How do we accomplish those steps?

That fact? You can prove it in the extra credit problem on HW5. It's a nice combination of lots of things we've done with modular arithmetic.

Let's talk about finding $C = a^e \% n$.

e is a BIG number (about 2^{16} is a common choice)

```
int total = 1;
for(int i = 0; i < e; i++){
    total = (a * total) % n;
}
```

One More Example for Reference

Find $3^{25}\%7$ using the fast exponentiation algorithm.

$3^1\%7 = 3$

$3^2\%7 = 2$

$3^4\%7 = 4$

$3^8\%7 = 2$

$3^{16}\%7 = 4$

$3^{25}\%7 = 3^{16+8+1}\%7$
$= [(3^{16}\%7) \cdot (3^8\%7) \cdot (3^1\%7)]\%7$
$= [4 \cdot 2 \cdot 3]\%7$
$= (1 \cdot 3)\%7 = 3$