Software Design Document

Matemáticas Computacionales

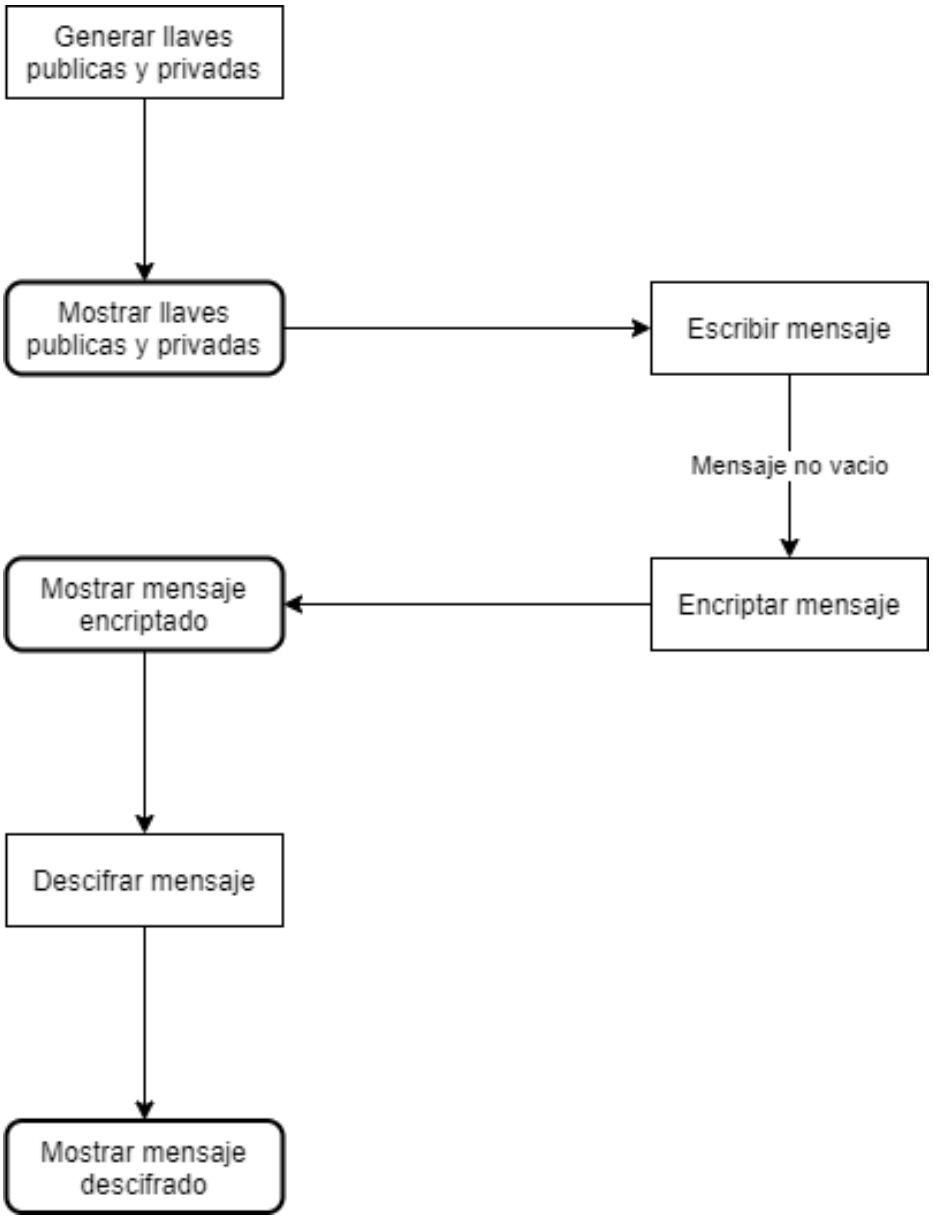
Luis Bodart A01635000
2-6-2021

Índice

CONTENIDO

DIAGRAMAS

VISTA GENERAL



ALGORITMO

VERIFICAR SI ES PRIMO

is_prime(n)

1. Si n es menor o igual a 3.
    a. Si n es mayor a 1, regresa True.
2. Si el resto de dividir n entre 2 o entre 3 es 0, regresa False.
3. Mientras el cuadrado de i sea menor o igual a n.
    a. Si el resto de n entre i es igual a 0 o el resto de n entre i más 2 es igual a 0, regresa False.
4. Regresa True.

DETERMINAR EL MÁXIMO COMÚN DIVISOR

gcd(int a, int b)

1. Mientras b sea diferente de 0, a es igual a b y b es igual al resto de a entre b.
2. Regresa a.

INVERSO MULTIPLICATIVO MODULAR

mod_inverse(int a, int mod)

1. Mientras a sea mayor a 0 y el mod temporal sea diferente de 1, hace los cálculos.
2. Regresa d más mod.

EXPONENCIACIÓN RÁPIDA

fast_pow(int a, int n)

1. Si n es igual a 0, regresa 1.
2. x es igual a fast_pow(a, división entera de n entre 2).
3. x por x.
4. Si el resto de n entre 2 es 1, x es igual a x por a.
5. Regresa x.

GENERAR EL PAR DE LLAVES PÚBLICAS Y PRIVADAS

generate_key_pair()

1. Crea la longitud de bits aleatoria 2^(3-5).
2. Crea el min y max número con longitud de bits similar.
3. Crea el start y stop de los números primos.
4. Genera los números primos hasta stop.
5. Quita los números primos que sean menores a start.
6. Genera p y q de acuerdo con los números primos generados de manera aleatoria asegurando que sean diferentes.
7. Crea n, φ, e y g.
8. Asegura que e y φ sean coprimos.

9. Mientras g sea diferente a 1, vuelve a crear e y g.
10. Crea d.
11. La llave publica es (e, n), guardada como hexadecimal.
12. La llave privada es (d, n), guardada como hexadecimal.

ENCRIPTAR EL MENSAJE

encrypt()

1. Encripta solo si el mensaje no en nulo.
2. key y n se crean con la llave publica (e, n) como int.
3. Cifra el mensaje convirtiendo cada carácter en hexadecimal.

DESCIFRAR EL MENSAJE ENCRIPTADO

decrypt()

1. key y n se crean con la llave privada (d, n) como int.
2. Descifra el mensaje convirtiendo cada carácter hexadecimal a alfabeto.

REPO

Link del repo donde se encuentra el código y el video

https://github.com/Luis99B/RSA_Algorithm

https://youtu.be/JvVAmgv-Z-k