Number Theory Section Summary: 7.5
The RSA algorithm

The RSA algorithm (developed by Rivest, Shamir, and Adleman in 1977) depends on the fact that

Computers can't quickly and efficiently factor humongous numbers.

So here are the steps:

- Come up with two large primes: p and q. Shhhh! Don't tell a soul your secret numbers!
- Your public modulus will be $n = pq$: you can tell that to anyone.
- Come up with a value for k such that $\gcd(k, \phi(n)) = 1$ (easy choice: a prime bigger than either p or q: since $\phi(n) = (p-1)(q-1)$, k must be relatively prime to $\phi(n)$; unfortunately, it could be horrendously large!).
- Publish (k, n) in the great big universal keybook – these are your public keys. Brag about them to your friends!
- Compute the *decripting* (or *recovery*) *exponent* j as the solution of

  $$kj \equiv 1 (\text{mod } \phi(n))$$

  To do this, the Euclidean algorithm is used: that is, solve

  $$kj + \phi(n)y = 1$$

  for j. Alternatively, you can use the result of exercise #8(a), p. 139: if $\gcd(a, n) = 1$, then the linear congruence $ax \equiv b(\text{mod } n)$ has the solution $x \equiv ba^{\phi(n)-1}(\text{mod } n)$. Hence, in our case, we've got

  $$j = k^{\phi(\phi(n))-1}(\text{mod } \phi(n))$$

- If CHAOS want to send you an encrypted message, they

– Write their message as a number, M, using ASCII or some other coding (such as the one on page 148).

  Note: if the plaintext message number M is too long (larger than n), then you must break M into n-sized blocks before encoding. Otherwise, there's not a unique solution, and the RSA scheme will find the smallest congruent message (between 0 and $n-1$) – which will likely be utter nonsense!

– Then send
$$r \equiv M^k (\text{mod } n).$$

- You decode the message as

$$r^j \equiv (M^k)^j \equiv M^{kj} \equiv M^{1+\phi(n)t} \equiv M(M^{\phi(n)})^t \equiv M(\text{mod } n)$$

whenever $gcd(M,n) = 1$ (which is almost always, given the construction of n).

Suppose (WLOG) that p divides M (we're not worried about q dividing M too, since $M < n$). Then

$$M^{\phi(n)} = M^{(p-1)(q-1)} = (M^{(p-1)})^{(q-1)} \equiv 1(\text{mod } q)$$

Hence
$$r^j \equiv M(\text{mod } q)$$
Furthermore, $M \equiv 0(\text{mod } p)$, so that
$$r^j \equiv M(\text{mod } p)$$
Therefore
$$r^j \equiv M(\text{mod } n)$$
even if $gcd(M,n) \neq 1$.

So once you've calculated j, you can throw away (eat, burn, etc.) p and q: the only secret needed to decode a message sent to you is j. Don't lose that! Put that in a safe place, because anyone can decode your messages given j.

Example: $p = 11$, $q = 13$ – **two enormous primes!**

$p = 11$
$q = 13$
$n = 143$
$\varphi(n) = 120$
Find $k \ni$ $gcd(k, \varphi(n)) = 1$
e.g. $k = 7$ Publish (k, n)

Find j such that

$kj \equiv 1 \pmod{\varphi(n)}$

$7j \equiv 1 \pmod{120}$

Find j /

$7j + 120y = 1$

$120 = 17 \cdot 7 + 1$

$7(-17) + 120 \cdot 1 = 1$

$7(120 - 17 - 120) + 120 \cdot 1 = 1$

$7 \cdot \boxed{103} + 120(-6) = 1$

$103 = j$, y – who cares?

Let's try a message:

$S = 18$ in the secret code book

Send

$M^k \pmod{n}$: $18^7 \pmod{143} \equiv 138$

We receive 138 : $r^j \pmod{n}$

$138^{103} \pmod{n} \equiv 18$
