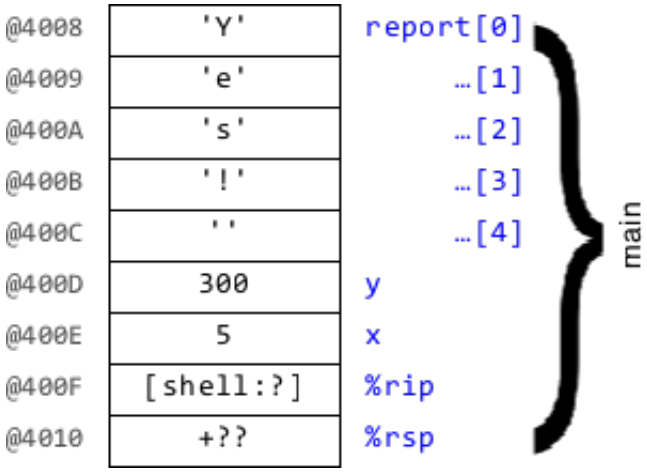
Welcome to DrRacket, version 5.3.6 [3m].
Language: racket; memory limit: 1024 MB.

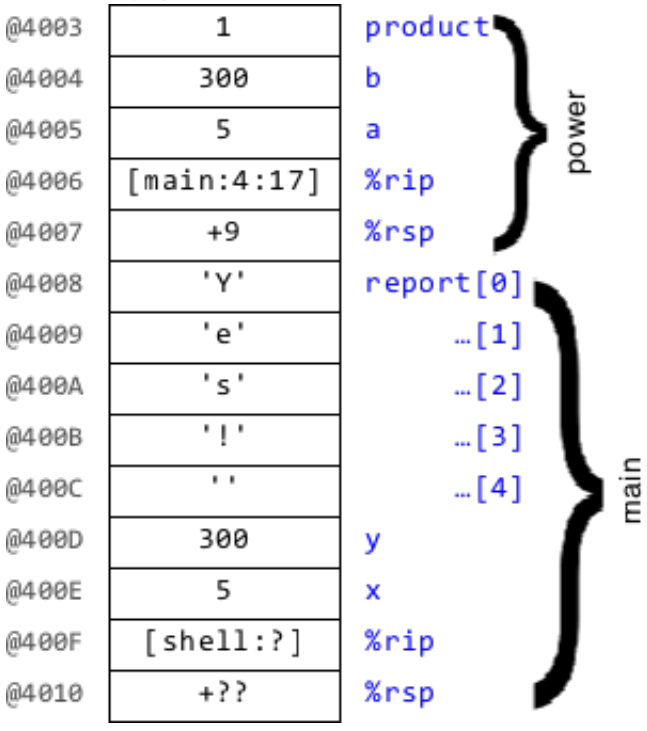
```
A C program, and how information is placed on the run-time stack at three moments
in time.

The purpose is to help understand how the run-time stack holds the current
function's local variables (incl. its parameters), as well as one piece of
important book-keeping: what program-instruction to resume at, when the current
helper function finishes.

This is important, since it explains how an attacker, if they can get a stack
overflow to both (a) place malicious code onto the stack, *and* (b) overwrite the
return-instruction-pointer so that the program 'returns' to that malicious code
rather than the real return-site, then the attacker has achieved "running of
arbitrary code".


Notes:
- "%rip" is a local system variable for "return instruction pointer" -- where to
resume the program at,
  when finishing the current helper function.
- "%rsp" is a local system variable for "return stack pointer" -- where to adjust
the top-of-stack to,
  when finishing the current helper function.


"The sample C program:"
#include <stdio.h>

int main() {
  printf("This program verifies whether 5 to the 300th power is bigger than 0.\n");
  int x = 5;
  int y = 300;
  char report[5] = "Yes!";

  if (power(x,y) >= 0) {
    printf("%s\n",report);
  }
  else {
    printf( "It's not!  Hmmm; overflow?\n" );
  }
  return 1; // indicate an error, to the shell / caller.
}


// Return a^b.
//
int power(int a, int b) {
  int product = 1;
```

```
  while (b!=0) {
    product = multiply(product, a);
    b--;
  }
  return product;
}


// Return x*y.
//
int multiply (int x, int y) {
 return x*y;
}
```

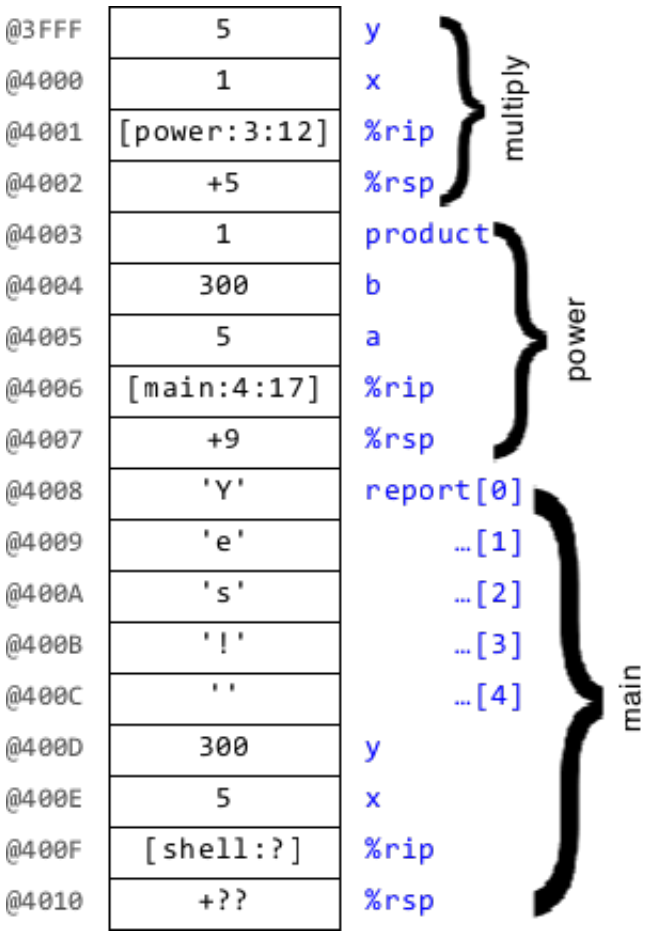
"In main:"



"calling power from main:"



"calling multiply from power from main:"


@3FFF
5
y
@4000
1
x
@4001
[power:3:12]
%rip
@4002
+5
%rsp
multiply
@4003
1
product
@4004
300
b
@4005
5
a
@4006
[main:4:17]
%rip
@4007
+9
%rsp
power
@4008
'Y'
report[0]
@4009
'e'
…[1]
@400A
's'
…[2]
@400B
'!'
…[3]
@400C
''
…[4]
@400D
300
y
@400E
5
x
@400F
[shell:?]
%rip
@4010
+??
%rsp
main

>