PAGE No.
DATE / /

Assignment-2

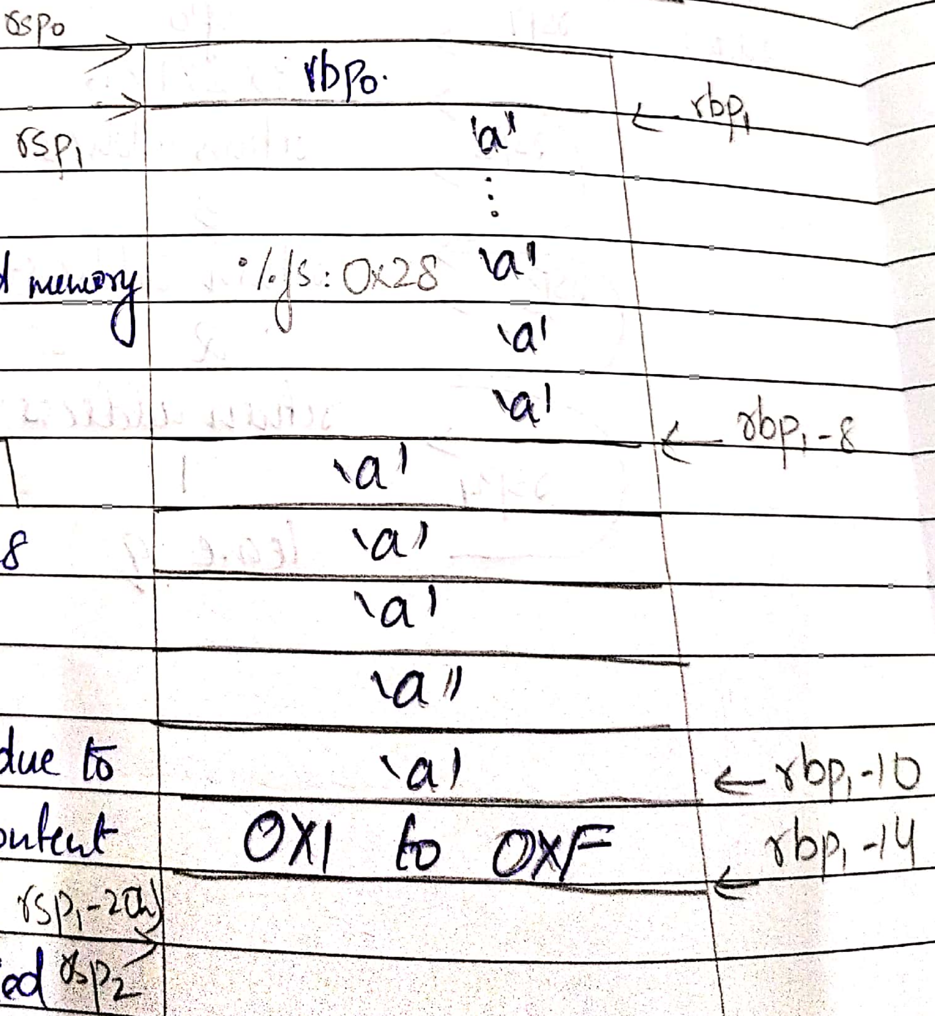
Stack Overflow

Q.1) Perform stack smashing and draw stack frame

```
#include<stdio.h>
int main(){
    char str[5];
    int i=0;
    for(i=0; i<=15;i++){
        str[i]='a';
    }
    return 0;
}
```

rdx
%fs:0x28

eax
0



Stack:
overflow of allocated memory

rdx
%(rbp-8)

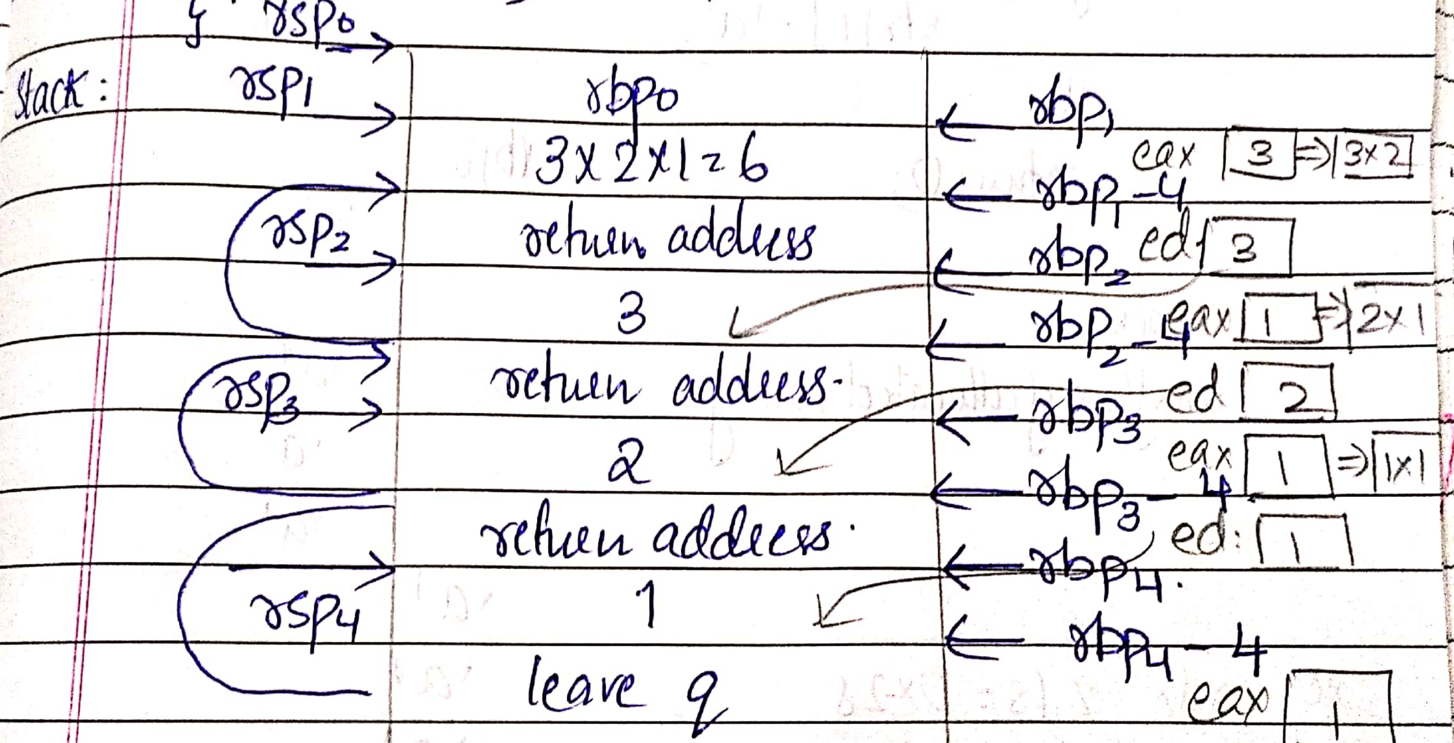
xor rdx %fs:0x28
(stack smash)

rdx content is changed due to overwriting of 'a'. So rdx content is no more %fs:0x28 (rsp1-20h)
∴ stack_chk_fail is called
∴ stack smash has occured.

Scanned with CamScanner

Q82) Stack diagram of recursive Program.

```
#include<stdio.h>
int fact(int n){
     if (n<=1) return 1;
    else   return n*fact(n-1);
}
int main(){
        int a=fact(3);
      return 0;
}
```


rsp0
Stack:
rsp1
rbp0
3x2x1=6
rsp2
return address
3
rsp3
return address.
2
return address.
1
rsp4
leave q
rbp1
eax
3
3x2
rbp1-4
ed
3
rbp2
rbp2-4
eax
1
2x1
ed
2
rbp3
eax
1
1x1
rbp3-4
ed:
1
rbp4.
rbp4-4
eax
1