We will describe a method to compute $a^k \mod m$ known as the *Method of Successive Squaring.* Before describing it in general, we will illustrate it by computing

$$7^{327} \mod 853.$$

The first step is to create a table giving the values of 7, 7^2, 7^4, 7^8, 7^{16}, ... modulo 853. Notice that to get each successive entry in the list, we just have to square the previous number. Furthermore, since we always reduce modulo 853 before squaring, we never have to work with any numbers larger than 852^2. Here is the table of 2^k-powers of 7 modulo 853.

$$\begin{array}{llllll}
7^1 & & & \equiv 7 & \equiv 7 & \mod 853 \\
7^2 & \equiv (7^1)^2 & \equiv 7^2 & \equiv 49 & \equiv 49 & \mod 853 \\
7^4 & \equiv (7^2)^2 & \equiv 49^2 & \equiv 2401 & \equiv 695 & \mod 853 \\
7^8 & \equiv (7^4)^2 & \equiv 695^2 & \equiv 483025 & \equiv 227 & \mod 853 \\
7^{16} & \equiv (7^8)^2 & \equiv 227^2 & \equiv 51529 & \equiv 349 & \mod 853 \\
7^{32} & \equiv (7^{16})^2 & \equiv 349^2 & \equiv 121801 & \equiv 675 & \mod 853 \\
7^{64} & \equiv (7^{32})^2 & \equiv 675^2 & \equiv 455625 & \equiv 123 & \mod 853 \\
7^{128} & \equiv (7^{64})^2 & \equiv 123^2 & \equiv 15129 & \equiv 628 & \mod 853 \\
7^{256} & \equiv (7^{128})^2 & \equiv 628^2 & \equiv 394384 & \equiv 298 & \mod 853
\end{array}$$

The next step is to write the exponent 327 as a sum of powers of 2. This is called the *binary expansion* of 327. The largest power of 2 less thatn 327 is $2^8 = 256$, so we write $327 = 256 + 71$. Then the largest power of 2 less than 71 is $2^6 = 64$, so $327 = 256 + 64 + 7$. And continue in this manner to get:

$$\begin{aligned}
327 &= 256 + 71 \\
&= 256 + 64 + 7 \\
&= 256 + 64 + 4 + 3 \\
&= 256 + 64 + 4 + 2 + 1.
\end{aligned}$$

Now we use the binary expansion of 327 to compute

$$\begin{aligned}
7^{327} &= 7^{256+64+4+2+1} \\
&= 7^{256} \cdot 7^{64} \cdot 7^4 \cdot 7^2 \cdot 7^1 \\
&\equiv 298 \cdot 123 \cdot 695 \cdot 49 \cdot 7 \mod 853.
\end{aligned}$$

The numbers in the last line are taken from the table of powers of 7 that we computed earlier.

To complete the computation of $7^{327} \mod 853$, we just need to multiply the five numbers $298 \cdot 123 \cdot 695 \cdot 49 \cdot 7$ and reduce them modulo 853. If the product of all five numbers is too large, we can just multiply the first two, reduce modulo 853, multiply by the third, reduce modulo 853, and so on. In this way we will never need to work with any number bigger than $(852)^2$. Thus,

$$\begin{aligned}
298 \cdot 123 \cdot 695 \cdot 49 \cdot 7 &\equiv 828 \cdot 695 \cdot 49 \cdot 7 \\
&\equiv 538 \cdot 49 \cdot 7 \\
&\equiv 772 \cdot 7 \equiv 286 \mod 853.
\end{aligned}$$

We are now done and we see that

$$7^{327} \equiv 286 \mod 853.$$

This may seem like a lot of work, but suppose instead that we try to compute $7^{327} \mod 853$ directly by first computing 7^{327} and then dividing by 853 and taking the remainder. It is possible to do this with a small computer and you will get a number 7^{327} which has 277 digits in its decimal expansion. However, it is completely infeasible to compute a^k exactly when k has, say 20 digits, much less when k has the hundreds of digits required to construction of secure codes.

On the other hand, the method of successive squaring can be used to compute $a^k \mod m$ even when k has hundreds or thousands of digits.

We now describe the general method of computing powers by successive squaring.

Successive Squaring to Compute $a^k \mod m$. The following steps compute the value of a^k mod m:

1. Write k as a sum of powers of 2,

$$k = u_0 + u_1 \cdot 2 + u_2 \cdot 4 + u_3 \cdot 8 + \cdots + u_r \cdot 2^r,$$

   where each u_i is either 0 or 1. (This is called the *binary expansion* of k.)

2. Make a table of powers of a modulo m using successive squaring.

$$\begin{array}{lcccll} a^1 & & & & \equiv A_0 & \mod m \\ a^2 & \equiv & (a^1)^2 & \equiv & A_0^2 \equiv A_1 & \mod m \\ a^4 & \equiv & (a^2)^2 & \equiv & A_1^2 \equiv A_2 & \mod m \\ a^8 & \equiv & (a^4)^2 & \equiv & A_2^2 \equiv A_3 & \mod m \\ & & \vdots & \equiv & \vdots & \\ a^{2^r} & \equiv & \left(a^{2^{r-1}}\right)^2 & \equiv & A_{r-1}^2 \equiv A_r & \mod m \end{array}$$

   Note that to compute each line of the table you only need to take the number at the end of the previous line, square it, and then reduce it modulo m. Also note that the table has $r+1$ lines, where r is the highest exponent of 2 appearing in the binary expansion of k in Step 1.

3. The product

$$A_0^{u_0} \cdot A_1^{u_1} \cdot A_2^{u_2} \cdots A_r^{u_r} \mod m$$

   will be congruent to $a^k \mod m$. Note that all of the u_i's are either 0 or 1, so this number is really just the product of those A_i's for which u_1 is 1.

Why does this work? We compute

$$\begin{aligned} a^k &= a^{u_0 + u_1 \cdot 2 + u_2 \cdot 4 + u_3 \cdot 8 + \cdots + u_r \cdot 2^r} && \text{using Step 1,} \\ &= a^{u_0} \cdot (a^2)^{u_1} \cdot (a^4)^{u_2} \cdots (a^{2^r})^{u_r} \\ &\equiv A_0^{u_0} \cdot A_1^{u_1} \cdot A_2^{u_2} \cdots A_r^{u_r} && \text{using the table from Step 2.} \end{aligned}$$