RSA decoding.

(A) Recall the setup:

(1) **Theorem RSA$_1$**: If $a, b \in \mathbb{N}$ are coprime ($\gcd(a,b)=1$), then there exist $x, y \in \mathbb{N}$ with

$$ax - by = 1.$$

<u>Example</u>: 570 and 1111 are coprime (since $570 = 2\cdot 3\cdot 5\cdot 19$ and $1111 = 11\cdot 101$); note that

$$570\cdot 115 - 1111\cdot 19 = 1.$$

(2) **Theorem RSA$_2$**: Let $m = pq$ where p, q are distinct primes; define $\varphi(m) = (p-1)(q-1)$. Then for any $a \in \mathbb{Z}$ with $\gcd(a,m)=1$, we have

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

<u>Example</u>: Let $a = 570$ and $m = 1111 = 11\cdot 101$. We've seen that $\gcd(a,m) = 1$. Since $\varphi(m) = (11-1)(101-1) = 1000$, Theorem RSA$_2$ says

$$570^{1000} \equiv 1 \pmod{1111}.$$

(B) Decodable encoding.

To assure a message n can be encoded in a decodable way:

(1) Choose two (large) primes p and q; let $m = pq$.

(2) Make sure that $n < m$ and $\gcd(n, m) = 1$.

(3) Choose an exponent k with $\gcd(k, \varphi(m)) = 1$.

(4) Compute $n^k \pmod{m}$.

<u>Remark</u>: k and m (but <u>not</u> the factorization $m = pq$) can be shared, so anyone can encode.

(c) Decoding.

You're given a message $b \equiv n^k \pmod{m}$, coded as above. To decode it:

(1) Find $x, y \in \mathbb{N}$ with

$$kx - \varphi(m)y = 1. \qquad (*)$$

(possible by Theorem RSA_1).

(2) Compute $b^x \pmod{m}$ (by successive squaring). The result <u>is</u> the original message n!

Proof:

$$b^x \equiv (n^k)^x \equiv n^{kx} \overset{\text{by } (*)}{\equiv} n^{1+\varphi(m)y}$$

$$\equiv n^1 (n^{\varphi(m)})^y$$

$$\overset{\text{by Thm. } RSA_2}{\equiv} n \cdot 1^y \equiv n \pmod{m}. \qquad !!$$

(None of this works if you don't know p and q: without them, you don't know $\varphi(m)$, so you can't find x.)

(D) Example.
Decode the coded message $b = 33$, with $k = 7$ and $m = 35 = 5 \cdot 7$.

Solution.
Since $k = 7$ and $\varphi(m) = 4 \cdot 6 = 24$, we have $\gcd(k, \varphi(m)) = 1$. Note that

$$\underset{k}{7} \cdot \underset{x}{7} - \underset{\varphi(m)}{24} \cdot \underset{y}{2} = 1,$$

so we need to compute $b^x \pmod m$, which is $33^7 \pmod{35}$, by successive squaring:

$$7 = 4 + 2 + 1$$

$$33^1 \equiv 33 \pmod{35}$$
$$33^2 \equiv 1089 = 35 \cdot 31 + 4 \equiv 4 \pmod{35}$$
$$33^4 \equiv (33^2)^2 \equiv 4^2 \equiv 16 \pmod{35}$$

So

$$\begin{aligned} 33^7 &\equiv 33^{4+2+1} \\ &\equiv 33^4 \cdot 33^2 \cdot 33^1 \equiv 16 \cdot 4 \cdot 33 \\ &\equiv 64 \cdot 33 \equiv 29 \cdot 33 \\ &\equiv 957 = 35 \cdot 27 + 12 \equiv 12 \pmod{35}. \end{aligned}$$

Compare with the last example from the class of 8/27!!