RSA Cryptosystem

Yufei Tao

Department of Computer Science and Engineering
Chinese University of Hong Kong

In this lecture, we will discuss the RSA cryptosystem, which is widely adopted as a way to

- encrypt a message, or
- digitally sign a message.

Let us start with encryption.

Encryption

Consider that Alice wants to send Bob a message m over the Internet. Let us consider m in its binary form, namely, m is a sequence of 0's and 1's, and therefore, can also be regarded as a (perhaps very big) integer.

As m needs to be delivered over a public network, it may be intercepted by a hacker. Our goal is to encrypt m into another integer C so that

- It is very difficult for the hacker to infer m from C.
- It is very easy for Bob to restore m from C.

C is therefore called a ciphertext.

Encryption

RSA achieves the above in three steps.

- Preparation: Bob prepares certain information that will be used by others to encrypt the messages to him. This step is carried out only once, namely, the same information will be used forever.
- Encryption: Alice encrypts her message m for Bob into a ciphertext C.
- Decryption: Bob converts C back to m.

Preparation

Bob carries out the following:

1. Choose two large prime numbers p and q randomly.
2. Let $n = pq$.
3. Let $\phi = (p-1)(q-1)$.
4. Choose a large number $e \in [2, \phi - 1]$ that is co-prime to ϕ.
5. Compute $d \in [2, \phi - 1]$ such that

   $$e \cdot d \quad = \quad 1 \pmod{\phi}$$

   There is a unique such d. Furthermore, d must be co-prime to ϕ.
6. Announce to the whole word the pair (e, n), which is his public key.
7. Keep d secret to himself, which together with n forms his private key.

Example

1. Choose $p = 23$ and $q = 37$.
2. $n = pq = 851$.
3. $\phi = 792$.
4. Choose a number $e = 85$ that is co-prime to ϕ.
5. Compute $d = 205$ such that

$$e \cdot d = 1 \pmod{792}$$

6. Announce to the public key $(85, 851)$.
7. Keep the private key $(205, 851)$.

Encryption

Knowing the public key (e, n) of Bob, Alice wants to send a message $m \leq n$ to Bob. She converts m to C as follows:

$$C = m^e \pmod{n}$$

Example

From the previous slide, Bob's public key is (85, 851). Assume that $m = 583$. Then:

$$\begin{aligned} C &= 583^{85} \pmod{851} \\ &= 395 \end{aligned}$$

Alice sends C to Bob.

Decryption

Using his private key (d, n), Bob recovers m from C as follows:

$$m = C^d \pmod{n}$$

The above equation is guaranteed to hold.

Example

In preparation, Bob has obtained his private key is (205, 851) (which he keeps secret). So he calculates:

$$\begin{aligned} m &= 596^{205} \pmod{851} \\ &= 583 \end{aligned}$$

namely, the message from Alice.

How to break RSA?

1. Factor n back into p and q.
    - Once this is done, essentially the entire preparation carried out by Bob has been revealed. So the following steps become trivial.
2. Obtain ϕ.
3. Compute d from e and ϕ.
4. Convert C using d and n back into m.

In our earlier example, the encryption can be easily broken because it is trivial to factor $n = 851$ into $p = 23$ and $q = 37$. However, this is because both p and q are small.

The presumed security of RSA is based on the following hypothesis:

Assumption

When primes p and q are big, it is computationally intractable to factor $n = pq$.

In practice, p and q should both be, for example, 1024 bits long.

WARNING

The best factorization algorithm known today requires excessively long time (e.g., a month) to factor a large n even on the fastest computer. However, nobody has ever proved that the hypothesis is correct. Even worse, nobody has ever proved that factoring n is the fastest way to break RSA. In other words, there may exist a clever algorithm (for either factoring n or breaking RSA in a different manner) that remains undiscovered yet. Once found, RSA algorithm will become insecure, and therefore, obsolete.

Digital Signature

Now consider that Bob wants to send a message m to Alice. He does not mind if a hacker can see the message, but he wants to make sure that m is not altered. Or equivalently, he wants Alice to be able to detect whether the message she receives has ever been changed by a hacker along its delivery.

Digital Signature

Bob does the following:

1. Using his privacy key (d, e), compute

$$S = m^d \pmod{n}$$

2. Send Alice the pair (m, S).
   - S is often referred to as the signature.

Alice, after receiving (m, S), does the following:

1. Using Bob's public key (e, n), compute

$$m' = S^e \pmod{n}$$

2. m has not been altered if and only if $m = m'$.

Example

Recall that Bob has private key (205, 851), and public key (85, 851). Suppose that he wants to send Alice a message $m = 672$. He does the following:

1. Calculate

$$\begin{aligned} S &= 672^{205} \pmod{851} \\ &= 339 \end{aligned}$$

2. Send Alice the pair $(672, 339)$.

Example (cont.)

After receiving $(672, 339)$, Alice does the following using Bob's public key (85, 851):

1. Calculate

$$\begin{aligned} m' &= 339^{85} \pmod{851} \\ &= 672 \end{aligned}$$

2. Since $m' = m$, Alice believes that m has not been altered.