CS70 Public Key Cryptography(RSA)

Kelvin Lee

kelvinlee@berkeley.edu

September 28, 2020

Overview

Intro to RSA

Intro to RSA

Basic setting:

Intro to RSA

Basic setting:

- Alice and Bob wish to communicate secretly over some (insecure) link, and Eve tries to discover what they are saying.

Intro to RSA

Basic setting:

- Alice and Bob wish to communicate secretly over some (insecure) link, and Eve tries to discover what they are saying.
- Alice transmits a message x (in binary) to Bob by applying her **encryption function** E to x and send the encrypted message $E(x)$ over the link.

Intro to RSA

Basic setting:

- Alice and Bob wish to communicate secretly over some (insecure) link, and Eve tries to discover what they are saying.
- Alice transmits a message x (in binary) to Bob by applying her **encryption function** E to x and send the encrypted message $E(x)$ over the link.
- Bob, after receiving $E(x)$, applies his **decryption function** D to it and recover the original message: i.e., $D(E(x)) = x$.

Intro to RSA

Basic setting:

- Alice and Bob wish to communicate secretly over some (insecure) link, and Eve tries to discover what they are saying.
- Alice transmits a message x (in binary) to Bob by applying her **encryption function** E to x and send the encrypted message $E(x)$ over the link.
- Bob, after receiving $E(x)$, applies his **decryption function** D to it and recover the original message: i.e., $D(E(x)) = x$.
- Since the link is insecure, Eve may know what $E(x)$ is.

Intro to RSA

Intro to RSA

Basic setting (Continued):

Intro to RSA

Basic setting (Continued):

- We would like to have an encryption function E such that only knowing $E(x)$ cannot reveal anything about x.

Intro to RSA

Basic setting (Continued):

- We would like to have an encryption function E such that only knowing $E(x)$ cannot reveal anything about x.
- The idea is that each person has a **public key** known to the whole world and a **private key** known only to him- or herself.

Intro to RSA

Basic setting (Continued):

- We would like to have an encryption function E such that only knowing $E(x)$ cannot reveal anything about x.
- The idea is that each person has a **public key** known to the whole world and a **private key** known only to him- or herself.
- Alice encodes x using Bob's public key. Bob then decrypts it using his private key, thus retrieving x.

RSA Encryption

RSA Encryption

RSA:

RSA Encryption

RSA:

- Let p and q be two large primes, and let $N = pq$ (p and q are not public).

RSA Encryption

RSA:

- Let p and q be two large primes, and let $N = pq$ (p and q are not public).
- Treat messages to Bob as numbers modulo N, excluding trivial values 0 and 1.

RSA Encryption

RSA:

- Let p and q be two large primes, and let $N = pq$ (p and q are not public).
- Treat messages to Bob as numbers modulo N, excluding trivial values 0 and 1.
- Let e be any number that is relatively prime to $(p-1)(q-1)$ (Typically e is a small value).

RSA:

- Let p and q be two large primes, and let $N = pq$ (p and q are not public).
- Treat messages to Bob as numbers modulo N, excluding trivial values 0 and 1.
- Let e be any number that is relatively prime to $(p-1)(q-1)$ (Typically e is a small value).
- Then Bob's public key is the pair of numbers (N, e) and his private key is $d = e^{-1} \pmod{(p-1)(q-1)}$.

RSA Encryption

RSA Encryption

RSA(Continued):

RSA(Continued):

- **Encryption**: Alice computes the value $E(x) = x^e \bmod N$ and sends this to Bob.

RSA Encryption

RSA(Continued):

- **Encryption**: Alice computes the value $E(x) = x^e \bmod N$ and sends this to Bob.
- **Decryption:** Upon receiving the value $y = E(x)$, Bob computes $D(y) = y^d \bmod N$; this will be equal to the original message x.

RSA Encryption

RSA Encryption

Theorem

RSA Encryption

Theorem

Using the encryption and decryption functions E and D, we have $D(E(x)) = x \pmod{N}$ for every possible message $x \in \{0, 1, ..., N-1\}$.

RSA Encryption

Theorem

Using the encryption and decryption functions E and D, we have $D(E(x)) = x \pmod N$ for every possible message $x \in \{0, 1, ..., N-1\}$.

Proof:

This can be proved using Chinese Remainder Theorem or Fermat's Little Theorem. For more details, please refer to notes. □

Problem Time!