More on RSA.

1) Encoding, continued.

Throughout, $n, k, m \in \mathbb{N}$.

Recall: we can compute $n^k \pmod{m}$ (that is, the remainder of n^k after division by m) by successive squaring:

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

Step 2.

Raise n to successive powers of 2, reducing $\pmod{m}$ along the way, up to the highest power of 2 in Step 1.

Step 3

Combine Steps 1 and 2, reducing $\pmod{m}$ along the way, to find $n^k \pmod{m}$.

Example 1.

Find $19^{23} \pmod{35}$.

Solution.

Step 1: $23 = 16 + 4 + 2 + 1$

Step 2: $19^1 \equiv 19 \pmod{35}$

$19^2 \equiv 361 \equiv 35 \cdot 10 + 11 \equiv 11 \pmod{35}$

$19^4 \equiv (19^2)^2 \equiv 11^2 \equiv 121 \equiv 35 \cdot 3 + 16$

$\equiv 16 \pmod{35}$

$19^8 \equiv (19^4)^2 \equiv 16^2 \equiv 256 \equiv 35 \cdot 7 + 11$

$\equiv 11 \pmod{35}$

$19^{16} \equiv (19^8)^2 \equiv 11^2 \equiv 16 \pmod{35}$.

So

$$
\begin{aligned}
19^{23} &\equiv 19^{16}\cdot 19^{4}\cdot 19^{2}\cdot 19\\
&\equiv 16\cdot 16\cdot 11\cdot 19\\
&\equiv 256\cdot 209\\
&\equiv 11\cdot 209 \equiv 11\cdot(35\cdot 5+34)\\
&\equiv 11\cdot 34 \equiv 374 \equiv 35\cdot 10+24\\
&\equiv 24 \pmod{35}.
\end{aligned}
$$

Example 2

Find $21^{101} \pmod{143}$.

Solution

Step 1: $101 = 64+32+4+1$.

Step 2:

$$
\begin{aligned}
21 &\equiv 21 \pmod{143}\\
21^2 &\equiv 441 \equiv 143\cdot 3+12 \equiv 12 \pmod{143}\\
21^4 &\equiv (21^2)^2 \equiv 12^2 \equiv 144 \equiv 1 \pmod{143}\\
21^8 &\equiv (21^4)^2 \equiv 1^2 \equiv 1 \pmod{143}
\end{aligned}
$$

Similarly, we see that $21^{16} \equiv 21^{32} \equiv 21^{64} \equiv 1 \pmod{143}$.

Step 3:

$$
\begin{aligned}
21^{101} &\equiv 21^{64}\cdot 21^{32}\cdot 21^{4}\cdot 21^{1}\\
&\equiv 1\cdot 1\cdot 1\cdot 21 \equiv 21 \pmod{143}.
\end{aligned}
$$

//

(B) Prelude to decoding.

We'll need some number theory definitions and theorems.

1) Greatest common divisor.

Definition Let $a, b \in \mathbb{Z}$.
We define the greatest common divisor of a and b, denoted $\gcd(a,b)$, by

$\gcd(a,b)$ = largest natural number n dividing both a and b, unless $a=b=0$: we define $\gcd(0,0)=0$.

Examples:

$$\gcd(12,21) = 3$$
$$\gcd(-17,34) = 17$$
$$\gcd(1,b) = 1 \text{ for any } b \in \mathbb{Z}.$$
$$\gcd(5,0) = 5$$
$$\gcd(0,-3) = 3$$
$$\gcd(a,0) = |a| \text{ for any } a \in \mathbb{Z}.$$

In general, to find $\gcd(a,b)$: factor a and b into products of prime powers: $\gcd(a,b)$ is the product of all prime powers common to both factorizations.

Example 3.

$$\gcd(8640, 63000) = \gcd(2^6 \cdot 3^3 \cdot 5,\ 2^3 \cdot 3^2 \cdot 5 \cdot 7)$$
$$= 2^3 \cdot 3^2 \cdot 5$$
$$= 360.$$

$$\gcd(23^7 \cdot 51^{95},\ 17^3 \cdot 46^{101})$$
$$= \gcd(23^7 \cdot 3^{95} \cdot 17^{95},\ 17^3 \cdot 2^{101} \cdot 23^{101})$$
$$= 23^7 \cdot 17^3 = 16{,}727{,}907{,}421{,}111.$$