CS 70 Discussion 4B

September 27, 2024

RSA Algorithm

Goal: Alice wants to send a secure message to Bob. But, the message channel is insecure.

Algorithm: We will do the following:

1) Bob picks some large, distinct primes p and q.
2) Bob picks some non-trivial $e, d \in \mathbb{N}$ where $ed \equiv 1 \pmod{(p-1)(q-1)}$.
3) Bob broadcasts (N, e) to everyone on the network, but keeps d, p, and q to himself ($N = pq$).
4) To send a message $x \in \{0, 1, ..., N-1\}$, Alice sends an encrypted message $y = x^e \bmod N$ over the channel to Bob.
5) Two things can happen:
   - Eve could intercept y, but since she doesn't know the value d, she can't decrypt and get x.
   - Bob gets y, so he performs $y^d \bmod N$ to get the original un-encrypted message (i.e. $y^d \equiv x \pmod{N}$).

RSA Algorithm (Cont.)

Why Secure?

- It is easy to generate large primes p and q.
- It is hard to factor numbers (you can't factor N quickly if N is extremeley large, such as if N is 1024 bits).

Note: RSA assumes that the message value is coprime to N