TUTORIAL

CRYPTOGRAPH

Y

Asymmetric Key – Public Key Cryptography

I. RSA Encryption Algorithm

RSA encryption algorithm is a type of public-key encryption algorithm. To better understand RSA, lets first understand what is public-key encryption algorithm.

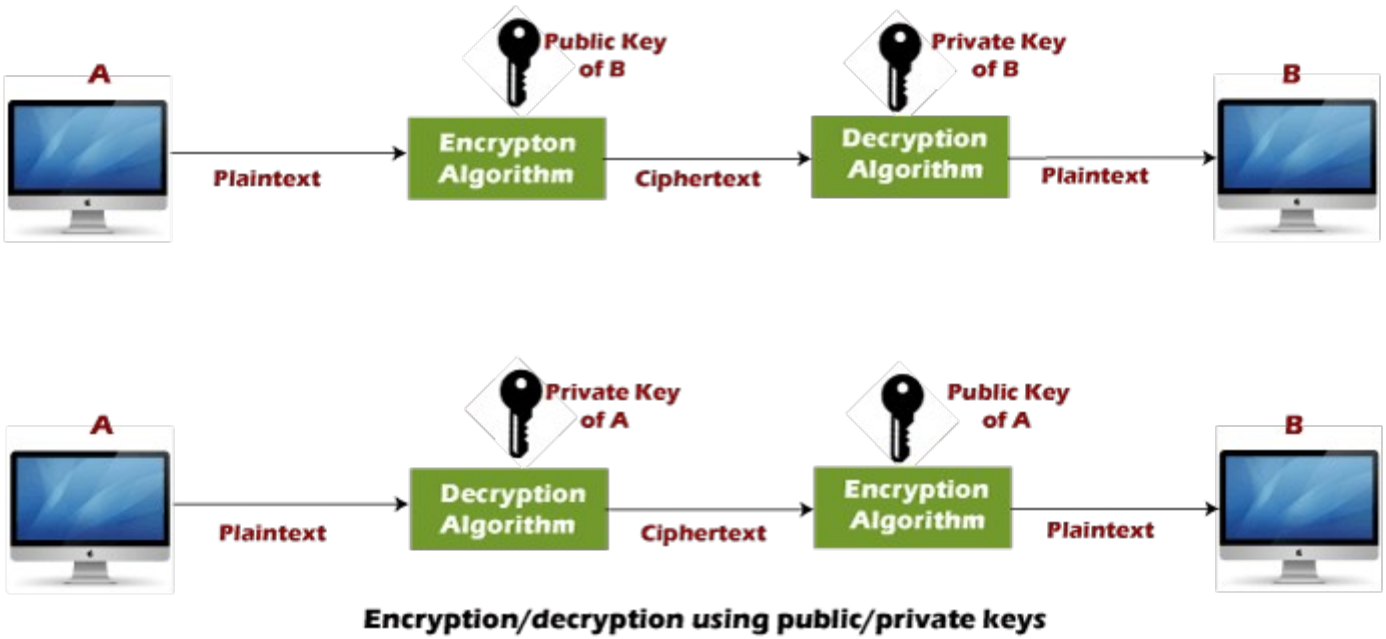
Public key encryption algorithm:

Public Key encryption algorithm is also called the Asymmetric algorithm. Asymmetric algorithms are those algorithms in which sender and receiver use different keys for encryption and decryption. Each sender is assigned a pair of keys:

- **Public key**
- **Private key**

The **Public key** is used for encryption, and the **Private Key** is used for decryption. Decryption cannot be done using a public key. The two keys are linked, but the private key cannot be derived from the public key. The public key is well known, but the private key is secret and it is known only to the user who owns the key. It means that everybody can send a message to the user using user's public key. But only the user can decrypt the message using his private key.

The Public key algorithm operates in the following manner:

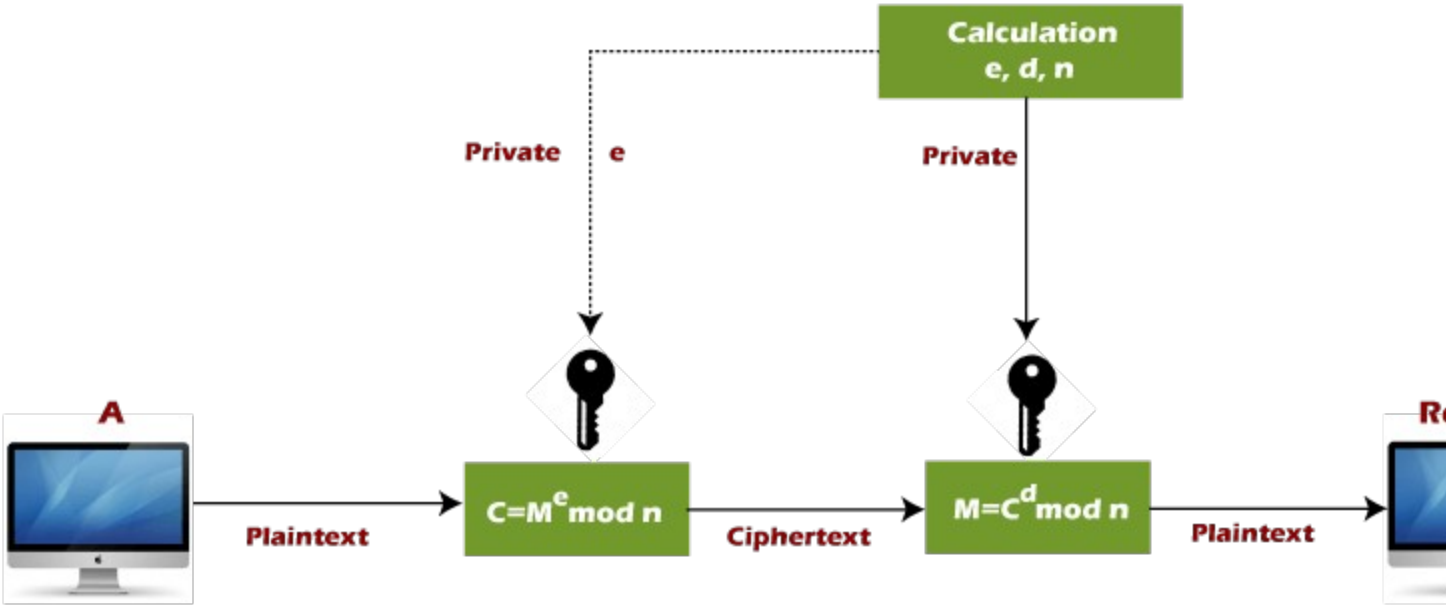


Encryption/decryption using public/private keys

- The data to be sent is encrypted by sender **A** using the public key of the intended receiver
- B decrypts the received ciphertext using its private key, which is known only to B. B replies to A encrypting its message using A's public key.
- A decrypts the received ciphertext using its private key, which is known only to him.

RSA encryption algorithm:

RSA is the most common public-key algorithm, named after its inventors **Rivest, Shamir, and Adelman (RSA).**



RSA

RSA algorithm uses the following procedure to generate public and private keys:

- Select two large prime numbers, p and **q**.
- Multiply these numbers to find **n = p x q,** where **n** is called the modulus for encryption and decryption.
- Choose a number **e** less than **n**, such that n is relatively prime to **(p - 1) x (q -1).** It means that **e** and **(p - 1) x (q - 1)** have no common factor except 1. Choose "e" such that 1<e < φ (n), e is prime to φ (n), **gcd (e,d(n)) =1**
- If **n = p x q,** then the public key is <e, n>. A plaintext message **m** is encrypted using public key <e, n>. To find ciphertext from the plain text following formula is used to get ciphertext C.
  $C = m^e \bmod n$
  Here**, m** must be less than **n**. A larger message (>n) is treated as a concatenation of messages, each of which is encrypted separately.
- To determine the private key, we use the following formula to calculate the d such that:
  $D_e \bmod \{(p - 1) x (q - 1)\} = 1$
  Or
  $D_e \bmod \varphi(n) = 1$
- The private key is <d, n>. A ciphertext message **c** is decrypted using private key <d, n>. To calculate plain text **m** from the ciphertext c following formula is used to get plain text m.
  $m = c^d \bmod n$

Let's take some example of RSA encryption algorithm:
Example 1:

This example shows how we can encrypt plaintext 9 using the RSA public-key encryption algorithm. This example uses prime numbers 7 and 11 to generate the public and private keys.

Explanation:

Step 1: Select two large prime numbers, p, and **q**.

p = 7

q = 11

Step 2: Multiply these numbers to find **n = p x q,** where **n** is called the modulus for encryption and decryption.

First, we calculate

n = p x q

n = 7 x 11

n = 77

Step 3: Choose a number **e** less that **n**, such that n is relatively prime to **(p - 1) x (q -1).** It means that **e** and **(p - 1) x (q - 1)** have no common factor except 1. Choose "e" such that 1<e < φ (n), e is prime to φ (n), gcd (e, d (n)) =1.

Second, we calculate

φ (n) = (p - 1) x (q-1)

φ (n) = (7 - 1) x (11 - 1)

φ (n) = 6 x 10

φ (n) = 60

Let us now choose relative prime e of 60 as 7.

Thus the public key is <e, n> = (7, 77)

Step 4: A plaintext message **m** is encrypted using public key <e, n>. To find ciphertext from the plain text following formula is used to get ciphertext C.

To find ciphertext from the plain text following formula is used to get ciphertext C.

$C = m^e \bmod n$

$C = 9^7 \bmod 77$

$C = 37$

Step 5: The private key is <d, n>. To determine the private key, we use the following formula d such that:

$D_e \bmod \{(p - 1) \times (q - 1)\} = 1$

7d mod 60 = 1, which gives d = 43

The private key is <d, n> = (43, 77)

Step 6: A ciphertext message **c** is decrypted using private key <d, n>. To calculate plain text **m** from the ciphertext c following formula is used to get plain text m.

$m = c^d \bmod n$

$m = 37^{43} \bmod 77$

m = 9

In this example, Plain text = 9 and the ciphertext = 37

Example 2:

In an RSA cryptosystem, a particular A uses two prime numbers, 13 and 17, to generate the public and private keys. If the public of A is 35. Then the private key of A is .....?.

Explanation:

Step 1: in the first step, select two large prime numbers, **p** and **q**.

p = 13

q = 17

Step 2: Multiply these numbers to find **n = p x q,** where **n** is called the modulus for encryption and decryption.

First, we calculate

n = p x q

n = 13 x 17

n = 221

Step 3: Choose a number **e** less that **n**, such that n is relatively prime to **(p - 1) x (q -1).** It means that **e** and **(p - 1) x (q - 1)** have no common factor except 1. Choose "e" such that 1<e < φ (n), e is prime to φ (n), gcd (e, d (n)) =1.

Second, we calculate

φ (n) = (p - 1) x (q-1)

φ (n) = (13 - 1) x (17 - 1)

φ (n) = 12 x 16

φ (n) = 192

g.c.d (35, 192) = 1

Step 3: To determine the private key, we use the following formula to calculate the d such that:

Calculate $d = d_e \bmod \varphi(n) = 1$

d = d x 35 mod 192 = 1

d = (1 + k.φ (n))/e [let k =0, 1, 2, 3.....]

Put k = 0

d = (1 + 0 x 192)/35

d = 1/35

Put k = 1

d = (1 + 1 x 192)/35

d = 193/35

Put k = 2

d = (1 + 2 x 192)/35

d = 385/35

d = 11

The private key is <d, n> = (11, 221)

Hence, private key i.e. d = 11

Example 3:

A RSA cryptosystem uses two prime numbers 3 and 13 to generate the public key= 3 and the private key = 7. What is the value of cipher text for a plain text?

Explanation:

Step 1: In the first step, select two large prime numbers, **p** and **q**.

p = 3

q = 13

Step 2: Multiply these numbers to find **n = p x q,** where **n** is called the modulus for encryption and decryption.

First, we calculate

n = p x q

n = 3 x 13

n = 39

Step 3: If **n = p x q,** then the public key is <e, n>. A plaintext message **m** is encrypted using public key <e, n>. Thus the public key is <e, n> = (3, 39).

To find ciphertext from the plain text following formula is used to get ciphertext C.

$C = m^e \bmod n$

$C = 5^3 \bmod 39$

C = 125 mod 39

C = 8

Hence, the ciphertext generated from plain text, C = 8.

Example 4:

A RSA cryptosystem uses two prime numbers, 3 and 11, to generate private key = 7. What is the value of ciphertext for a plain text 5 using the RSA public-key encryption algorithm?

Explanation:

Step 1: in the first step, select two large prime numbers, **p** and **q**.

p = 3

q = 11

Step 2: Multiply these numbers to find **n = p x q,** where **n** is called the modulus for encryption and decryption.

First, we calculate

n = p x q

n = 3 x 11

n = 33

Step 3: Choose a number **e** less that **n**, such that n is relatively prime to **(p - 1) x (q -1).** It means that **e** and **(p - 1) x (q - 1)** have no common factor except 1. Choose "e" such that 1< e < φ (n), e is prime to φ (n), gcd (e, d (n)) =1.

Second, we calculate

φ (n) = (p - 1) x (q-1)

φ (n) = (3 - 1) x (11 - 1)

φ (n) = 2 x 10

φ (n) = 20

Step 4: To determine the public key, we use the following formula to calculate the d such that:

Calculate e x d = 1 mod φ (n)

e x 7 = 1 mod 20

e x 7 = 1 mod 20

e = (1 + k. φ (n))/ d [let k =0, 1, 2, 3.....]

Put k = 0

e = (1 + 0 x 20) / 7

e = 1/7

Put k = 1

e = (1 + 1 x 20) / 7

e = 21/7

e = 3

The public key is <e, n> = (3, 33)

Hence, public key i.e. e = 3

https://www.javatpoint.com/rsa-encryption-algorithm

II. Practice with Public Key Cryptography in Java: RSA

Download code here:

https://drive.google.com/drive/folders/1XwXOXOgU_VJNrUebmgipXHd18XVq8Woa?usp=share_link