- RSA decoding.

(A) Recall the setup:

(i) Definition: for $a, b \in \mathbb{Z}$,

$\gcd(a,b)$ = largest positive common divisor of a and b (unless $a=b=0$. Define $\gcd(0,0)=0$).

Example:

$$\gcd(720, 405) = \gcd(2^4 \cdot 3^2 \cdot 5,\ 3^4 \cdot 5) = 3^2 \cdot 5 = 45.$$

Also, if $\gcd(a,b)=1$, we say a and b are <u>coprime</u>. E.g. 570 and 1111 are coprime (since $\gcd(570, 1111)$ $\gcd(2 \cdot 3 \cdot 5 \cdot 19,\ 11 \cdot 101) = 1$).

(ii) Theorem RSA_1: If $a, b \in \mathbb{N}$ are coprime, then $\exists x, y \in \mathbb{N}$ with
$$ax - by = 1.$$

Example: we have
$$570 \cdot 115 - 1111 \cdot 59 = 1.$$

(iii) Theorem RSA_2: If $m = pq$ is a product of distinct primes and we define $\varphi(m) = (p-1)(q-1)$, then for any $a \in \mathbb{Z}$ that's coprime to m,
$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Example: let $m = 37 \cdot 73 = 2701$ and $a = 35$.

Then $\gcd(a,m) = \gcd(3\cdot 5, 37\cdot 73) = 1$, so

$$a^{\varphi(m)} \equiv 1 \pmod{m}, \text{ that is,}$$

$$35^{(37-1)(73-1)} \equiv 1 \pmod{2701}$$

$$35^{2592} \equiv 1 \pmod{2701}$$

as can be verified by successive squaring.

(B) Decodable encoding.

To assure an encoded message n can be decoded, but only by someone who knows how:

1) Choose two (large) primes p and q; let $m = pq$. Make sure the message n is:

   (a) $< m$;
   (b) coprime to m.
   (c) Choose an exponent k that's coprime to $\varphi(m) = (p-1)(q-1)$.

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

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

(C) Decoding.

You're given a coded message $b = n^k \pmod{m}$. You know k, m, and the factorization $m = pq$. To find n:

(1) Find integers x and y such that

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

(possible by Thm. RSA_1).

(2) Compute $b^x \pmod{m}$. Amazing fact: your answer is equal to n!!

Proof:

$$
\begin{aligned}
b^x &\equiv (n^k)^x \equiv n^{kx} \overset{\text{by } (*)}{\equiv} n^{1+\varphi(m)y} \\
&\equiv n^1 (n^{\varphi(m)})^y \\
&\overset{\text{by Thm. } RSA_2}{\equiv} n \cdot 1^y \equiv n \pmod{m}. \qquad !!
\end{aligned}
$$

(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.

In class on 11/11, we encoded a certain message n, with $k = 7$ and $m = 35 = 5 \cdot 7$, to get a coded message $b = 33$. Let's recover n:

We have $k = 7$ and $\varphi(m) = 4 \cdot 6 = 24$;

note that $\gcd(k,\varphi(m)=1)$. We check that

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

so we compute $b^x = 33^7 \pmod{35}$. We use successive squaring:

$$7 = 4+2+1,$$

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

So

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

So $n=12$ which <u>was</u> the n we started with on 11/11 !