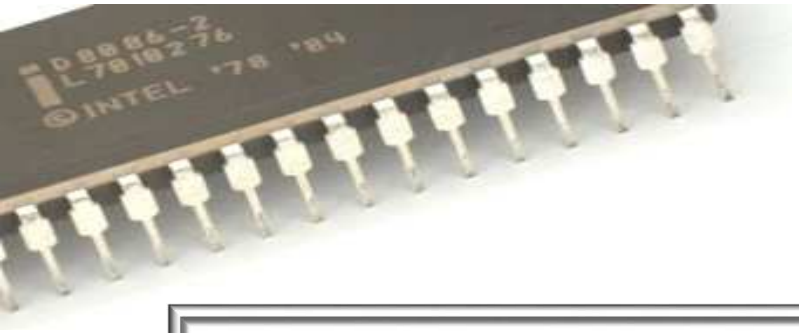
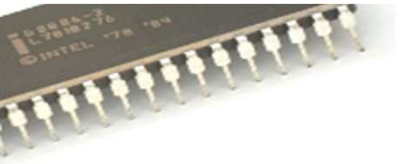


Calling a function in assembly

Dr. Varga, Imre

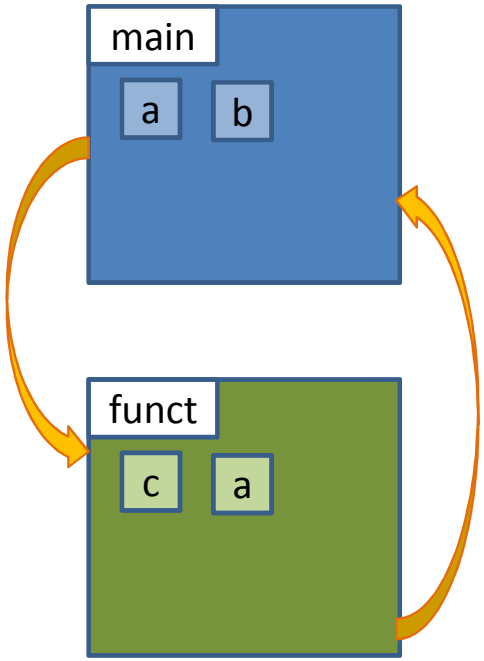
University of Debrecen

Department of IT Systems and Networks

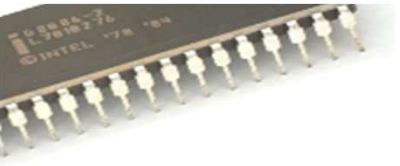


Example in C language

```
int funct(int c){
   int a;
   a=c+1;
   return a;
   }
int main(int argc, char *argv[]){
   int a, b;
   a=argc;
   b=funct(a);
   return b;
   }
```

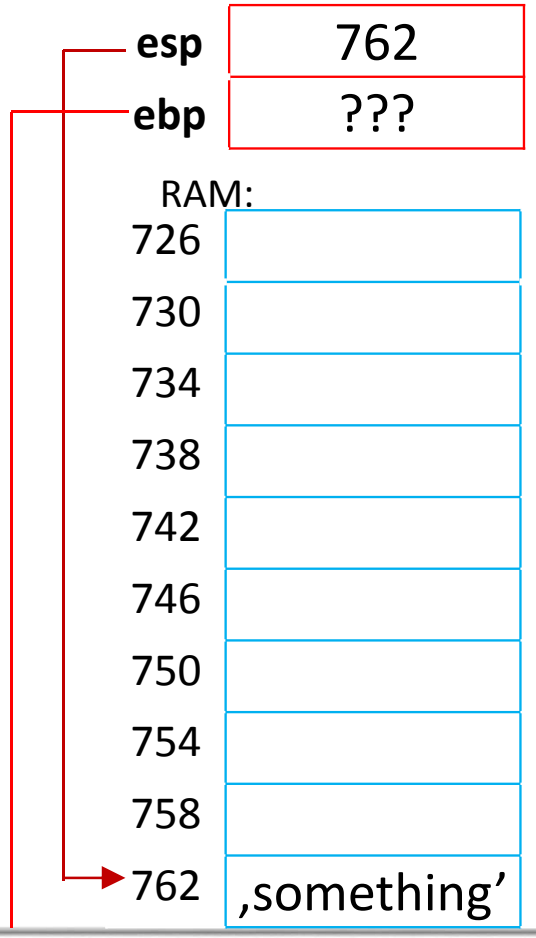



```
gcc prog.c -o prog
```

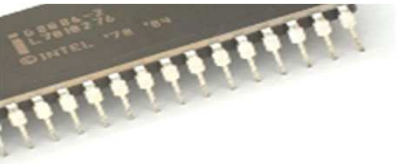


Example in assembly

Initial state at program launch:

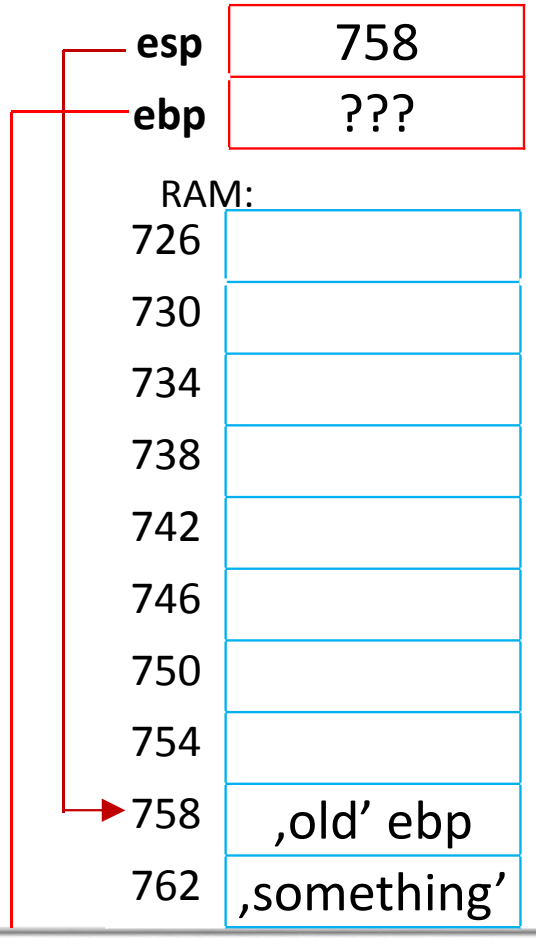



```
./prog
```

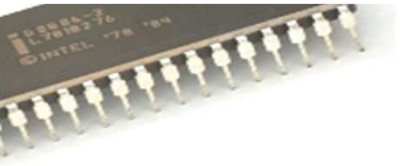


Example in assembly

```
main:    push    ebp
```

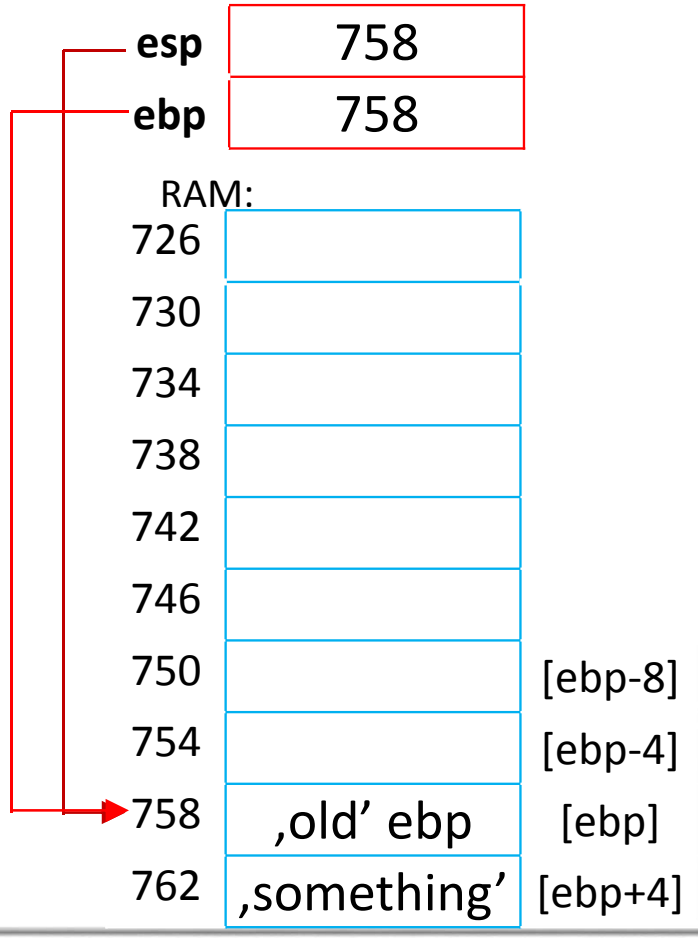



```
int main(){
```

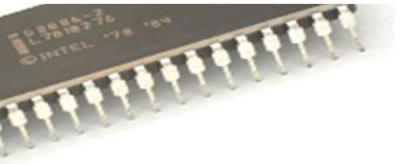


Example in assembly

```
main:    push    ebp
         mov     ebp, esp
```



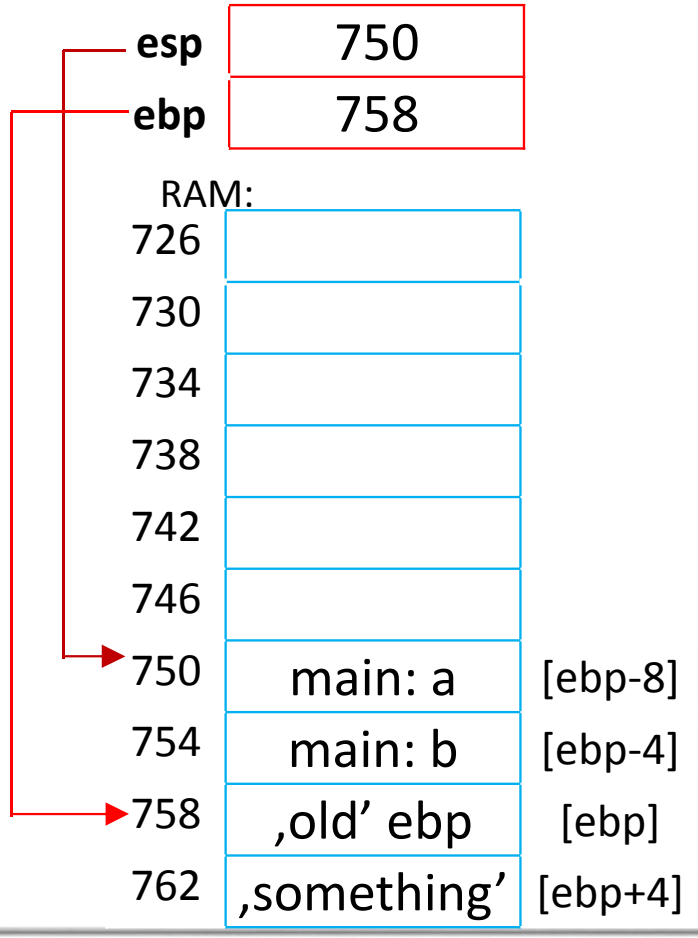

```
int main(){
```

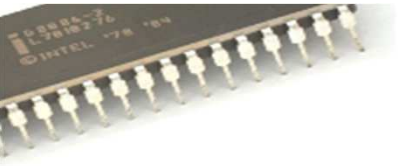


Example in assembly

```
main:   push    ebp
        mov     ebp, esp
        sub     esp, 8
```

```
int a, b;
```

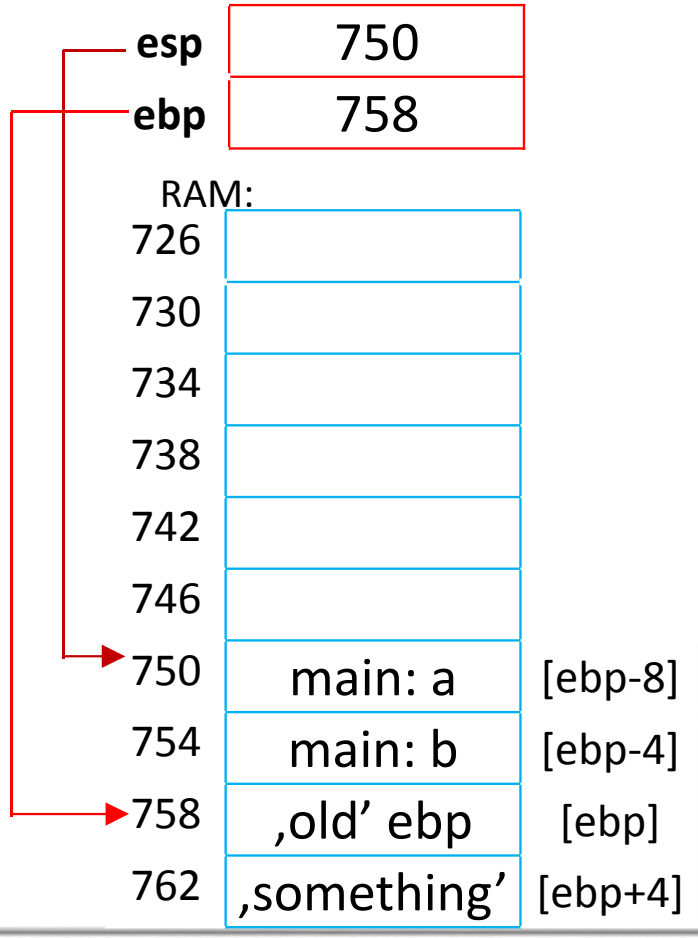


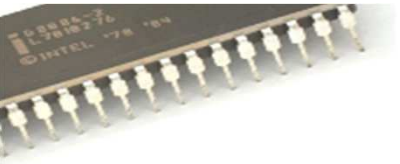


Example in assembly

```
main:    push    ebp
         mov     ebp, esp
         sub     esp, 8
         mov     DWORD PTR [ebp-8], edi
```

```
a=argc;
```

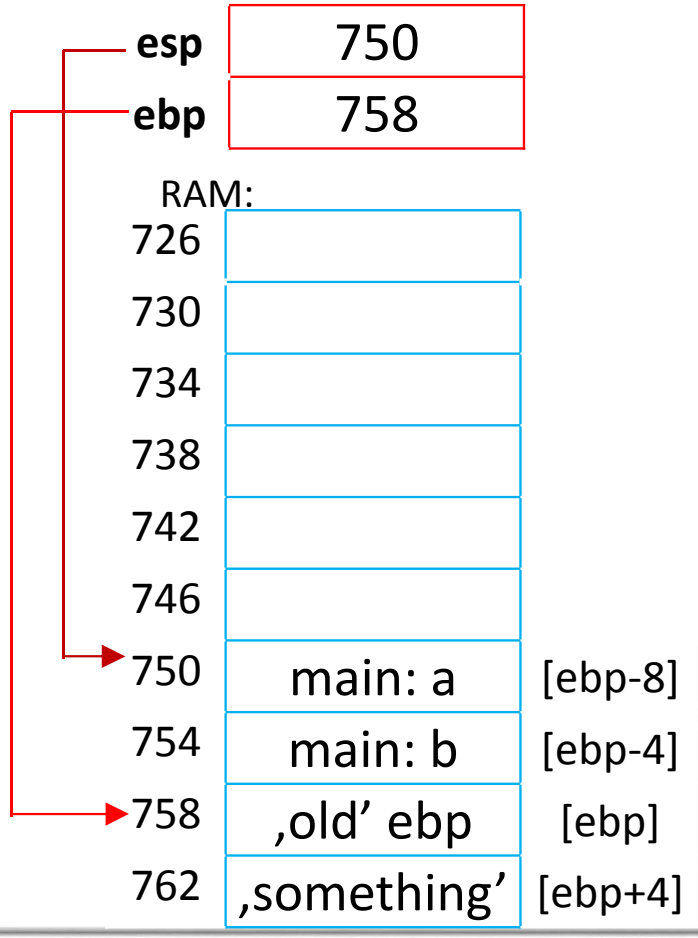


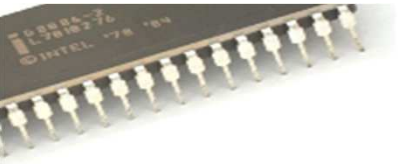


Example in assembly

```
main:    push    ebp
         mov     ebp, esp
         sub     esp, 8
         mov     DWORD PTR [ebp-8], edi
         mov     eax, DWORD PTR [ebp-8]
```

```
b=funct(a);
```

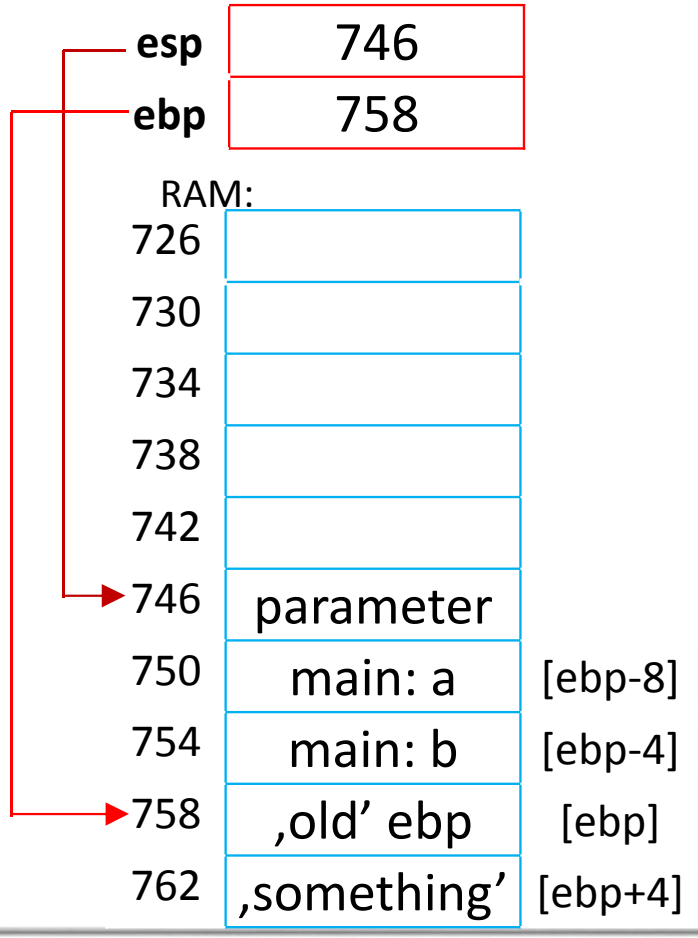


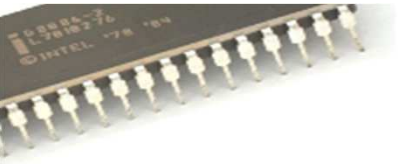


Example in assembly

```
main:    push    ebp
         mov     ebp, esp
         sub     esp, 8
         mov     DWORD PTR [ebp-8], edi
         mov     eax, DWORD PTR [ebp-8]
         push    eax
```

```
b=funct(a);
```

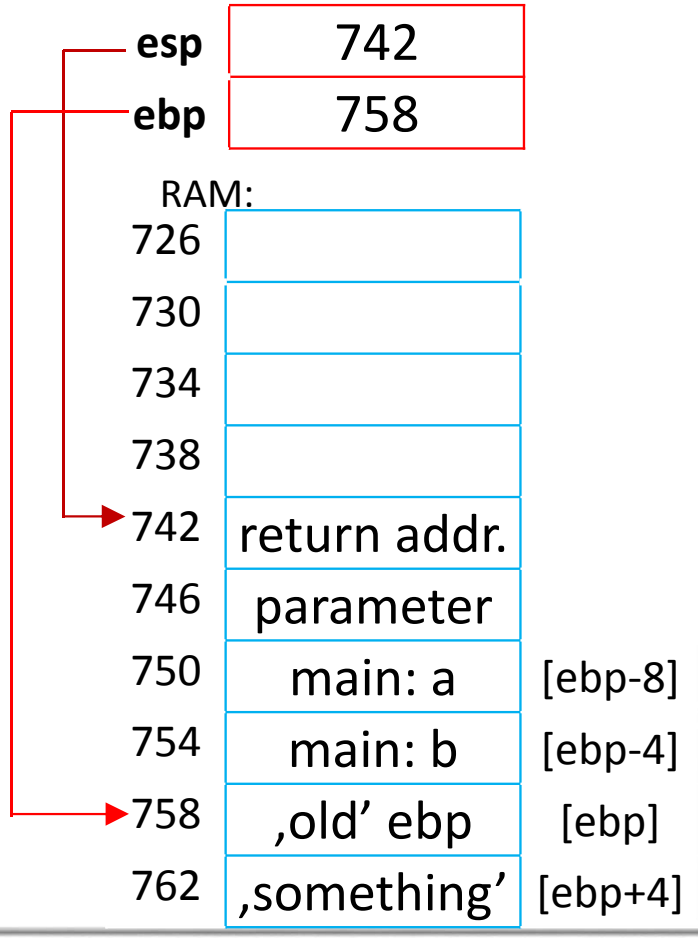


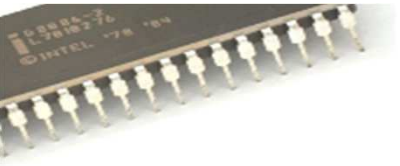


Example in assembly

```
main:   push    ebp
        mov     ebp, esp
        sub     esp, 8
        mov     DWORD PTR [ebp-8], edi
        mov     eax, DWORD PTR [ebp-8]
        push    eax
        call    funct
```

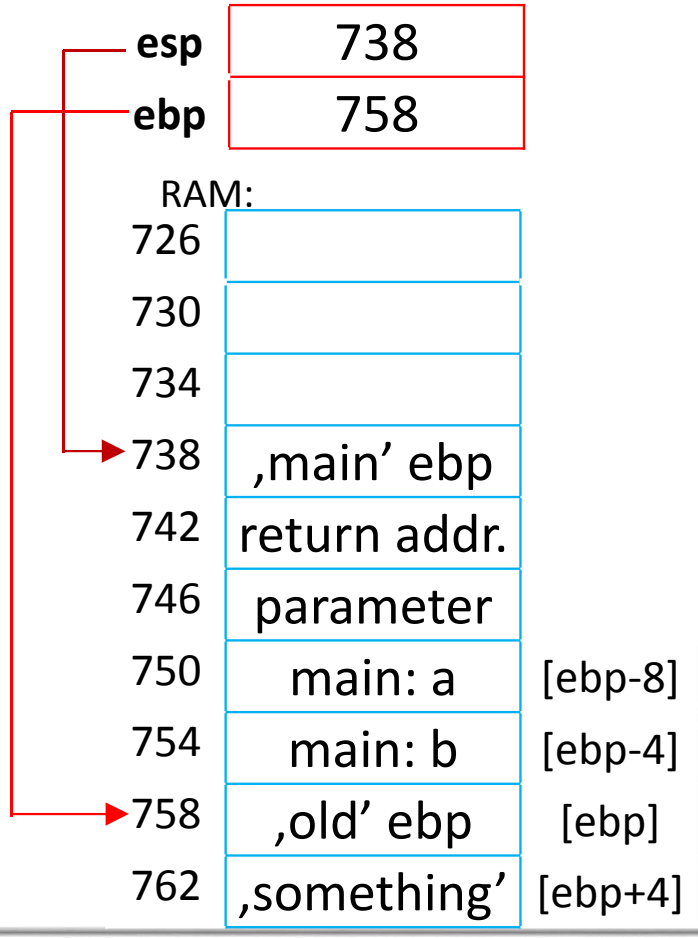
```
b=funct(a);
```



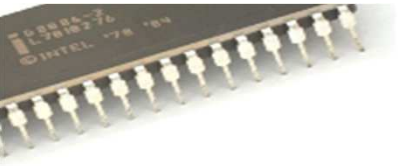


Example in assembly

```
funct:   push     ebp
```

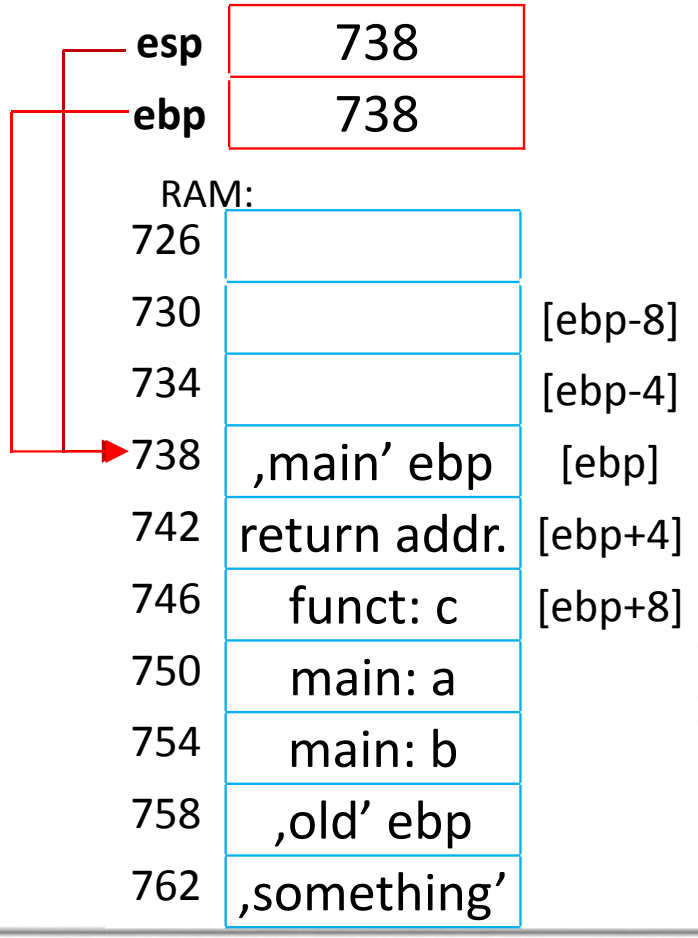



```
int funct(int c){
```

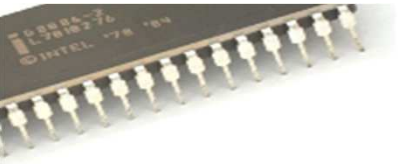


Example in assembly

```
funct:   push     ebp
         mov      ebp, esp
```

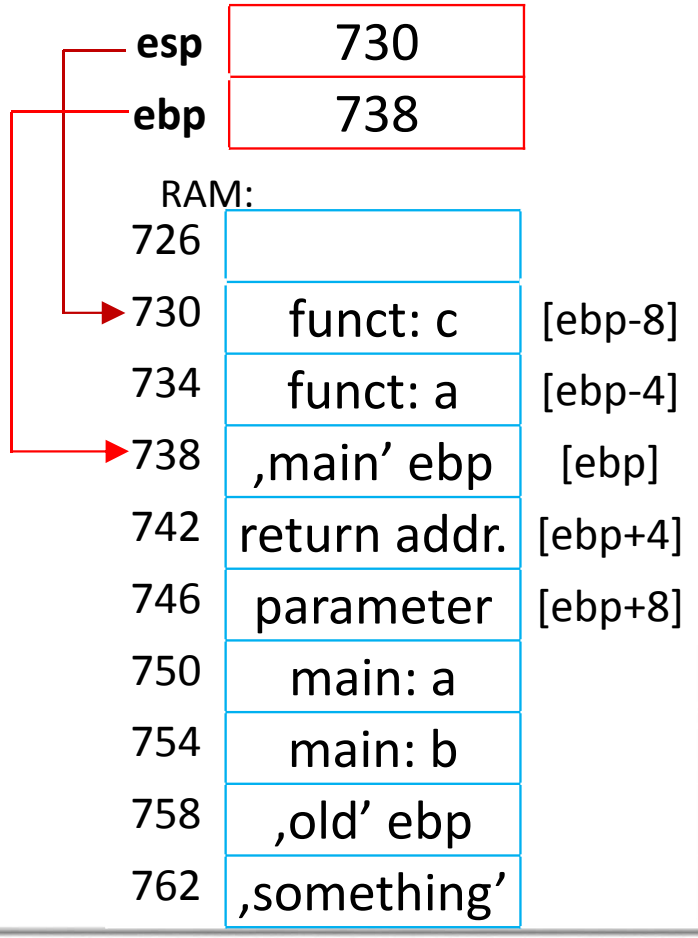



```
int funct(int c){
```

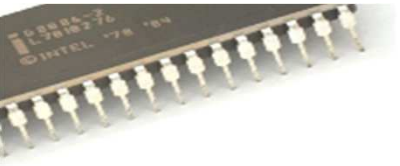


Example in assembly

```
funct:   push     ebp
         mov      ebp, esp
         sub      esp, 8
```

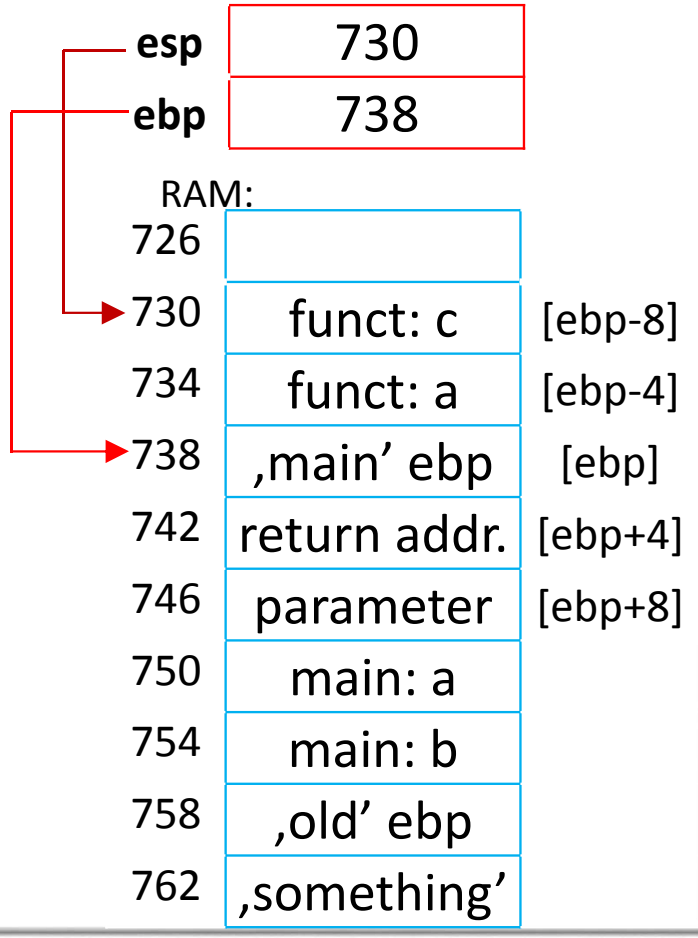



```
int funct(int c){ int a;
```

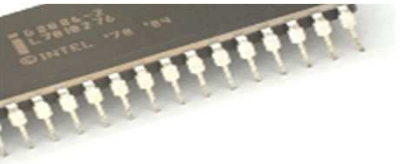


Example in assembly

```
funct:   push     ebp
         mov      ebp, esp
         sub      esp, 8
         mov      eax, DWORD PTR [ebp+8]
```



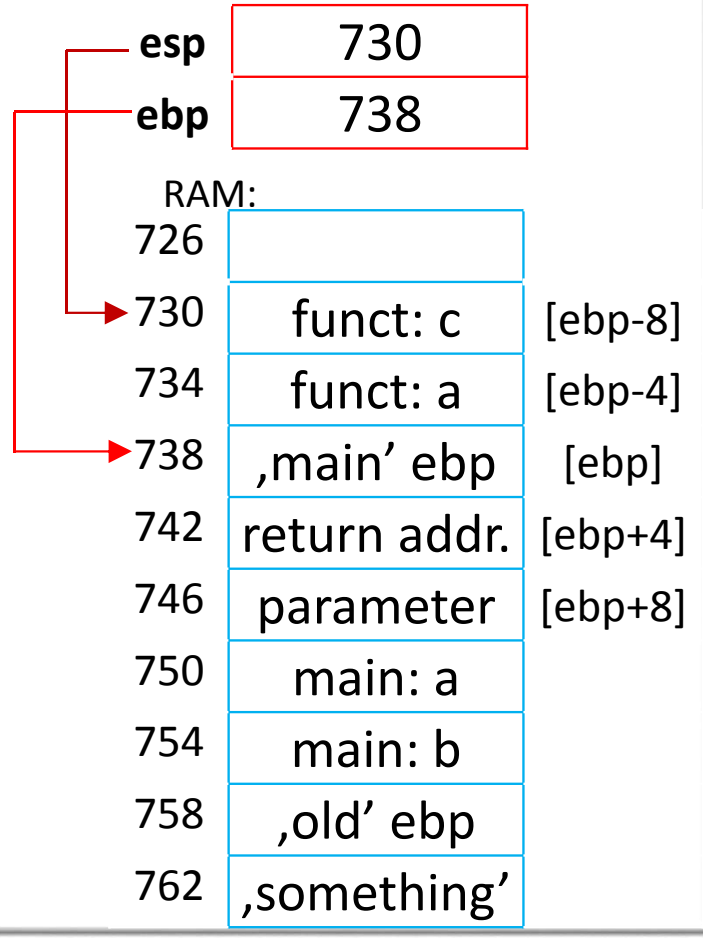

```
int funct(int c){
```

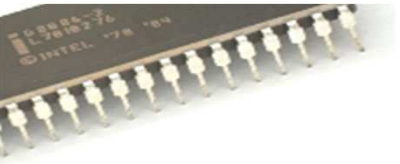


Example in assembly

```
funct:   push     ebp
         mov      ebp, esp
         sub      esp, 8
         mov      eax, DWORD PTR [ebp+8]
         mov      DWORD PTR [ebp-8], eax
```

```
int funct(int c){
```

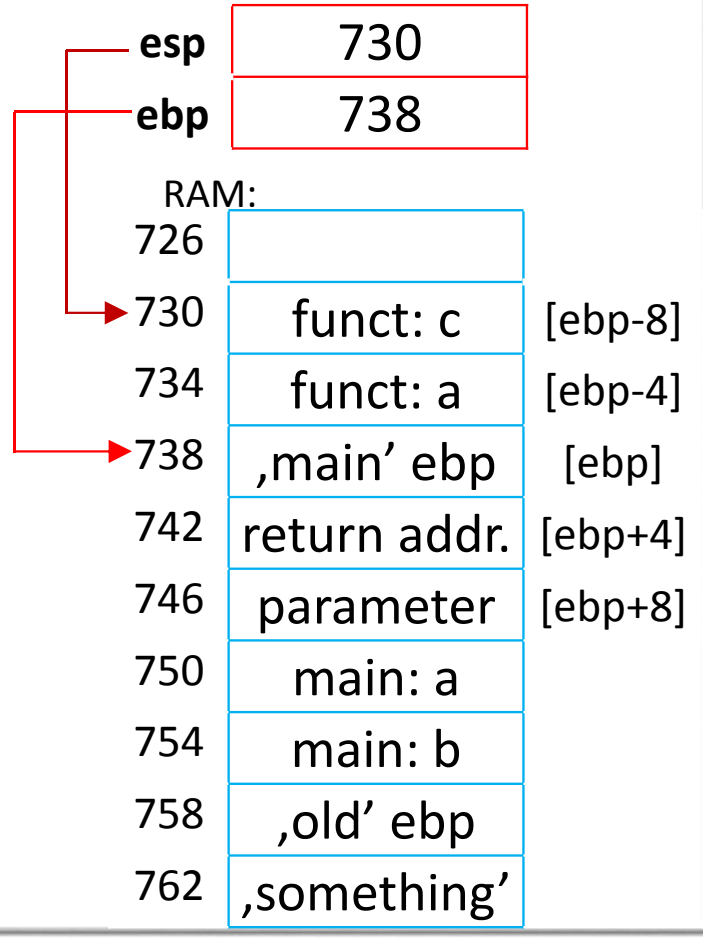


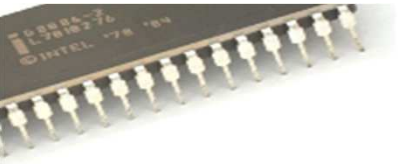


Example in assembly

```
funct:   push     ebp
         mov      ebp, esp
         sub      esp, 8
         mov      eax, DWORD PTR [ebp+8]
         mov      DWORD PTR [ebp-8], eax
         mov      eax, DWORD PTR [ebp-8]
```

```
a=c+1;
```

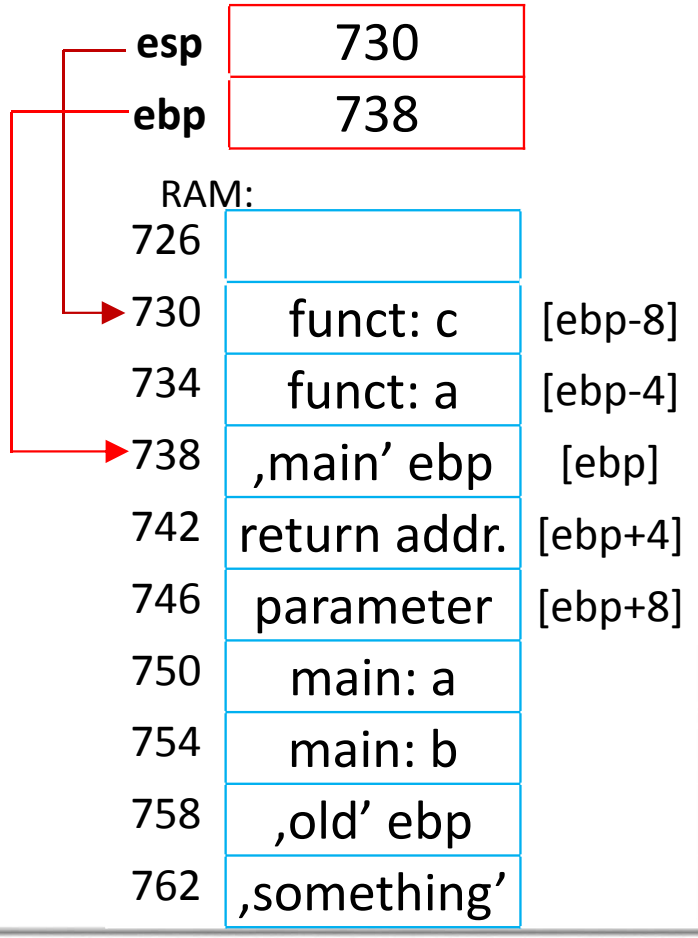


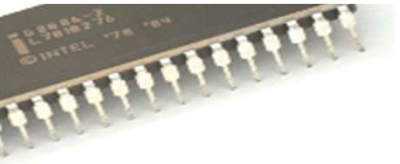


Example in assembly

```
funct:   push     ebp
         mov      ebp, esp
         sub      esp, 8
         mov      eax, DWORD PTR [ebp+8]
         mov      DWORD PTR [ebp-8], eax
         mov      eax, DWORD PTR [ebp-8]
         add      eax, 1
```

```
a=c+1;
```

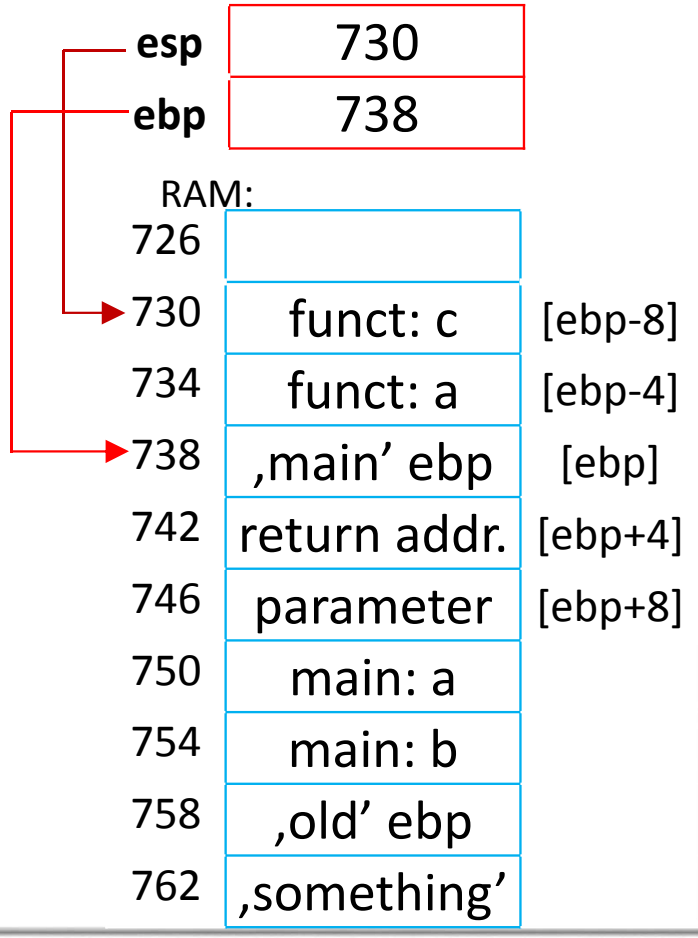


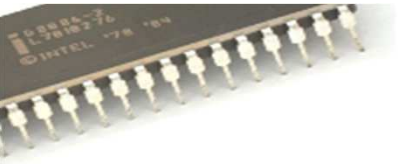


Example in assembly

```
funct:   push     ebp
         mov      ebp, esp
         sub      esp, 8
         mov      eax, DWORD PTR [ebp+8]
         mov      DWORD PTR [ebp-8], eax
         mov      eax, DWORD PTR [ebp-8]
         add      eax, 1
         mov      DWORD PTR [ebp-4], eax
```

```
a=c+1;
```

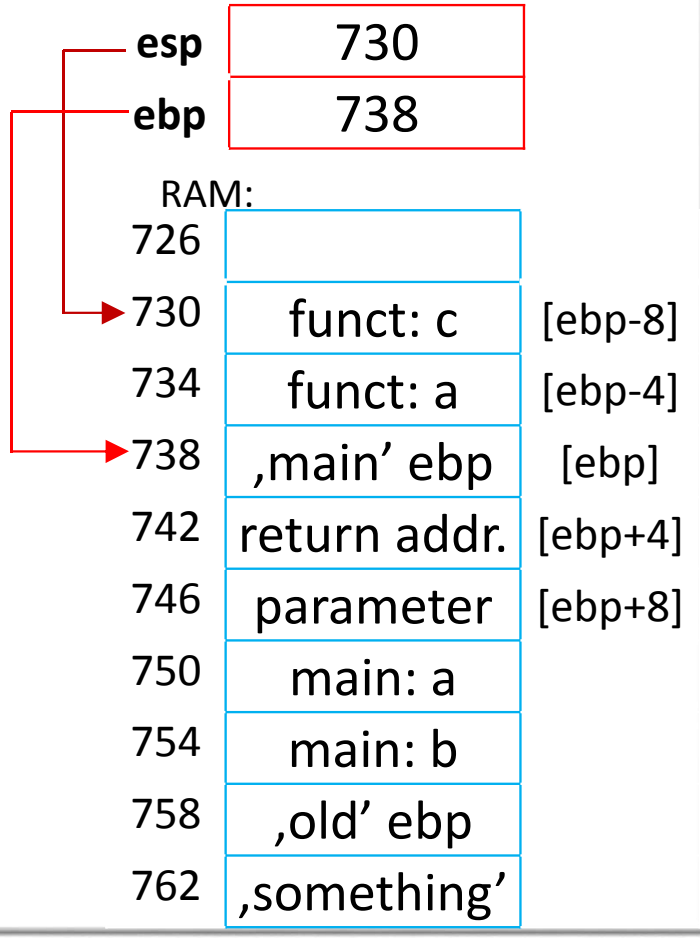


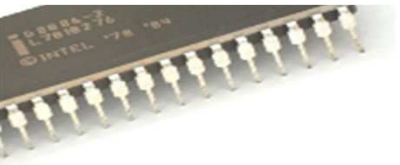


Example in assembly

```
funct:   push     ebp
         mov      ebp, esp
         sub      esp, 8
         mov      eax, DWORD PTR [ebp+8]
         mov      DWORD PTR [ebp-8], eax
         mov      eax, DWORD PTR [ebp-8]
         add      eax, 1
         mov      DWORD PTR [ebp-4], eax
         mov      eax, DWORD PTR [ebp-4]
```

```
return a;
```

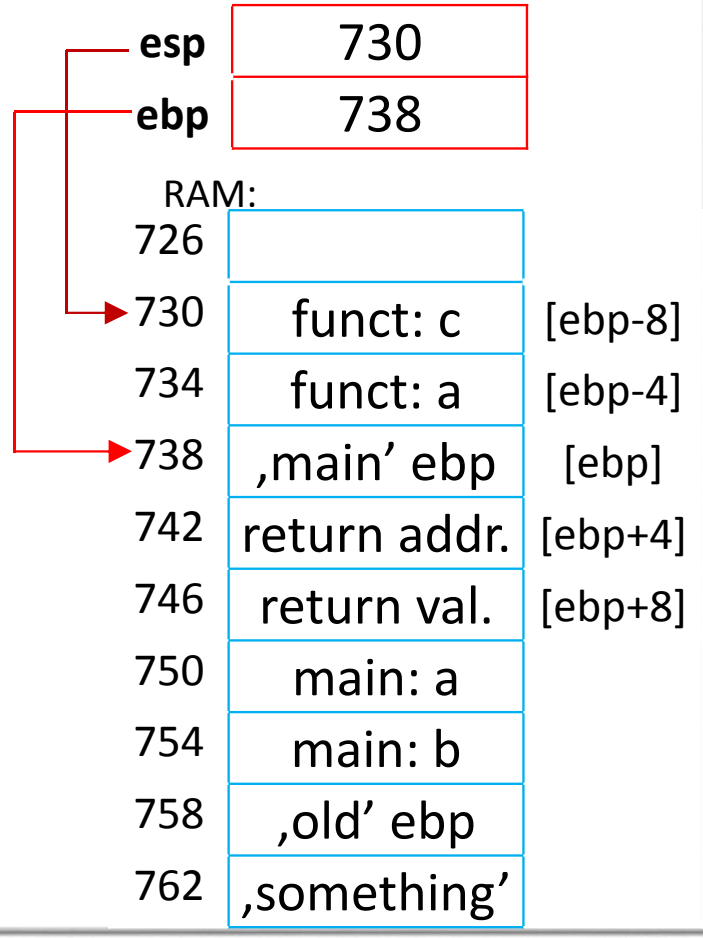


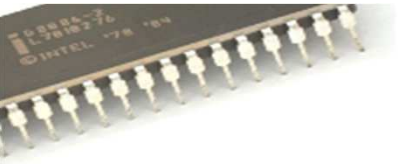


Example in assembly

```
funct:   push     ebp
         mov      ebp, esp
         sub      esp, 8
         mov      eax, DWORD PTR [ebp+8]
         mov      DWORD PTR [ebp-8], eax
         mov      eax, DWORD PTR [ebp-8]
         add      eax, 1
         mov      DWORD PTR [ebp-4], eax
         mov      eax, DWORD PTR [ebp-4]
         mov      DWORD PTR [ebp+8], eax
```

```
return a;
```

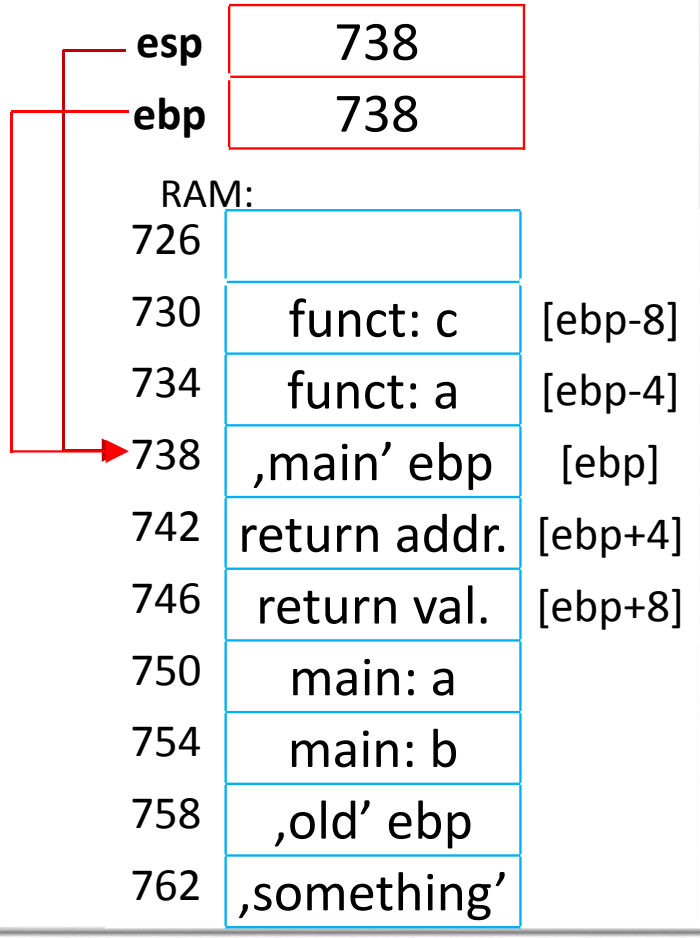


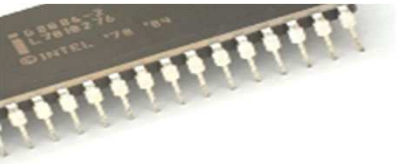


Example in assembly

```
funct:   push    ebp
         mov     ebp, esp
         sub     esp, 8
         mov     eax, DWORD PTR [ebp+8]
         mov     DWORD PTR [ebp-8], eax
         mov     eax, DWORD PTR [ebp-8]
         add     eax, 1
         mov     DWORD PTR [ebp-4], eax
         mov     eax, DWORD PTR [ebp-4]
         mov     DWORD PTR [ebp+8], eax
         mov     esp, ebp
```

```
return a;
```

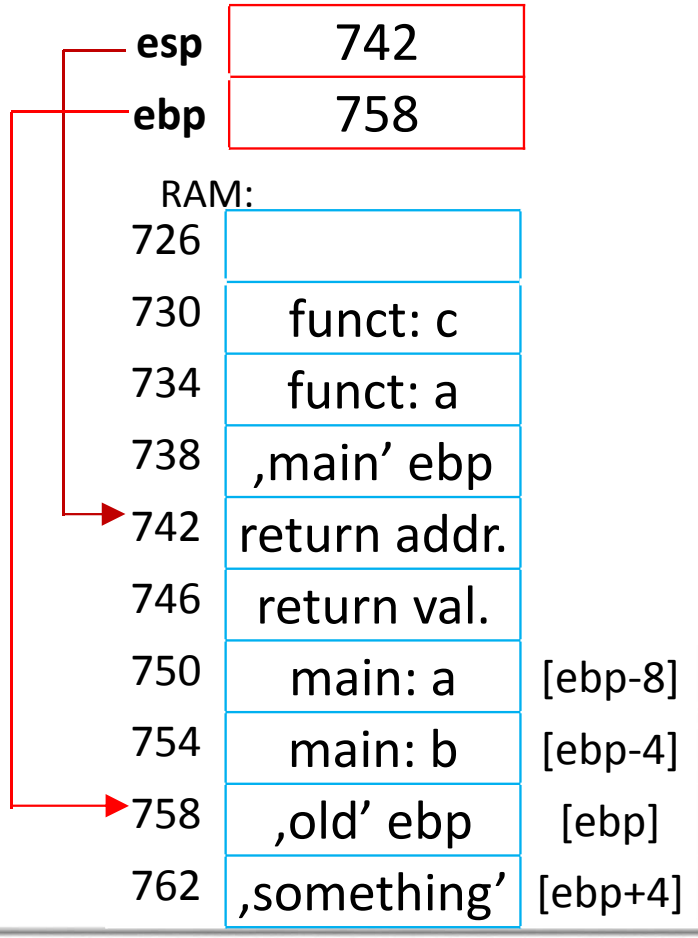


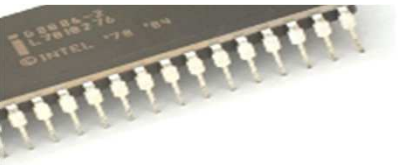


Example in assembly

```
funct:   push    ebp
         mov     ebp, esp
         sub     esp, 8
         mov     eax, DWORD PTR [ebp+8]
         mov     DWORD PTR [ebp-8], eax
         mov     eax, DWORD PTR [ebp-8]
         add     eax, 1
         mov     DWORD PTR [ebp-4], eax
         mov     eax, DWORD PTR [ebp-4]
         mov     DWORD PTR [ebp+8], eax
         mov     esp, ebp
         pop     ebp
```

```
return a;
```

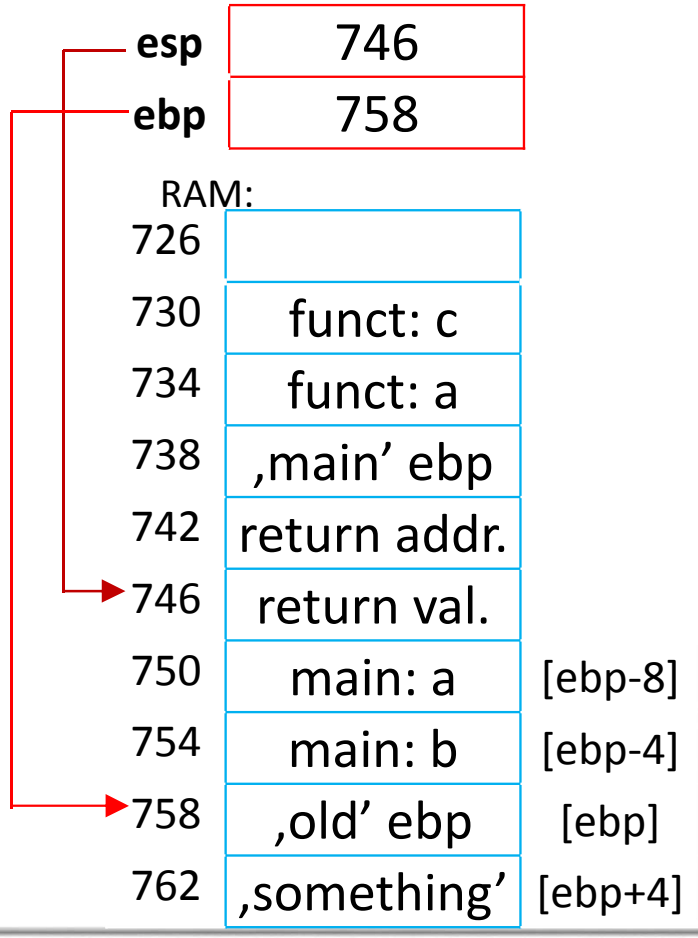


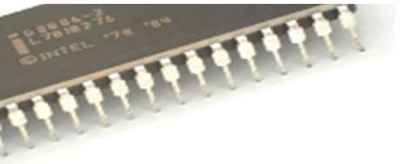


Example in assembly

```
funct:   push    ebp
         mov     ebp, esp
         sub     esp, 8
         mov     eax, DWORD PTR [ebp+8]
         mov     DWORD PTR [ebp-8], eax
         mov     eax, DWORD PTR [ebp-8]
         add     eax, 1
         mov     DWORD PTR [ebp-4], eax
         mov     eax, DWORD PTR [ebp-4]
         mov     DWORD PTR [ebp+8], eax
         mov     esp, ebp
         pop     ebp
         ret
```

```
return a;
```

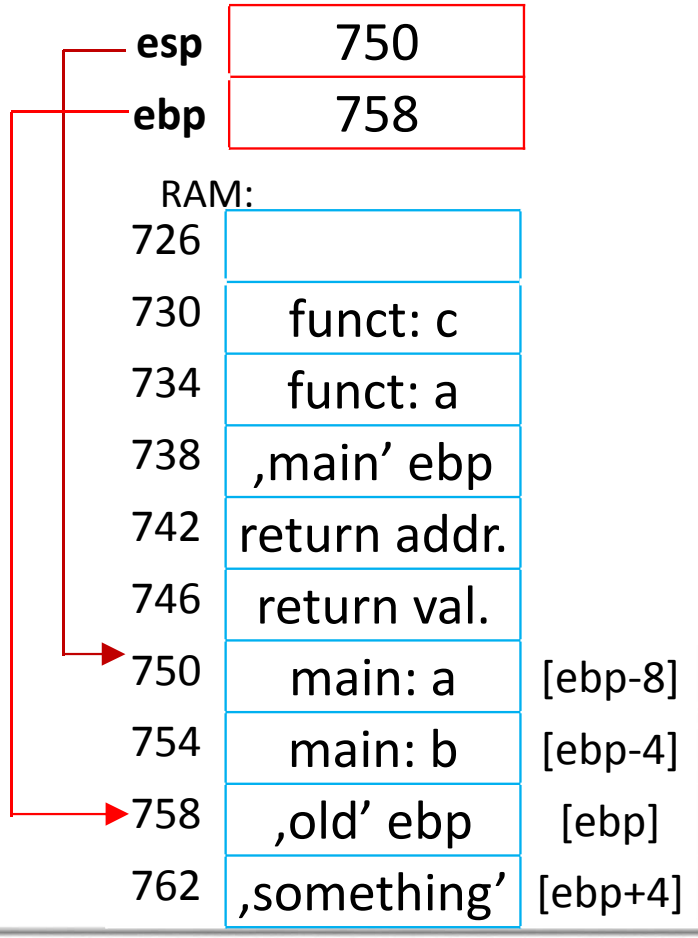


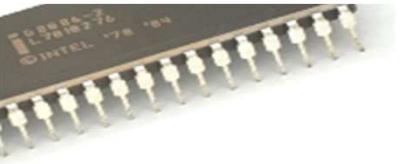


Example in assembly

```
main:   push    ebp
        mov     ebp, esp
        sub     esp, 8
        mov     DWORD PTR [ebp-8], edi
        mov     eax, DWORD PTR [ebp-8]
        push    eax
        call    funct
        pop     eax
```

```
b=funct(a);
```

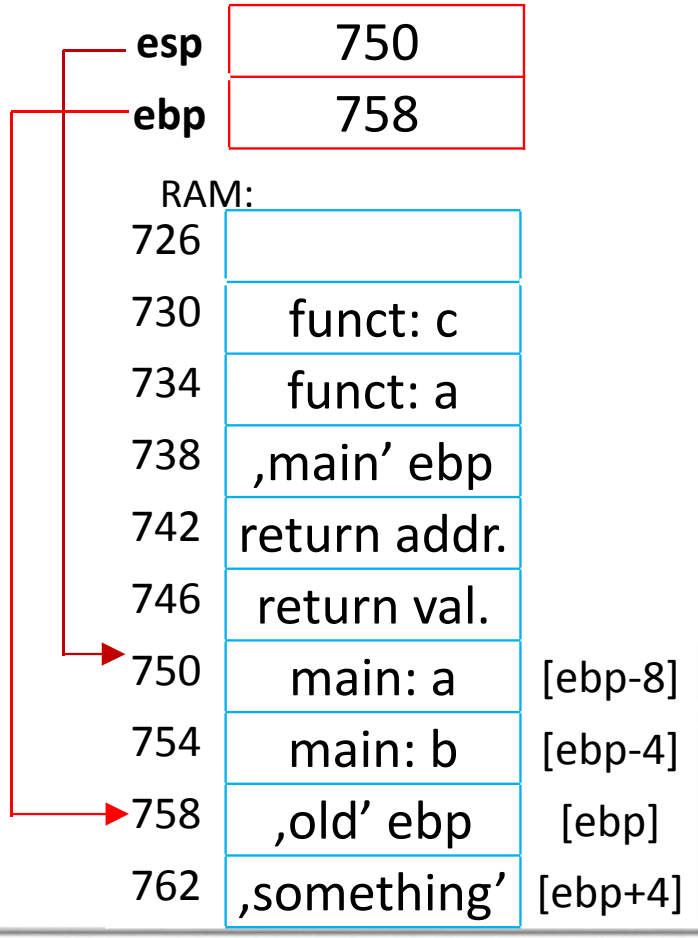


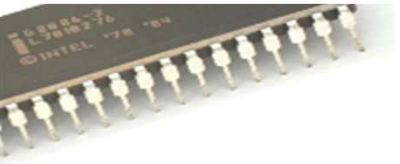


Example in assembly

```
main:    push    ebp
         mov     ebp, esp
         sub     esp, 8
         mov     DWORD PTR [ebp-8], edi
         mov     eax, DWORD PTR [ebp-8]
         push    eax
         call    funct
         pop     eax
         mov     DWORD PTR [ebp-4], eax
```

```
b=funct(a);
```

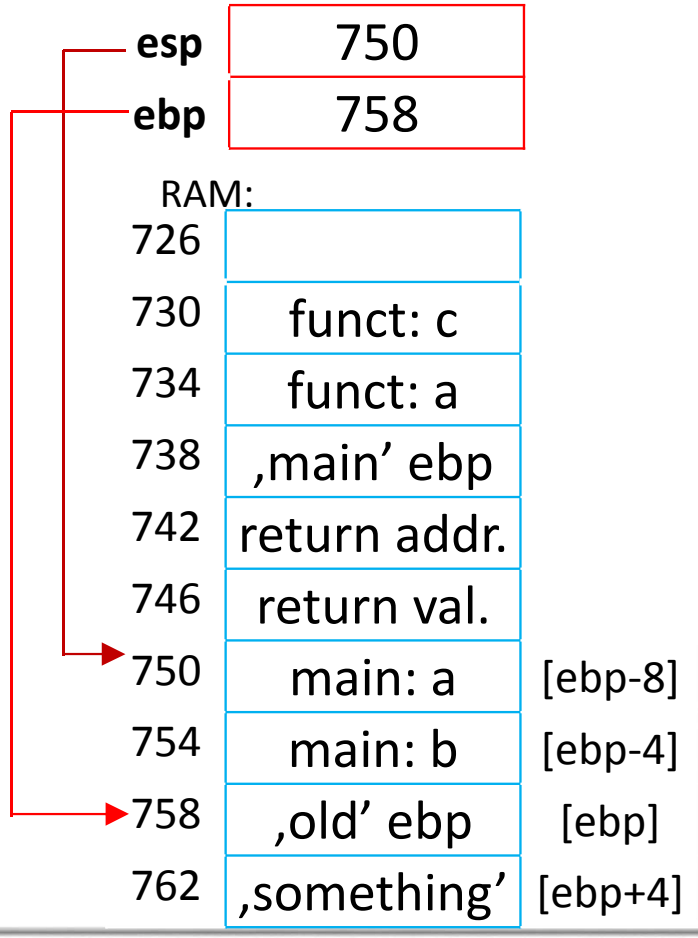


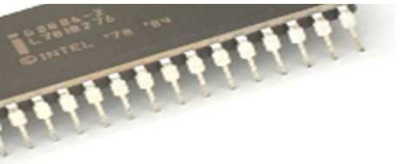


Example in assembly

```
main:    push    ebp
         mov     ebp, esp
         sub     esp, 8
         mov     DWORD PTR [ebp-8], edi
         mov     eax, DWORD PTR [ebp-8]
         push    eax
         call    funct
         pop     eax
         mov     DWORD PTR [ebp-4], eax
         mov     eax, DWORD PTR [ebp-4]
```

```
return b;
```

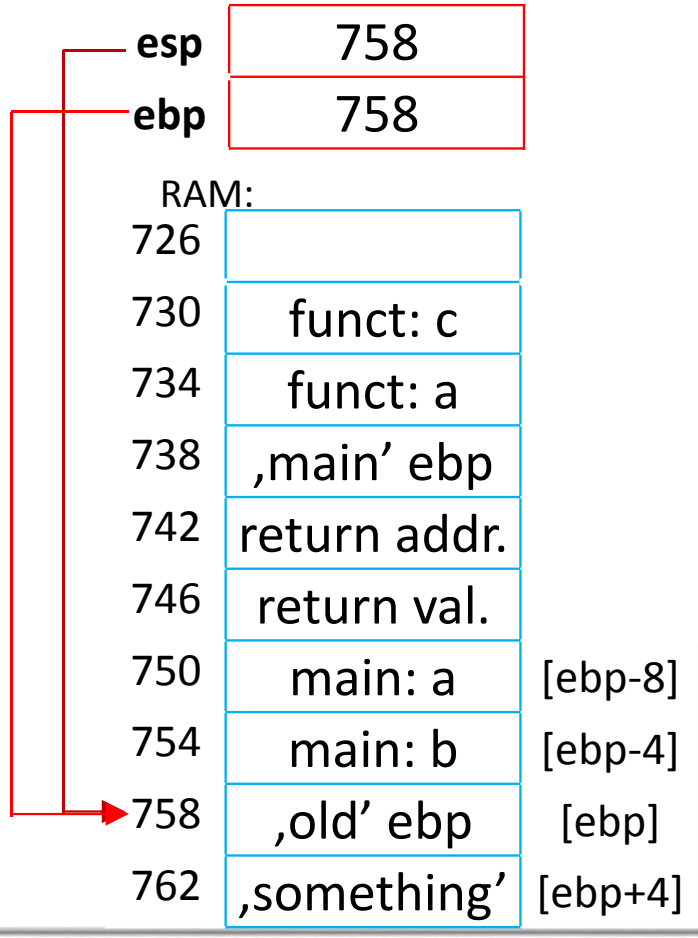


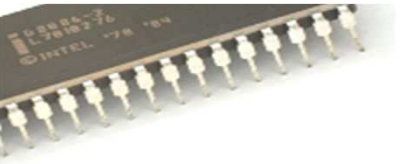


Example in assembly

```
main:    push    ebp
         mov     ebp, esp
         sub     esp, 8
         mov     DWORD PTR [ebp-8], edi
         mov     eax, DWORD PTR [ebp-8]
         push    eax
         call    funct
         pop     eax
         mov     DWORD PTR [ebp-4], eax
         mov     eax, DWORD PTR [ebp-4]
         mov     esp, ebp
```

```
return b;
```

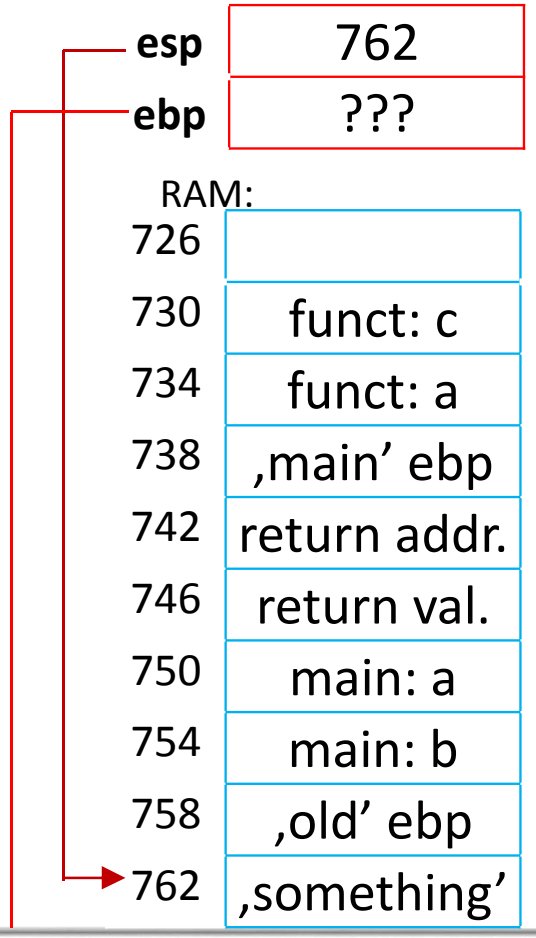


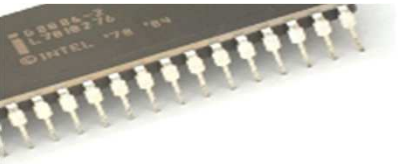


Example in assembly

```
main:   push    ebp
        mov     ebp, esp
        sub     esp, 8
        mov     DWORD PTR [ebp-8], edi
        mov     eax, DWORD PTR [ebp-8]
        push    eax
        call    funct
        pop     eax
        mov     DWORD PTR [ebp-4], eax
        mov     eax, DWORD PTR [ebp-4]
        mov     esp, ebp
        pop     ebp
```

```
return b;
```





Example in assembly

```
main:   push    ebp
        mov     ebp, esp
        sub     esp, 8
        mov     DWORD PTR [ebp-8], edi
        mov     eax, DWORD PTR [ebp-8]
        push    eax
        call    funct
        pop     eax
        mov     DWORD PTR [ebp-4], eax
        mov     eax, DWORD PTR [ebp-4]
        mov     esp, ebp
        pop     ebp
        ret
```

```
return b;
```