recap

RSA : share private information over public network

Setup

Alice wants to send a  to **Bob**

Eve (sdropper) can see everything sent publicly

④ encrypts message m as $\mathcal{E}(m) = m^e \bmod N$

① picks large p, q, e st $(p-1)(q-1)$ and e are coprime

② finds $N = pq$ and publishes (N, e) ← public key

③ finds $d \equiv e^{-1} \bmod (p-1)(q-1)$ ← private key

⑤ takes $\mathcal{E}(m)$ and applies $D(\mathcal{E}(m))$ where $D(c) = c^d \bmod N$ $\quad D(\mathcal{E}(m)) = m$

Quick Facts

- $m^{ed} \equiv m \bmod N$
- $ed \equiv 1 \bmod (p-1)(q-1)$

	p	q	e	N	d	m	$\mathcal{E}(m)$
Alice			✓	✓		✓	✓
Bob	✓	✓	✓	✓	✓	✓	✓
Eve			✓	✓			✓

what does each person know?

recap

Relevant Proofs

$m \equiv m^{ed} \pmod N$, $N = pq$, $ed \equiv 1 \mod (p-1)(q-1)$

$ed = (p-1)(q-1)k + 1 \longrightarrow m^{ed} \equiv m^{(p-1)(q-1)k+1} \mod pq$

$m^{(p-1)(q-1)k+1} - m \equiv 0 \mod pq \longrightarrow m(m^{(p-1)(q-1)k} - 1) \equiv 0 \mod pq$

how to prove this?

Prove for p, q independently.

Prove $m(m^{(p-1)(q-1)k} - 1) \equiv 0 \mod p$.

1. if $m \equiv 0 \mod p$, done.
2. if $m \not\equiv 0 \mod p$, m & p coprime.

   $m^{(p-1)} \equiv 1 \mod p \longrightarrow (m^{(p-1)})^{k(q-1)} \equiv 1 \mod p$

   $m^{(p-1)(q-1)k} - 1 \equiv 0 \mod p$. done.

} casework based on if $p \mid m$. repeat same argument for q.

We know $m^{ed} \equiv m \mod p$, $m^{ed} \equiv m \mod q$. $\longrightarrow$ $p \mid m^{ed} - m$, $q \mid m^{ed} - m$, so $pq \mid m^{ed} - m$

How do we know $m^{ed} \equiv m \mod pq$? $\longrightarrow$ this is a system of equations that, by CRT, has unique solution mod pq

things to remember

- factoring is hard → knowing $(p-1)(q-1)$ given pq is computationally expensive
- finding gcd is efficient
- try to follow steps for original RSA proof for any alternate RSA schemes.

thanks for coming! help me help you → https://www.tinyurl.com/aishani-sp21-fb