RSA

- In Diffie-Hellman, two parties agree on a shared key. RSA keys are asymmetric. First, some prereqs.

Def a and b are coprime if they have no common factors other than 1.

e.g. 7 and 15 coprime ✓

12 and 15 not coprime: both mults of 3.

Def The Euler φ function (also called totient) is

$$\varphi(n) = \#\{1 \le k \le n \text{ such that } k \text{ is coprime to } n\}$$

ex $\varphi(12)$

$1 \; \cancel{2} \; \cancel{3} \; \cancel{4} \; 5 \; \cancel{6} \; 7 \; \cancel{8} \; \cancel{9} \; \cancel{10} \; 11 \; \cancel{12}$

$\varphi(12) = 4$

$\varphi(10)=4$

1 2 3 4 5 6 7 8 9 10

$\varphi(13)=12$

1 2 3 4 5 6 7 8 9 10 11 12 ~~13~~

everything coprime to it, since 13 is prime!

$\varphi(p)=p-1$

same reason

only things not coprime to pq are mults of p, mults of q

$$\varphi(pq)=\underbrace{pq}_{\text{all numbers}}-\underbrace{p}_{\text{mults of }q}-\underbrace{q}_{\text{mults of }p}+\underbrace{1}_{\text{pq itself was double-counted}}$$

$q, 2q, 3q, 4q, \ldots pq$

$=(p-1)(q-1)$

One fact.

Suppose b and n are coprime. Then there exists a unique $1 \le a \le n$ such that $ab \equiv 1 \mod n$.

a is the "inverse of b modulo n"

Ex $n=25$, $b=12$

Looking for a so $ab \equiv 1 \mod 25$

a	1	2	3	4	5	6	7	8 ...
$12a$:	12,	24,	36,	48,	60, ...			
$12a \mod 25$								

$-1 \mod 25$.

$a=-2$ works! But $-2 \equiv 23 \mod 25$,

so $a=23$ works.

Check: $23 \times 12 = 276 \equiv 275 + 1 \equiv 1 \mod 25$

Ex $n=7$, $b=3$.

Find a so $ab \equiv 1 \mod n$.

Sol: Check multiples of 3 until you get $1 \mod 7$

$3, 6, 9, 12, \underline{15}, 18$

$15 \equiv 1 \mod 7$.

$\underline{a=5}$

Fermat's Little Theorem

Suppose b and n are positive and coprime, then $b^{\varphi(n)} \equiv 1 \mod n$.

---

e.g. n is prime: $b^{n-1} \equiv 1 \mod n$

$n=10$ $\quad b^4 \equiv 1 \mod 10$

b coprime to 10 means last digit $1, 3, 7, 9$

Proof warm-up:

$n = 10, \quad b = 3.$

Make a list of all numbers less than 10, coprime to 10

$1 \quad 3 \quad 7 \quad 9 \xrightarrow[\text{mod } 10]{\text{product is}} 9$

multiply all by b, take result mod 10

$$\begin{array}{ccccc} 3\cdot 1 & 3\cdot 3 & 3\cdot 7 & 3\cdot 9 & \longrightarrow 3^4\cdot 9 \\ \parallel & \parallel & \parallel & \parallel & \\ 3 & 9 & 1 & 7 & \longrightarrow \text{also } 9 \end{array}$$

(same list!)

same as original list, scrambled

$3^4 \cdot 9 \equiv 9 \bmod 10.$ Multiply by inverse of 9 mod 10

$3^4 \equiv 1 \bmod 10$

"<u>Official" proof</u> $b^{\varphi(n)} \equiv 1 \bmod n$

Make a list of all numbers less than n, coprime to n:

$$a_1, a_2, a_3, \ldots, a_{\varphi(n)}.$$

Multiply everything in list by b (mod n).

$r_i = ba_i \bmod n$. New list:

$$r_1, r_2, r_3, \ldots, r_{\varphi(n)}.$$

I claim this is just original list, scrambled.

Why no duplicates in new list?

If $r_1 = r_2$ (for example)

Then $ba_1 \equiv ba_2 \bmod n$. Let c inverse of b mod n.

$$\underbrace{cb}_{1}a_1 \equiv \underbrace{cb}_{1}a_2 \bmod n$$

$$a_1 \equiv a_2 \bmod n.$$

So

$$a_1 \cdots a_{\varphi(n)} \equiv r_1 \cdots r_{\varphi(n)}$$

$$a_1 \cdots a_{\varphi(n)} \equiv (ba_1) \cdots (ba_{\varphi(n)})$$

$$\prod a_i \equiv b^{\varphi(n)} \left(\prod a_i\right) \bmod n$$

$$b^{\varphi(n)} \equiv 1 \bmod n.$$

RSA

The person receiving encrypted messages chooses two really big prime numbers, p and q.
~ 150 digits.

Computes product $n = pq$.

Picks an encryption key "e"

(in real life, often $e = 65537$)

Compute $\varphi(n) = (p-1)(q-1)$

Compute inverse of e mod $\varphi(n)$.

This is d so $de \equiv 1 \bmod \varphi(n)$.

Publicly announce: n, e

Keep secret: p, q, d.

How to check if p prime?

Compute 2^{p-1} mod p.

If not 1 mod p, not prime!

"Pseudoprime test"

Nemesis ~~They~~ could try to factor n and find p, q.

But n is so big this is impractical!

If you want to send a message:

- Represent it as a number M.
- Compute $E = M^e \bmod n$. (fast!)

E is the encrypted message!

To decrypt:

Just compute $\overset{M}{\overset{\shortparallel}{E^d \bmod n}}$ (the decrypter knows d and can do this)

Why? Secretly

$$E^d \equiv (M^e)^d \equiv M^{\overset{de = k\varphi(n)+1}{de}} = M^{k\varphi(n)+1} \bmod n.$$

$$= (M^{\varphi(n)})^k \cdot M \bmod n$$

$$= M \bmod n,$$

by Fermat's little theorem!

$\boxed{\text{After this we did the example on the worksheet, using CoCalc.}}$