More on RSA.

(A) Recall: to encode a message - made up, let's assume, of only the letters A,...,Z - we:

(1) Numerize: that is, convert to an integer n, using

$A \to 11,\ B \to 12,\ C \to 13, \ldots, Z \to 36.$

E.g. suppose our message is "B:" we convert it to $n = 12$.

(2) Raise n to a natural number k. E.g. if $k = 7$, then

$$n^k = 12^7 = 35{,}831{,}808.$$

(3) Let m be another natural number. Find the remainder r of n^k after division by m. E.g. let $m = 35$: it can be shown that

$$12^7 = 35 \cdot 1{,}023{,}765 + 33. \qquad (*)$$

So the encoded message we transmit <u>is</u> $r = 33$.

Big QUESTION: <u>how</u> did we find $(*)$? More generally, how do we "reduce $n^k \pmod{m}$"

(meaning: find the remainder of n^k after division by m)? ANSWER:

(B) Successive squaring.

Throughout, all lower-case variable names denote integers.

Recall: If $m \mid (a-b)$, we write
$a \equiv b \pmod{m}$.

E.g. $79 \equiv 7 \pmod{12}$ (since $79-7=72 = 12 \cdot 6$), $3^5 \equiv 3 \pmod{5}$ (since $3^5 - 3 = 5 \cdot 48$), $-242107 \equiv -107 \pmod{242}$, etc.

So, to find $n^k \bmod m$ – that is, to find the number r with
$$n^k = mq + r \qquad (0 \leq r < m),$$
we need to find the number r with
$$n^k \equiv r \pmod{m} \qquad (0 \leq r < m).$$

We do so by "successive squaring."

Example 1.
Reduce $12^7 \pmod{35}$.

Solution

Step 1. First, find the "binary expansion" of the exponent 7 (express 7 as sums of powers of 2).
We have
$$7 = 4 + 2 + 1.$$

Step 2. Raise the base 12 to successive powers of 2, and compute the results (mod 35). We have:

$$12^1 \equiv 12 \pmod{35},$$
$$12^2 = 144 \equiv 35 \cdot 4 + 4 \equiv 4 \pmod{35},$$
$$12^4 = (12^2)^2 \equiv 4^2 \equiv 16 \pmod{35}.$$

Step 3. Put it all together to find $12^7 \pmod{35}$. The trick is to keep reducing factors (mod 35), until the final result is < 35, like this:

$$\begin{aligned} 12^7 = 12^{4+2+1} &= 12^4 \cdot 12^2 \cdot 12^1 \\ &\equiv 16 \cdot 4 \cdot 12 \\ &\equiv 16 \cdot 48 \equiv 16 \cdot (35 \cdot 1 + 13) \\ &\equiv 16 \cdot 13 \\ &\equiv 208 \equiv 35 \cdot 5 + 33 \\ &\equiv 33 \pmod{35}. \end{aligned}$$

Example 2.
Reduce $11^{39} \pmod{51}$.

Solution

Step 1:
$$39 = 32 + 4 + 2 + 1.$$

Step 2:

$$11^1 \equiv 11 \pmod{51},$$
$$11^2 \equiv 121 \equiv 51 \cdot 2 + 19 \equiv 19 \pmod{51},$$
$$11^4 \equiv (11^2)^2 \equiv 19^2 = 361 \equiv 51 \cdot 7 + 4 \equiv 4 \pmod{51},$$
$$11^8 \equiv (11^4)^2 \equiv 4^2 \equiv 16 \pmod{51},$$

$$11^{16} \equiv (11^8)^2 \equiv 16^2 \equiv 256 \equiv 51\cdot 5+1 \equiv 1 \pmod{51},$$
$$11^{32} \equiv (11^{16})^2 \equiv 1^2 \equiv 1 \pmod{51}.$$

Step 3: So

$$\begin{aligned} 11^{39} &\equiv 11^{32+4+2+1} \\ &\equiv 11^{32}\cdot 11^4\cdot 11^2\cdot 11 \\ &\equiv 1\cdot 4\cdot 19\cdot 11 \\ &\equiv 76\cdot 11 \equiv (51\cdot 1+25)\cdot 11 \\ &\equiv 25\cdot 11 \\ &\equiv 275 \equiv 51\cdot 5+20 \\ &\equiv 20 \pmod{51}. \end{aligned}$$