More on RSA.

(A) 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, from the first power to the highest power of 2 from Step 1. Each power is computed by squaring the previous one and reducing (mod m).

Step 3. Combine Steps 1 and 2, reducing (mod m) along the way, to find $n^k \pmod m$.

Example 1. Find $21^{101} \pmod{143}$.

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

Step 2:

$21 \equiv 21 \pmod{143}$

$21^2 \equiv 441 \equiv 143 \cdot 3 + 12 \equiv 12 \pmod{143}$

$21^4 \equiv (21^2)^2 \equiv 12^2 \equiv 144 \equiv 1 \pmod{143}$

$21^8 \equiv (21^4)^2 \equiv 1^2 \equiv 1 \pmod{143}$

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

Step 3: $21^{101} \equiv 21^{64} \cdot 21^{32} \cdot 21^{4} \cdot 21^{1}$

$\equiv 1 \cdot 1 \cdot 1 \cdot 21 \equiv 21 \pmod{143}$.

(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 m dividing both a and b, unless $a=b=0$: we define $\gcd(0,0)=0$.

Example 2

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

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

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

2) Coprime integers.

Definition. If $a, b \in \mathbb{Z}$ satisfy $\gcd(a,b) = 1$, we say a, b are coprime (or relatively prime).

Example 4.

(i) 2 and 17 are coprime
(ii) $105 = 3 \cdot 5 \cdot 7$ and $256 = 2^8$ are coprime
(iii) 1 and 10^{98} are coprime
(iv) 111,111,111 and 111,111,112 are coprime.
We could check this by factoring,* or we could note that:

(v) a and $a+1$ are coprime for any $a \in \mathbb{Z}$.

[Proof later.]

* $111,111,111 = 3^2 \cdot 37 \cdot 333,667$
$111,111,112 = 2^3 \cdot 7 \cdot 109^2 \cdot 167$