RSA Algorithm and Public Key Cryptosystems

Rohan Datta, Divya Raj

Abstract

This text discusses the concept behind public key cryptosystems, while focusing on a very popular encryption method. It also presents an array of real world implementations of the algorithm. Building upon ground-breaking research papers, it interprets the intriguing subject matter into an accessible form, and goes further to put forth their major applications and a few of their limitless possibilities.

Key words and phrases: cryptosystems, discrete mathematics, encryption, decryption, prime numbers, digital signatures, public key cryptosystems, authentication, cyber security.

Introduction to public key cryptosystems

RSA Algorithm

RSA algorithm is an asymmetric cryptographic algorithm that is used extensively by computers nowadays. It was proposed by Ron Rivest, Adi Shamir and Leonard Adleman in their 1978 paper [reference], and hence, bears their name. It is one of the most popular implementations of public key cryptosystems.

It is driven by the fact that finding the prime factors of a number is one of the most complex mathematical problems. Initially, the user creates and publishes the product of two large prime numbers, along with an auxiliary value. The auxiliary value takes up the role of the "public key" which is known to all. *But, the prime factors must be kept secret.*

1. Choose two different, large, random prime numbers **p** and **q**
2. Calculate **n** = **p*q**
3. $\boldsymbol{\phi(n)}$ = **(p - 1)*(q - 1)**
4. Choose an integer **e** such that:

- 1 <**e** <$\boldsymbol{\phi(n)}$

- **e** is co-prime to $\boldsymbol{\phi(n)}$

5. Compute **d** such that **d*e** = 1+**k***$\boldsymbol{\phi(n)}$

A popular choice for public exponents is **e** = $\mathbf{2}^{\mathbf{16}}$+**1**