>

$message = m$
choose primes p, q (secret)
let f = (p-1)*(q-1)
let n = p*q
choose e with gcd(e,f)=1.
compute $e^{-1} \bmod f = d$

encode, send $x = m^e \bmod n$
decode compute $x^d \bmod n = m$

That's how RSA works.

relies on Euler's theorem, which says $m^{(p-1)(q-1)} = m \bmod (pq)$

generalizes Fermat, which says $m^p = m \bmod p$

To understand Euler's thm, want to look at $a^i \bmod n$

know that if n is prime, $a^i \bmod p$ is invertible for all 0<= i <p
Another way to say that is that
$Z_n^* = \{ a \text{ in } Z_n \mid a \text{ has an inverse mod } n \}$

Z_n^* is a multiplicative group for any n

How big is it? (if n prime, it has n-1 elements, what if not prime?)

Another question: if a is in my group, say that a has finite multiplicative order if there is a k so that $a^k = 1 \bmod n$. Least such k is called the order of a.

What is the order of elements in my group?
Let's look at some examples.

```
> Z18:= {seq(i mod 18, i=1..18)};
```

$$Z18 := \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17\} \quad (1)$$

want the invertible elements of this. ie, those guys that are rel prime to 18.

```
> gcd(5,18);
```

1 (2)

```
> gcd(4,18);
```

2 (3)

Two ways to go: 1) write a for loop and keep the guys with gcd=1
2) use select to keep those guys.

```
> isrelprime:=(x,n) -> if gcd(x,n) = 1 then true; else false; fi;
```

$$isrelprime := (x, n) \rightarrow \textbf{if } gcd(x, n) = 1 \textbf{ then } true \textbf{ else } false \textbf{ end if} \quad (4)$$

```
> isrelprime(4,18);
```

false (5)

```
> isrelprime(5,18);
```

$$true \quad (6)$$

```
> select(isprime,Z18);  ## this is not what we want!
```

$$\{2, 3, 5, 7, 11, 13, 17\} \quad (7)$$

```
> select(x -> if x>5 then true else false fi, Z18);
```

$$\{6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17\} \quad (8)$$

```
> select( (x,y) -> if x*y > 5 then true else false fi, Z18, 2);
```

$$\{3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17\} \quad (9)$$

```
> select(isrelprime, Z18, 18);
```

$$\{1, 5, 7, 11, 13, 17\} \quad (10)$$

```
> Zstar := n -> select(isrelprime, {seq(i, i=0..n-1)}, n);
```

$$Zstar := n \rightarrow select(isrelprime, \{seq(i, i=0..n-1)\}, n) \quad (11)$$

```
> Zstar(3);
```

$$\{1, 2\} \quad (12)$$

```
> Zstar(4);
```

$$\{1, 3\} \quad (13)$$

```
> for i from 3 to 16 do
    printf("Z*(%d)=%a,  size is %d\n",i,Zstar(i),nops(Zstar(i)));
  end;
Z*(3)={1, 2},  size is 2
Z*(4)={1, 3},  size is 2
Z*(5)={1, 2, 3, 4},  size is 4
Z*(6)={1, 5},  size is 2
Z*(7)={1, 2, 3, 4, 5, 6},  size is 6
Z*(8)={1, 3, 5, 7},  size is 4
Z*(9)={1, 2, 4, 5, 7, 8},  size is 6
Z*(10)={1, 3, 7, 9},  size is 4
Z*(11)={1, 2, 3, 4, 5, 6, 7, 8, 9, 10},  size is 10
Z*(12)={1, 5, 7, 11},  size is 4
Z*(13)={1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12},  size is 12
Z*(14)={1, 3, 5, 9, 11, 13},  size is 6
Z*(15)={1, 2, 4, 7, 8, 11, 13, 14},  size is 8
Z*(16)={1, 3, 5, 7, 9, 11, 13, 15},  size is 8
```

if n is prime, phi(n)= n-1.
if n=p^k then phi(n) = $p^k - p^{k-1}$
if n=a*b, then phi(n) = phi(a)*phi(b)

```
> numtheory[phi](16);
```

$$8 \quad (14)$$

let a be an element of Z_n^*. Define $aZ_n^* = \{\ a \cdot b \ \mathbf{mod}\ n \mid b \ \mathbf{in}\ Z_n^* \}$

Claim is that $aZ_n^* = Z_n^*$

```
> map ( x -> modp(x*5, 18), Zstar(18));
```

$$\{1, 5, 7, 11, 13, 17\} \quad (15)$$

```
> map ( x -> modp(x*3, 18), Zstar(18));
```

$$\{3, 15\} \quad (16)$$

$\mathrm{phi}(n) = size(Z_n^*)$
Euler says

$a^{\mathrm{phi}(n)}$ **mod** $n = 1$ **if** $gcd(a, n) = 1$.

proof: (given that $aZ_n^* = Z_n^*$)

Let N = $\prod_{b\ \mathbf{in} Z_n^*} b$

```
> N:=1; for j in Zstar(18) do
    N:=N*j;
  od;
```

$$N := 1$$
$$N := 1$$
$$N := 5$$
$$N := 35$$
$$N := 385$$
$$N := 5005$$
$$N := 85085 \quad \textbf{(17)}$$

```
> N mod 18;
```

$$17 \quad \textbf{(18)}$$

Let M = $\prod_{b\ \mathbf{in}\ aZ_n^*} b = a^{\mathrm{phi}(n)} N$

M mod n = N mod n ie
$a^{\mathrm{phi}(n)} N$ mod n = N mod n
$a^{\mathrm{phi}(n)} = 1$ **mod** n