



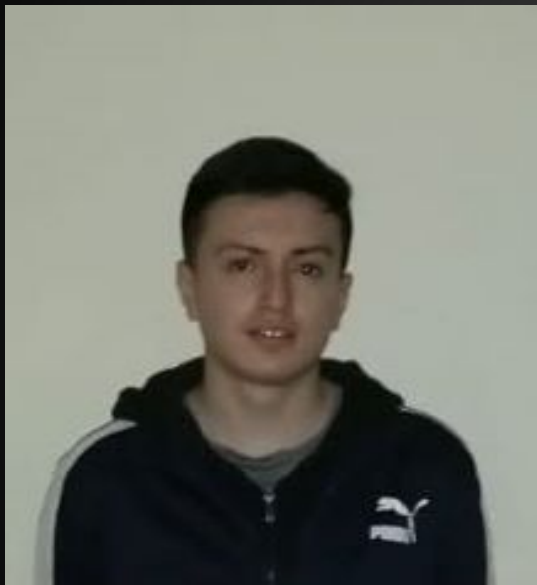
◀ | PyCrypt | ▶

Algoritmos de Encriptación



UNIVERSIDAD
NACIONAL
DE COLOMBIA

Grupo 3
Programación de computadores - G12



Pablo José Flórez Gómez
Ingeniería Electrónica



Nicolas Osorio Guarín
Ingeniería Electrónica



Sergio Andrés Gordillo Gómez
Ingeniería Electrónica

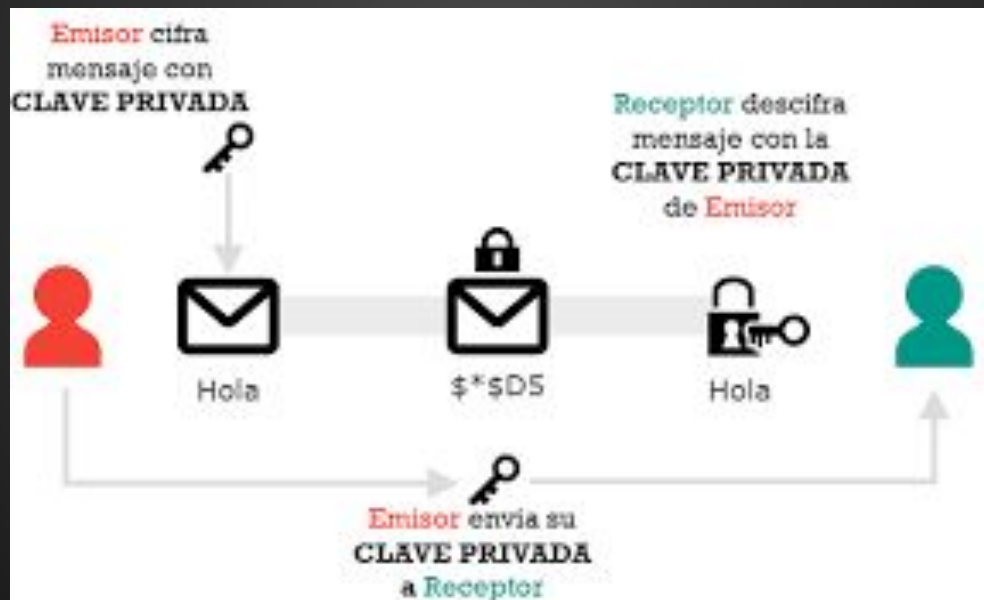
Introducción

¿Que es la Criptografía?



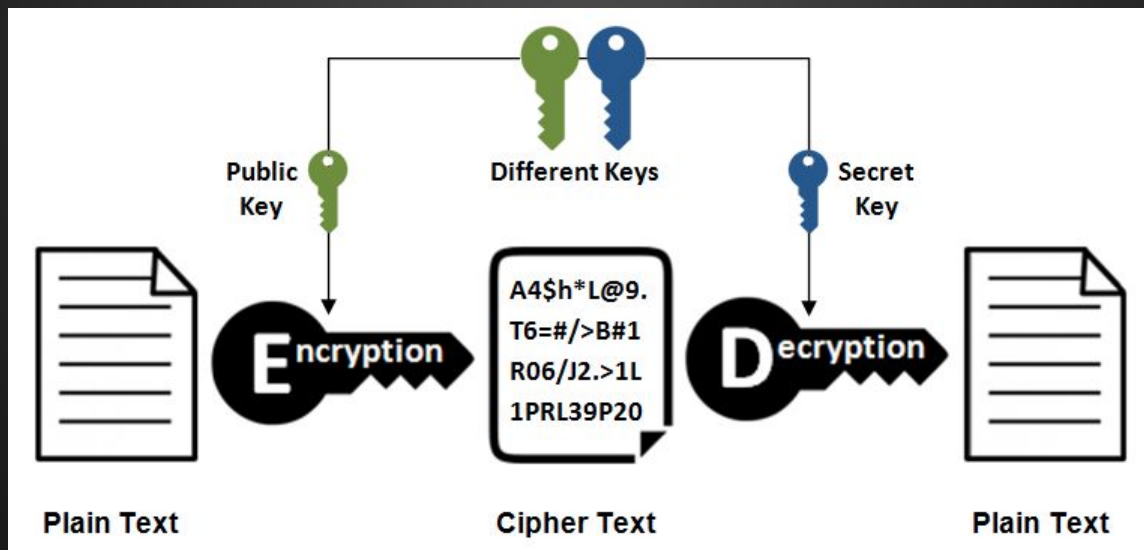
Tipos de criptografía

Simétrica

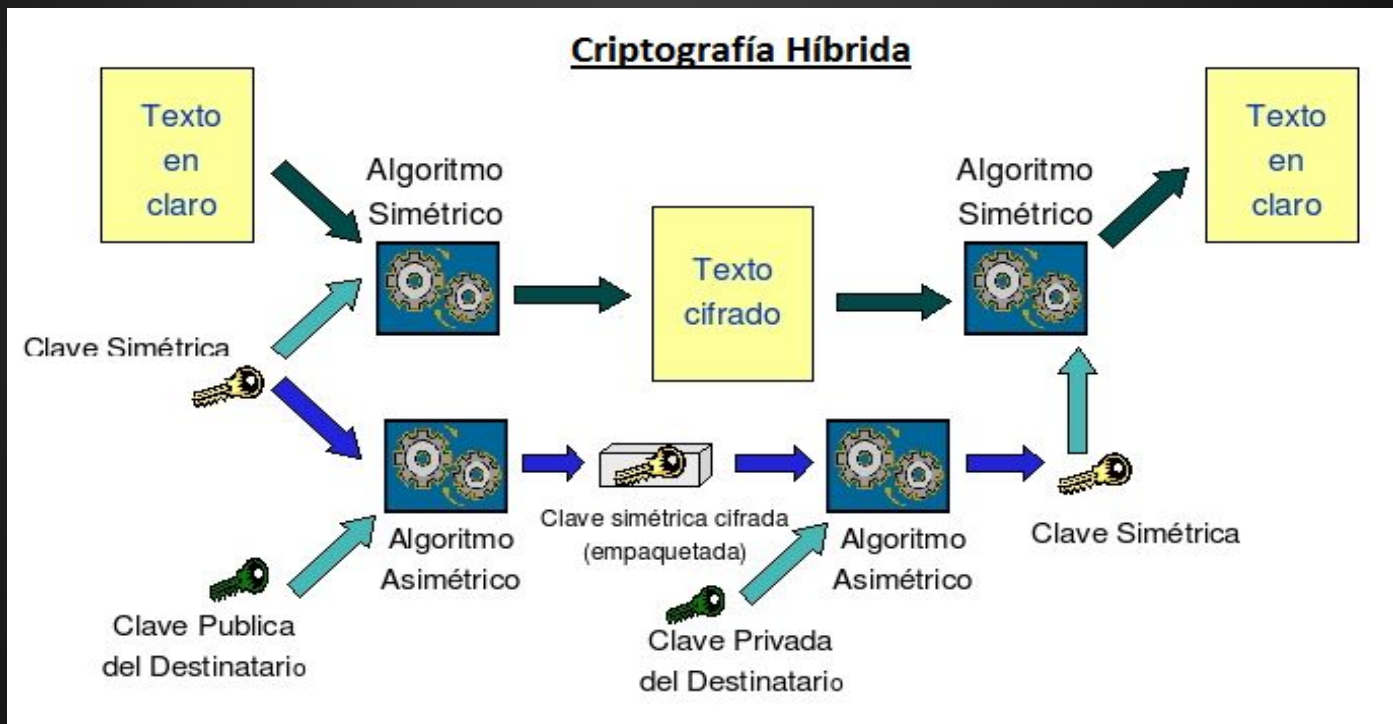


Tipos de criptografía

Asimétrica



Tipos de criptografía

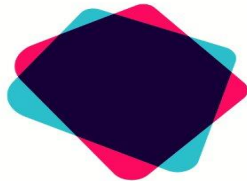




Campos de acción



amazon



NEQUI



REGISTRADURÍA
NACIONAL DEL ESTADO CIVIL



Definición general del proyecto:

Algoritmos de encriptación - PyCrypt

PyCrypt es un proyecto que trabaja con diferentes algoritmos de encriptación. Cada uno de estos algoritmos tiene su propio método de encriptación y desencriptación, sin embargo, todos son algoritmos simétricos. De modo que le permiten al usuario ingresar al usuario su mensaje y a su vez una clave que él desee o en otros casos rotar posiciones del mensaje dependiendo del algoritmo.

Cada uno de los algoritmos, le ofrece al usuario una manera de encriptación propia que siguen ciertas reglas en el programa. No obstante, algunos de los algoritmos no fueron diseñados para admitir todo tipo de caracteres, manteniendo el propósito y las condiciones bajo las cuales fueron creados.



Propósitos y objetivos

PyCrypt

Escoja el método de encriptación

Metodo Cesar

Metodo Solitario

Metodo P-I

Metodo Vigener

Metodo Verman

El proyecto tiene objetivo principal crear un programa en donde el usuario pueda escoger entre diferentes métodos para encriptar y desencriptar mensajes.

Para realizar este programa se utilizará la librería de Python tkinter que cumple con la función de crear la interfaz gráfica que se presenta al usuario.



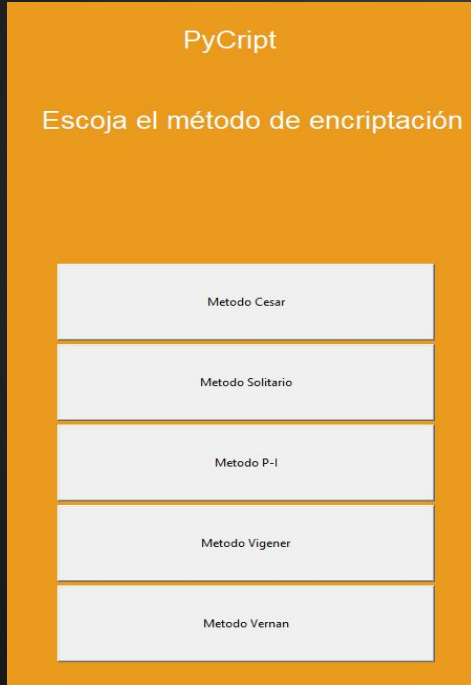
Descripción Web Scraper

El Web Scraper que realizamos extrae datos acerca de 4 de los algoritmos que usamos en nuestro proyecto PyCrypt. Estos datos se extraen directamente de la web y tomamos sólo las partes que necesitamos de información. Por ejemplo, buscamos una pagina con informacion del algoritmo y se extrae los datos que pidamos según nuestro código para utilizar más tarde.

Luego de obtener la información la guardamos y podemos verla mediante el botón de información. Luego de obtener estos datos podemos encriptarla a nuestro gusto posteriormente.



Resultado esperado



The image shows a screenshot of a software application titled "PyCrypt". Below the title, there is a prompt "Escoja el método de encriptación". Underneath this prompt is a vertical list of five buttons, each representing a different encryption method. The buttons are labeled "Metodo Cesar", "Metodo Solitario", "Metodo P-I", "Metodo Vigenere", and "Metodo Vernan".

PyCrypt

Escoja el método de encriptación

Metodo Cesar

Metodo Solitario

Metodo P-I

Metodo Vigenere

Metodo Vernan

El resultado esperado es una interfaz gráfica con un menú que presente los diferentes métodos de encriptación, a partir de este menú el usuario elegirá el método y se abrirá otra ventana para encriptar y desencriptar el mensaje con el método elegido.

Resultado obtenido



El resultado obtenido fue una interfaz muchísimo más atractiva a la primera presentada, esta posee dos nuevos algoritmos de encriptación, (imágenes y un algoritmo asimétrico “RSA”). un botón con información de varios de los algoritmos, que se usaron, un login en el cual se maneja todo el tema de los usuarios y con base a este login nos permite llevar registro con el botón de historial de todos los usuarios por aparte.

Trabajo a futuro

Para el trabajo de PyCrypt a futuro se puede realizar la implementación de archivos para uno de los algoritmos que presentan unas excepciones a la hora de crearlos. Este es un algoritmo realizado por nosotros llamado Par - Impar como su nombre lo indica trabajamos modificando los valores en números pares e impares para llegar a la encriptación. Sin embargo, los caracteres que se usan son UNICODE y al momento de generar un archivo con estos salen de manera errónea. Por lo tanto, se busca a futuro que esta salida sea la correcta y se pueda almacenar en los archivos como se hizo con los demás algoritmos de encriptación.





Conclusiones

- Trabajar con algoritmos asimétricos es más seguro que los simétricos por la complejidad que tiene su método de encriptación. Sin embargo, los algoritmos simétricos no son malos y tienen otros fines de menor relevancia la hora de tomar datos pero igual de necesarios.
- Se aprendió a cómo manejar el tiempo para gestionar los posibles problemas que surgen al momento de unificar un código que es extenso y posee varias subproblemas.
- Estamos satisfechos con el programa ya que permite darle un plus de seguridad a todos los mensajes o información que deseemos encriptar.