The RSA Public Key Cryptosystem

|Dr. Kusan Biswas*|kusan.biswas@dseu.ac.in

August 31, 2025

The RSA Public Key Cryptosystem, named after its inventors Ron Rivest, Adi Shamir and Leonard Adleman is on of the most important cryptographic algorithms. It is a key part of the TLS and SSL protocols which are the backbones of internet security. In RSA cryptosystem, all parties first generate their key-pairs. In our case, let's say there are two parties – Amit and Rakesh who wish to send and receive encrypted data among themselves. Both Amit and Rakesh generates their key-pairs. Amit generates his public and private keys and similarly Rakesh also generates his public and private key. Amit and Rakesh make their public keys public, but saves the privates keys secretly. This means, Amit knows Rakesh's public key and Rakesh also knows Amit's public key. However, Amit's private key is known only to Amit and no one else. Same goes for Rakesh's private key.

The most important point to remember about the RSA (or any public key cryptosystem for that matter) is that the keys of a key-pair are related. They are related in the sense that, data encrypted with one public key can only be decrypted with the corresponding private key. In our example, data encrypted with Amit's public key can only be decrypted with Amit's private key!

Now suppose Rakesh wants to send encrypted data to Amit. He encrypts the plaintext using Amit's public key and sends the ciphertext to Amit. This ciphertext can only be decrypted by Amit, because Amit's private key is is available only with Amit and no one else. Since Rakesh knows that this ciphertext can only be decrypted by Amit, Rakesh does not need to worry about eavesdropping in the communication channel. He can be sure that even if he broadcasts the ciphertext, nobody except Amit would be able to decrypt it!

The RSA Algorithm

1. Key generation by Amit
   - Select large primes p and q
   - Calculate $n = pq$
   - Calculate $\phi(n) = (p-1)(q-1)$
   - Select integer e such that $gcd(\phi(n), e) = 1$ and $1 < e < \phi(n)$
   - Calculate d such that $ed \equiv 1 \, mod \, \phi(n)$
   - Now, Amit's Public Key is: $K_{Pub}^{Amit} = \{e, n\}$
   - And Amit's Private Key is: $K_{Pvt}^{Amit} = \{d, n\}$
2. Encryption by Rakesh,(the sender) using Amit's Public Key
   - Plaintext is M such that $M < n$
   - Computer ciphertext $C = M^n \, mod(n)$
3. Decryption by Amit (the receiver) using Amit's Private Key
   - Ciphertext C (received from Rakesh)
   - Decrypt and get plaintext message $M = C^d \, mod(n)$

An Example

1. Key generation by Amit
   - Select large(!) primes $p = 3$ and $q = 11$. Small values are taken for the ease of calculation in this example.
   - Therefore, $n = pq = 3 \times 11 = 33$
   - Therefore, $\phi(n) = (p-1)(q-1) = (3-1)(11-1) = 2 \times 10 = 20$

*Typeset in markdown backed by LaTeX! Hosted at https://github.com/kusanvision/NOTES

- Select integer e such that $gcd(20, e) = 1$ and $1 < e < 20$. We can take $e = 3$, because $gcd(20, 3) = 1$, because 20 and 3 do not have any common factor.
- Calculate d such that $3 \times d \equiv 1 \, mod \, 20$. We see that $d = 7$ satisfies the condition. Because, $3 \times 7 \equiv 1 \, mod \, 20$.
- Now, Amit's Public Key is: $K_{Pub}^{Amit} = \{3, 33\}$
- And Amit's Private Key is: $K_{Pvt}^{Amit} = \{7, 33\}$

2. Encryption by Rakesh (the sender) using Amit's Public Key
   - Let's say plaintext message is $M = 5$.
   - Computer ciphertext $C = 5^3 \, mod \, 33$

$$\begin{aligned} C &= 5^3 \, mod \, 33 \\ &= 125 \, mod \, 33 \\ &= 26 \end{aligned}$$

3. Decryption by Amit (the receiver) using Amit's Private Key
   - Ciphertext $C = 26$ (received from Rakesh)
   - Decrypt and get plaintext message $M = C^d \, mod(n) = 26^7 \, mod \, 33$

$$\begin{aligned} M &= 26^7 \, mod \, 33 \\ &= \Big((26 \times 26) \, mod \, 33 \times (26 \times 26) \, mod \, 33 \times (26 \times 26) \, mod \, 33 \times 26 \, mod \, 33 \Big) \, mod \, 33 \\ &= (16 \times 16 \times 16 \times 26) \, mod \, 33 \\ &= 106496 \, mod \, 33 \\ &= 5 \end{aligned}$$

Exercises

1. Take $p = 5$, $q = 11$ and plaintext message $M = 9$. Take a suitable value of e. Then calculate d and compute the ciphertext C. Then decrypt C.
2. Take $p = 7$, $q = 11$. Take $e = 17$. Compute d and then encrypt $M = 8$
3. Take $p = 11$, $q = 13$, $e = 11$ and message $M = 7$. Compute d and encrypt M.