
szhan21@szhan21-NUC:~/ctf/monthly_security_challenge/re$ vi dec.py
szhan21@szhan21-NUC:~/ctf/monthly_security_challenge/re$ strings a.out
sse.c
.LC0
buff
.syntab
.strtab
.shstrtab
.rela.text
.data
.bss
.rodata.cst8
szhan21@szhan21-NUC:~/ctf/monthly_security_challenge/re$ python dec.py
3x1575}
0x9090

szhan21@szhan21-NUC:~/ctf/monthly_security_challenge/re$ vi dec.py
szhan21@szhan21-NUC:~/ctf/monthly_security_challenge/re$ python dec.py
3x1575}
0x9090
4cd 551
szhan21@szhan21-NUC:~/ctf/monthly_security_challenge/re$ vi dec.py
szhan21@szhan21-NUC:~/ctf/monthly_security_challenge/re$ python dec.py
3x1575}
0x9090
CTF{SSE
szhan21@szhan21-NUC:~/ctf/monthly_security_challenge/re$ vi dec.py
szhan21@szhan21-NUC:~/ctf/monthly_security_challenge/re$ python dec.py
3x1575}
0x9090
CTF{SSE_3x1575}
szhan21@szhan21-NUC:~/ctf/monthly_security_challenge/re$ vi dec.py
szhan21@szhan21-NUC:~/ctf/monthly_security_challenge/re$
```

Flag: CTF{SSE_3x1575}