INXHWJYJ RFYMJRFYNHX

Exercise: Solve for x and y mod 7.

$$2x + 6y \equiv 1 \pmod 7$$
$$4x + 3y \equiv 2 \pmod 7$$

$$\left.\begin{aligned} 2x + 6y &\equiv 1 \\ 8x + 6y &\equiv 4 \end{aligned}\right| \Rightarrow 6x \equiv 3 \Rightarrow x \equiv 6^{-1} \cdot 3 \pmod 7$$

What's the inverse of 6 modulo 7?

7	6	1	0
1	0	1	
0	1	-1	

$$7(1) + 6(-1) = 1$$

$$-1 \equiv 6 \pmod 7. \quad 6^{-1} = 6.$$

$$x \equiv 18 \pmod 7 \qquad x = 4$$

$$8 + 6y \equiv 1 \Rightarrow 6y \equiv -7 \equiv 0 \pmod 7 \qquad y = 0$$

Easy to solve system of linear equations in modulo n if n is prime.

What's not easy? Something like:

$$x^a \equiv b \pmod{n}$$

Solve for x, a, b, n known.

Cryptography

Encrypt a text: e.g. Caesar cipher

A	B	C	D	E	F	G	H	I	J	....	X	Y	Z
F	G	H	I	J	K	L	M	N	O	....	C	D	E

A:0, B:1, C:2, ... , Z:25. $s = 5$ (shift)

Encrypt: $y = (x + s) \bmod 26$

Decrypt: $x = (y - s) \bmod 26$

Any simplistic "substitution" code can be easily broken.

e.g. Frequency analysis of letters in text.

Public / Private key encryption - decryption : Introduction

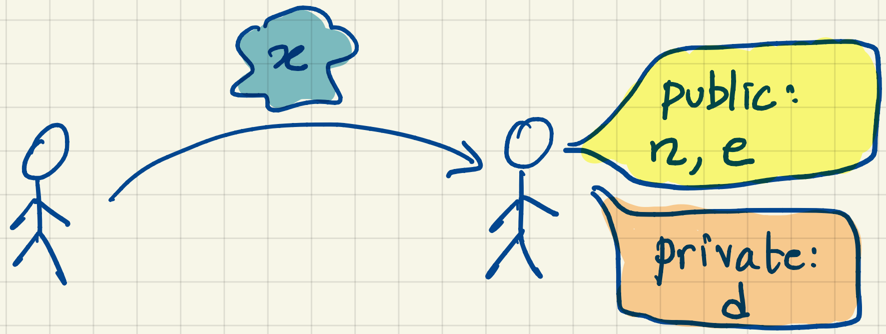
Two assumptions:

Given $x^e \bmod n$, solve for x : Hard

Given n, factor n into primes : Hard

Message:

$x < n$ $\qquad$ n : large prime



$\gcd(e, n-1) = 1$

$ed \equiv 1 \mod (n-1)$

d is inverse of e mod $n-1$

Instead of sending x, send

$$y = x^e \mod n$$

Upon seeing y, it's hard to solve for x. Unless we have d.

$$y^d \equiv [x^e]^d \equiv x^{ed} \equiv x^{k(n-1)+1} \equiv x \cdot x^{k(n-1)}$$

$$\equiv x \cdot [\underbrace{x^{(n-1)}}_{\equiv 1 \pmod n \text{ (Fermat)}}]^k \equiv x \pmod n$$

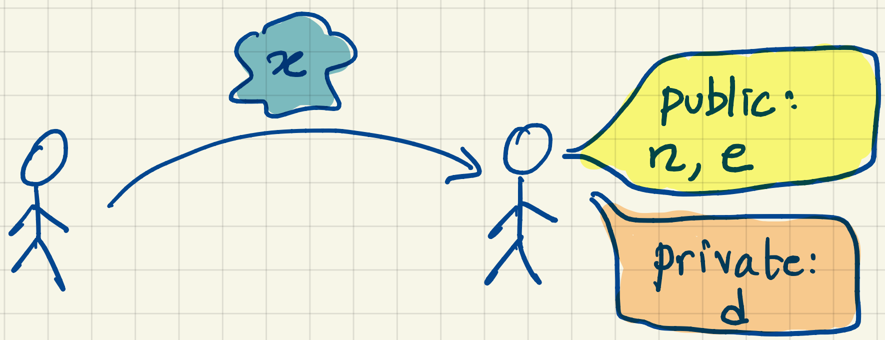
Fermat: $x < n$, n prime $\Longrightarrow x^{n-1} \equiv 1 \pmod n$

There is a problem with above approach!

Everyone can find d.

Knowing e and n, d can be found using the Euclidean algorithm. Because d is the inverse of e modulo $(n-1)$

Let's fix the approach.



$n = p \cdot q$

p and q are large primes

$ed \equiv 1 \mod (p-1)(q-1)$

To find d, we need to find the inverse of e mod $(p-1)(q-1)$
so we need to know p and q. So we need to factor n
into primes. HARD

Upon seeing $y = x^e \bmod n$, it also HARD to solve for x.

Unless we have d!

$$y^d \equiv [x^e]^d \equiv x^{ed} \equiv x^{k(p-1)(q-1)+1} \equiv x . [x^{p-1}]^{k(q-1)}$$

$p \nmid x$: $x^{p-1} \equiv 1 \pmod p$ (Fermat), so $y^d \equiv x \pmod p$

$p \mid x$: y^d and x are both multiples of p, so

$$y^d \equiv x \pmod p$$

$$y^d \equiv x \pmod{p}$$

$$y^d \equiv x \pmod{q}$$

$$\left.\begin{array}{l} p \mid y^d - x \\ q \mid y^d - x \end{array}\right\} \Longrightarrow$$ Since both p & q are primes

then $pq \mid y^d - x$

$n \mid y^d - x$

$$y^d \equiv x \pmod{n}.$$