

6-11-2024

**Nombre:** Álvarez García Brandon Azarael

**Nombre de la materia:** Selected topics in cryptography

**Grupo:** 7CM1

**Nombre del profesor:** Dra. Sandra Díaz Santiago

Session 7:

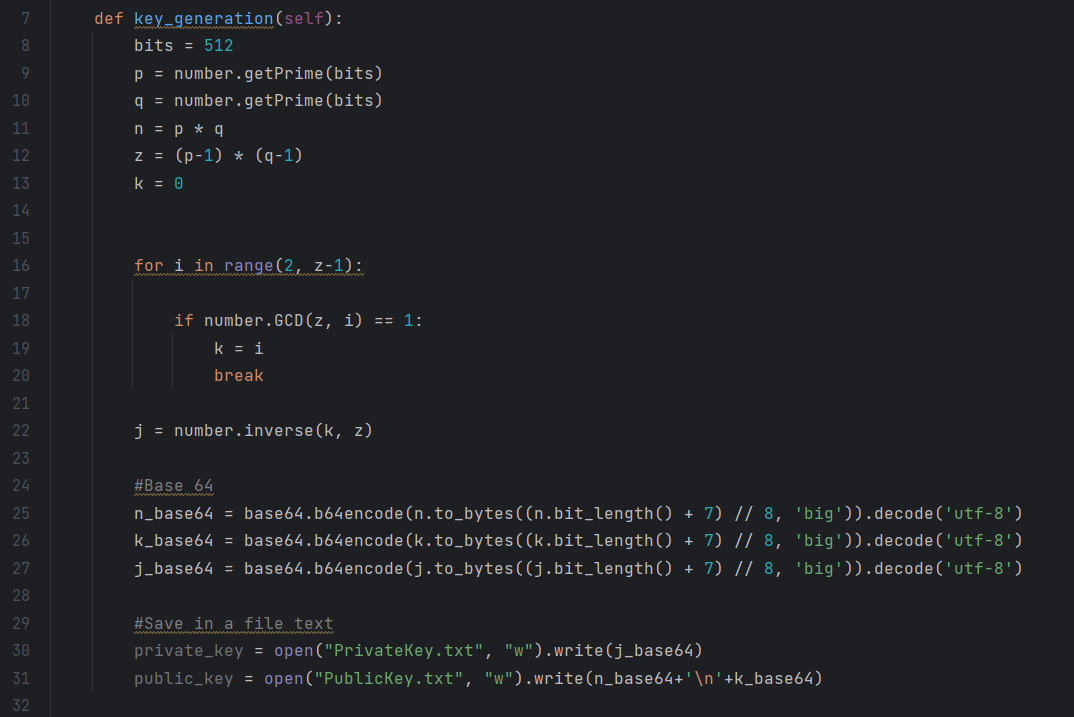
RSA schoolbook

**Ejercicios de programación**

Imagen que contiene Texto

Descripción generada automáticamente

Para esta parte cree una clase llamada RSA, en la cual se crearan los diferentes métodos que se solicitan a lo largo de la práctica, se separa en clases para tener un mejor control y orden en el código, yo me apoye de las librerías de Crypto de Python, para la generación de primos grandes



Se crea el método de key\_generation, el cual devuelve dos archivos de texto, uno incluye la llave publica y el otro la llave privada, y se hacen los cálculos correspondientes de los números primos (p y q) con la longitud de 512 bits, un valor k que sea coprimo con z y j es el calculo del inverso, posteriormente estos valores, se llevan a base 64 y se proceden a guardar en los archivos de texto generados



En esta función se hace el calculo de el texto cifrado, en el cual recibimos un archivo de texto que contiene la llave publica y decodificamos estos valores de base 64 para manejarlos como enteros, se procede a realizar el calculo de cifrado y este resultado se vuelve a pasar a base 64 y esto es lo que retornaremos, el texto cifrado

Texto

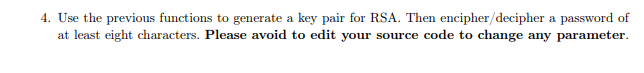
Descripción generada automáticamente



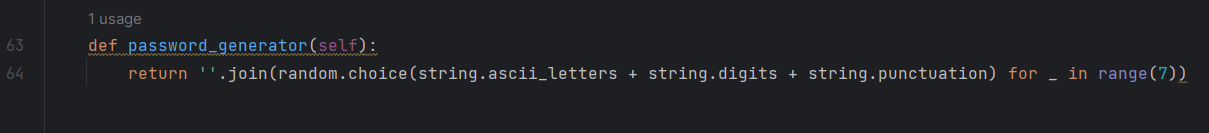
En esta función realizamos el proceso contrario, obteniendo como entradas el archivo de texto donde contiene nuestra llave privada y el texto cifrado, también de la llave publica obtenemos el valor de n para el cálculo, realizamos dicho cálculo de descifrado y lo decodificamos para que pueda ser leído, esto es lo que retorna la función

Texto

Descripción generada automáticamente



Para este punto adicionalmente, se crea un método que genera una contraseña al azar entre letras, número y caracteres de longitud 8



**Pruebas**

Este es el archivo main, en donde simplemente establecemos instancias y mandamos a llamar a los métodos

Texto

Descripción generada automáticamente

Prueba 1

Texto

Descripción generada automáticamente

Prueba 2

Texto

Descripción generada automáticamente

Prueba 3

Texto

Descripción generada automáticamente