The Essence of RSA Cryptosystem

Contents

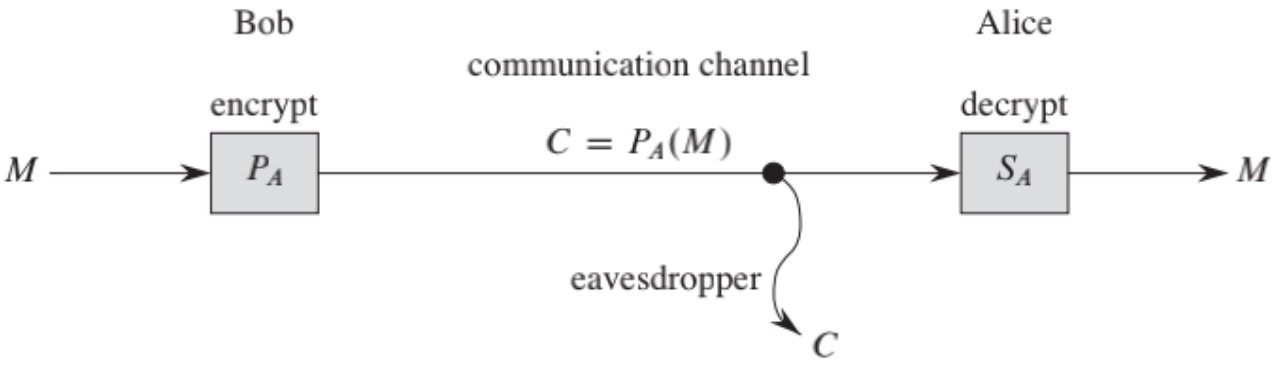
Overview

Number theory was once viewed as a beautiful but largely useless subject in pure mathematics. Today number-theoretic algorithms are used widely, due in large part to the invention of cryptographic schemes based on large prime numbers. These schemes are feasible because we can find large primes easily, and they are secure because we do not know how to factor the product of large primes efficiently.

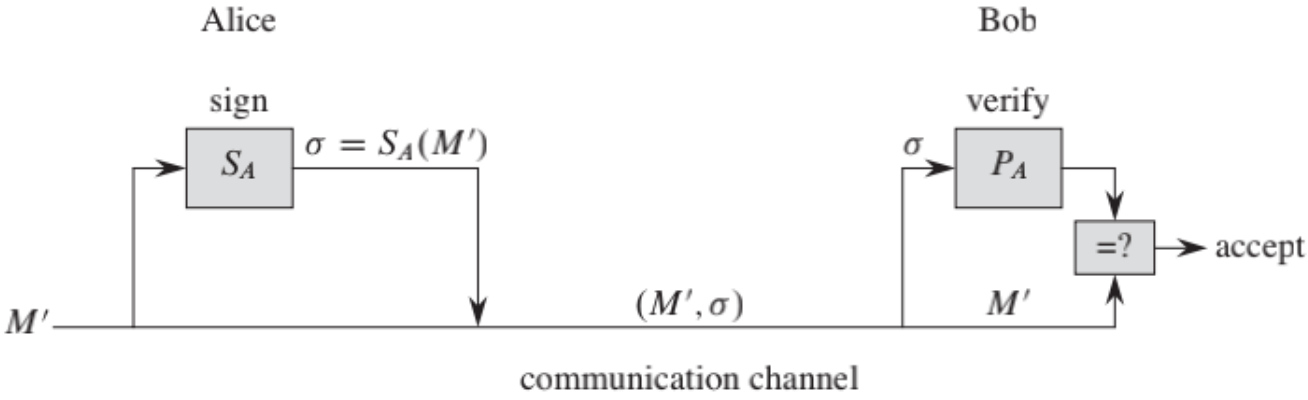
In RSA, each participant has both a **public key** and a **secret key**. Secret keys are kept secret, but public keys can be revealed to anyone or even published.

Usecase

- Encrypt messages



- Digital signature



Concept

Implementation

Algorithm

1. Select at random two large prime numbers and such that . The primes and might be, say, 1024 bits each.
2. Compute .
3. Select a small odd integer that is relatively prime to , which equals .
4. Compute as the multiplicative inverse of e, modulo .
5. Publish the pair as the participant's RSA public key.
6. Keep secret the pair as the participant's RSA secret key.

To transform a message associated with a public key compute

To transform a ciphertext associated with a secrete key compute

Proof

We have that for any M,

By Chinese remainder theorem,

Miscs

- The security of the RSA cryptosystem rests in large part on the difficulty of factoring large integers
- Shor algorithm in quantum computer.
- In order to achieve security with the RSA cryptosystem, however, we should use integers that are quite long—hundreds or even more than one thousand bits long to resist possible advances in the art of factoring
- For efficiency, RSA is often used in a “hybrid” or “key-management” mode with fast non-public-key cryptosystems
- A hybrid approach to make digital signatures efficiently. This approach combines RSA with a public collision-resistant hash function h - a function that is easy to compute but for which it is computationally infeasible to find two messages and such that .
- We note that the use of certificates makes distributing public keys much easier.

References

1. Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, and Clifford Stein. Introduction to Algorithms, chapter 31. The MIT Press, thrid edition, 2009
2. https://www.bilibili.com/video/av54679934/