Prelude to RSA decoding, continued.

1) Greatest common divisor.

Recall: the greatest common divisor $\gcd(a,b)$ of $a, b \in \mathbb{Z}$ is defined by

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

E.g. $\gcd(21, 28) = 7$,

$\gcd(810, 168) = \gcd(2 \cdot 3^4 \cdot 5,\ 2^3 \cdot 3 \cdot 7)$
$= 2 \cdot 3 = 6$,

$\gcd(1, 0) = 1$,

$\gcd(111111, 11111111)$
$= \gcd(3 \cdot 7 \cdot 11 \cdot 13 \cdot 37,\ 11 \cdot 73 \cdot 101 \cdot 137) = 11$,

etc.

2) Two theorems without proof (for now).

Theorem RSA$_1$.
Suppose $a, b \in \mathbb{N}$ are coprime, meaning $\gcd(a, b) = 1$. Then $\exists\, x, y \in \mathbb{N}$ such that

$$ax - by = 1.$$

Example 1:

(a) 35 and 128 are coprime; note that

$$35 \cdot 11 - 128 \cdot 3 = 1.$$

(b) a and $a+1$ are coprime for $a \in \mathbb{Z}$;
note that

$$a \cdot a - (a+1)(a-1) = a^2 - (a^2-1) = 1.$$

(c) 101 and 103 are coprime (and prime);
note that

$$101 \cdot 51 - 103 \cdot 50 = 1.$$

Note also that 103 and 101 are coprime, and

$$103 \cdot 51 - 101 \cdot 52 = 1.$$

<u>Theorem RSA$_2$</u> (Euler's formula.)
Let $p, q \in \mathbb{N}$ be distinct primes. Let $m = pq$,

and define

$$\varphi(m) = (p-1)(q-1)$$

("Euler's φ function").

Then for any $a \in \mathbb{Z}$ that's coprime to m,
we have

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

<u>Example 2.</u>
(a) Let $m = 35 = 5 \cdot 7$.
We have $\varphi(m) = (5-1)(7-1) = 4 \cdot 6 = 24$.
Let $a = 11$. Then $\gcd(a,m) = \gcd(11, 35) = 1$,
so by Theorem RSA$_2$, $a^{\varphi(m)} \equiv 1 \pmod{m}$:

$$11^{24} \equiv 1 \pmod{35}.$$

We can check this by successive squaring:

$18 = 16 + 8$

$11 \equiv 11 \pmod{35}$
$11^2 \equiv 121 \equiv 16 \pmod{35}$
$11^4 \equiv (11^2)^2 \equiv 16^2 = 256 \equiv 11 \pmod{35}$
$11^8 \equiv (11^4)^2 \equiv 11^2 \equiv 16 \pmod{35}$ (by the above)
$11^{16} \equiv (11^8)^2 \equiv 16^2 \equiv 11 \pmod{35}$ (by the above)

So
$$11^{18} \equiv 11^{16} 11^{8} \equiv 11 \cdot 16 \equiv 176 \equiv 1 \pmod{35}.$$

(b) Let $m = 10403 = 101 \cdot 103$.
Then
$$\varphi(m) = (101-1)(103-1) = 100 \cdot 102$$
$$= 10200 = 10^2 \cdot 2 \cdot 51$$
$$= 2^2 \cdot 5^2 \cdot 2 \cdot 3 \cdot 17 = 2^3 \cdot 3 \cdot 5^2 \cdot 17.$$

Let $a = 11011 = 7 \cdot 11^2 \cdot 13$.

Then $\gcd(a, m) = 1$, so by Theorem RSA_2,
$$11011^{10200} \equiv 1 \pmod{10403}.$$

DIY: check this by successive squaring.
(if you dare)!