ROP Gadgets

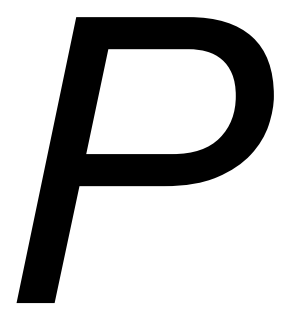
C A R P E T

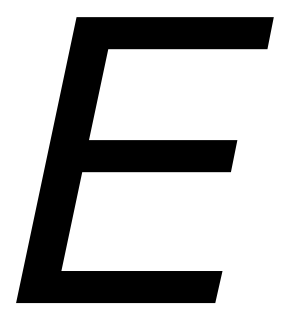
A D D R E S S

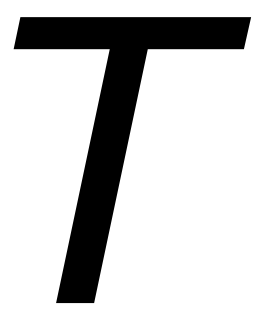
R I C E

E N G I N E E R I N G

F A C E B O O K

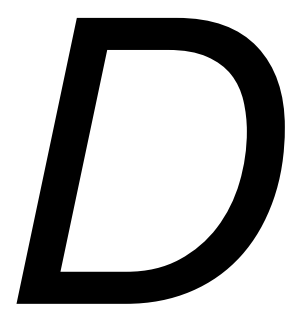


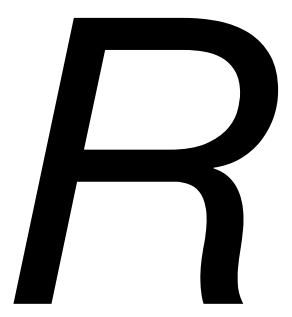


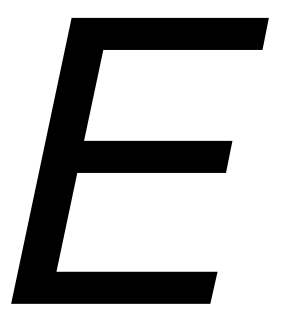


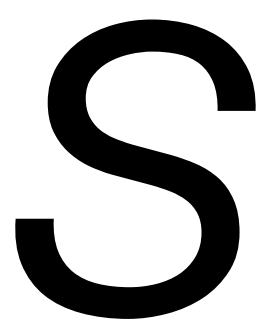
[redacted]

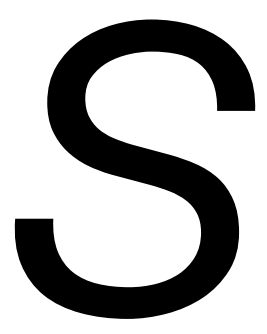
[redacted]

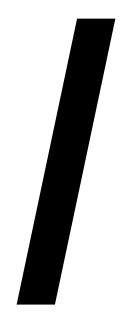


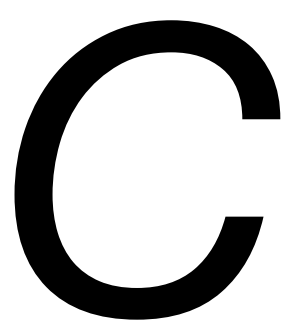


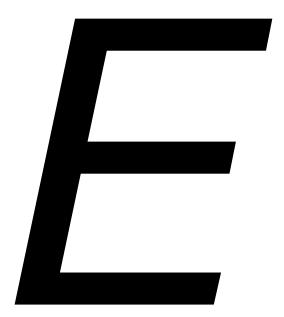


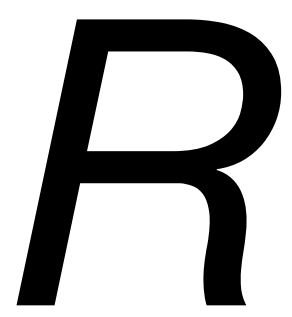


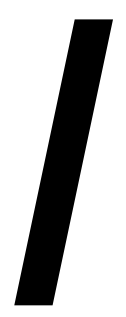


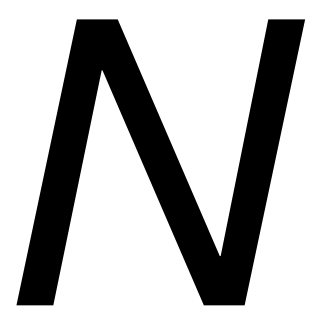


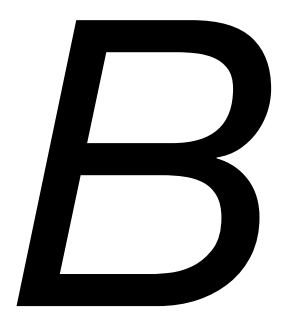


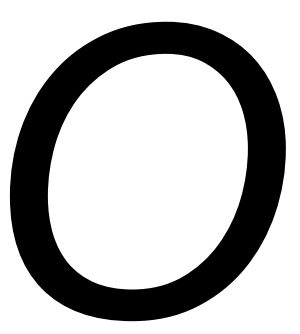


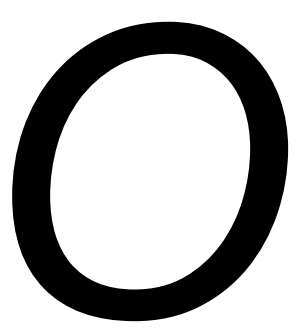


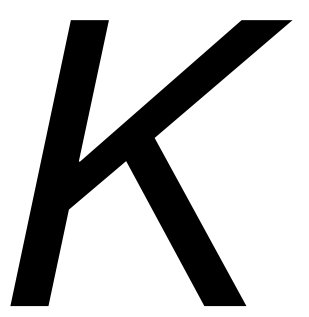








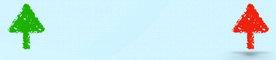




ROP Gadgets

C A R P E T = *P E T*

A D D R E S S = *D R E S S*



R I C E = *I C E*

E N G I N E E R I N G = *R I N G*

F A C E B O O K = *B O O K*

Byte Shift

- We can point the RIP (x64 bit instruction pointer register) to a location that contains a micro instruction that we want to execute followed by a ***RET***

```
f7 c7 07 00 00 00        test $0x00000007, %edi
0f 95 45 c3              setnzb -61(%ebp)
```