Uso de técnicas de cifrado en la ciberseguridad

En esta lección se estudiarán las técnicas de cifrado y su desempeño en la ciberseguridad. Para las actividades de aprendizaje activo en clase, es necesario orientar a los estudiantes a la instalación de software que les permita escribir código en Python, se recomienda emplear visual studio code y un intérprete de Python desde la versión 3.6 en adelante. Al momento de escritura de este documento, la versión más reciente es Python 3.13, sin embargo, se recomienda continuar con Python 3.10

Instalación de visual studio code

Visual studio code es un editor de texto que puede ser personalizado con plugin y sirve como entorno integrado de desarrollo. Entre sus ventajas es que es un software libre y gratuito mantenido por Microsoft. Se puede descargar desde: https://code.visualstudio.com/download , allí se debe seleccionar el sistema operativo con el que cada estudiante cuenta, y descargar el archivo instalador. (ver imagen 1)

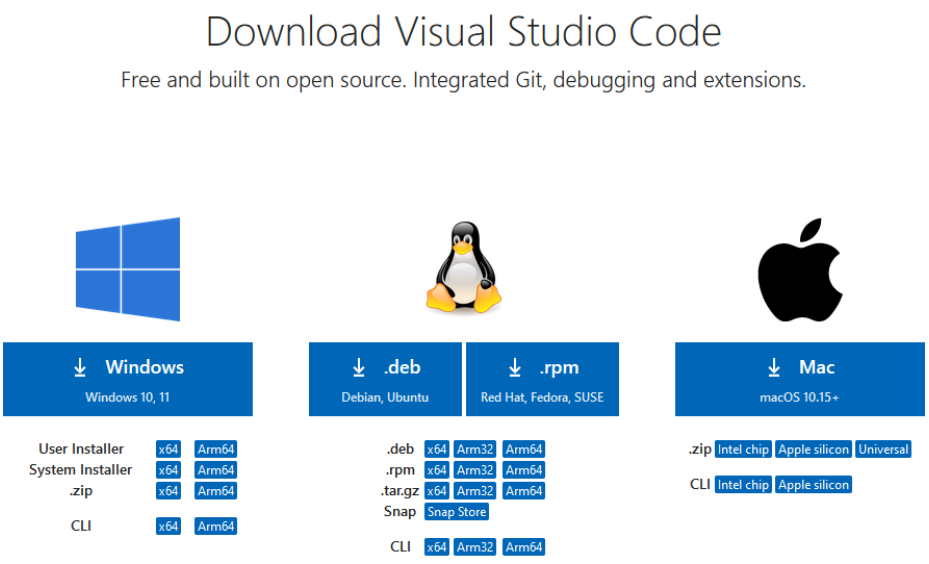

Imagen 1: selección del sistema operativo.

Una vez descargado en el computador local, se debe hacer doble clic al programa de instalación y seguir con el asistente de instalación (figura 2).

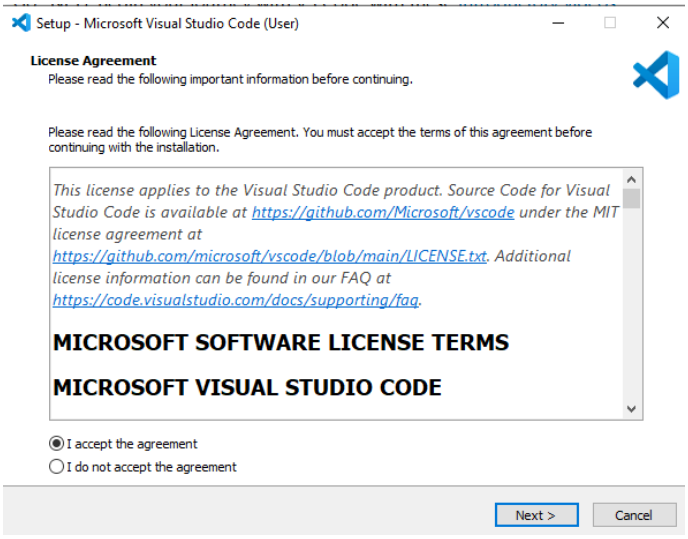

Figura 2: inicio del proceso de instalación.

Se recomienda marcar las opciones vistas en la figura 3:

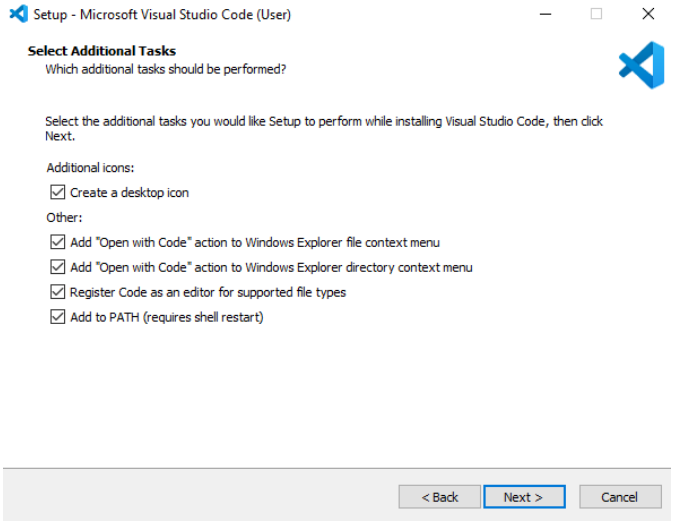

Figura 3 opciones de instalación a seleccionar.

Una vez termine la instalación, verificar que la casilla de la figura 4 esté marcada y dar clic en finalizar para lanzar el programa

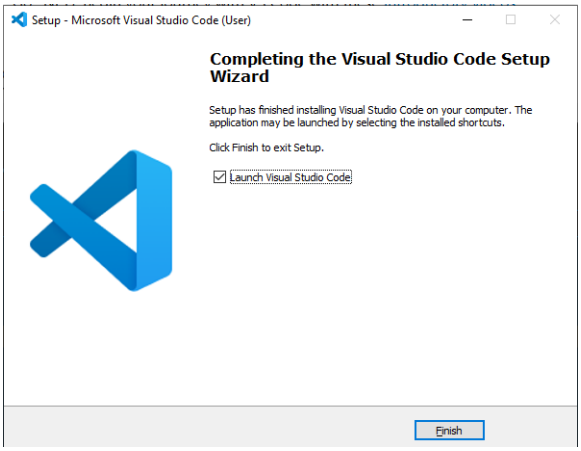

Figura 4: Instalador de visual studio code

Al abrir el programa, este pedirá que se seleccione un tema de colores, como se muestra en la figura 5. Se puede escoger cualquiera (es intercambiable en cualquier momento), Para seleccionarlos basta con hacer doble clic en el color deseado.

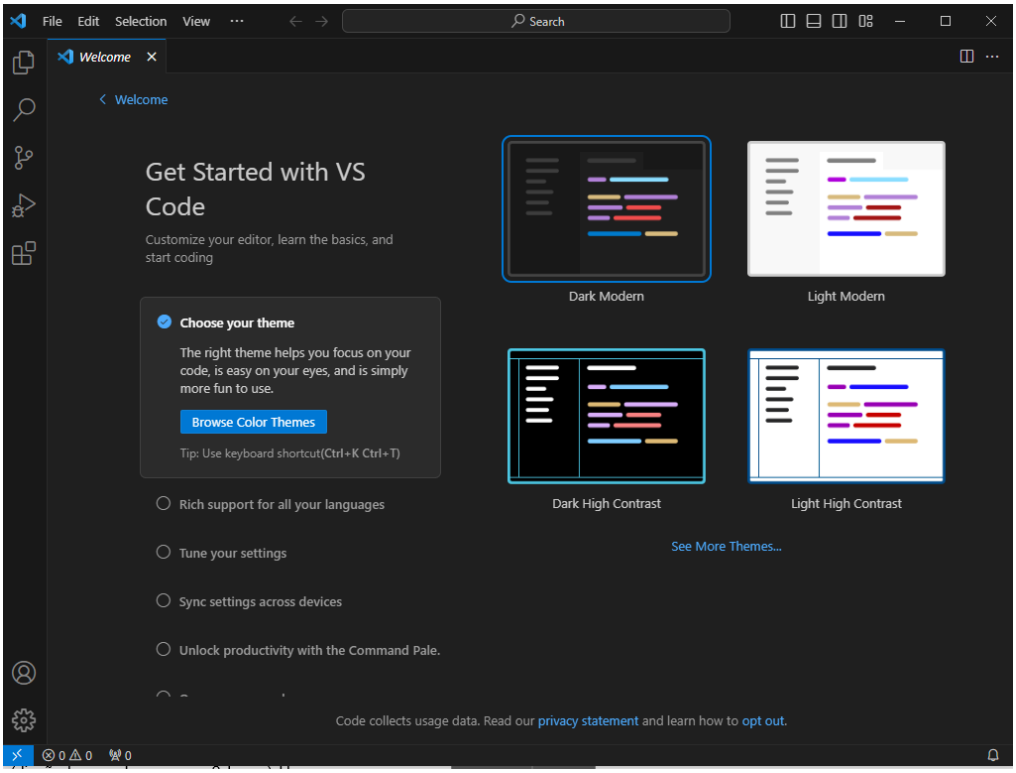

Figura 5: selección del tema de color

Instalación del intérprete de Python

Para continuar con la instalación del intérprete, los estudiantes deben dirigirse a la página: https://www.python.org/downloads/ y hacer clic en el botón downloads y luego en Windows (o en el sistema operativo necesario) como se muestra en la figura 6.

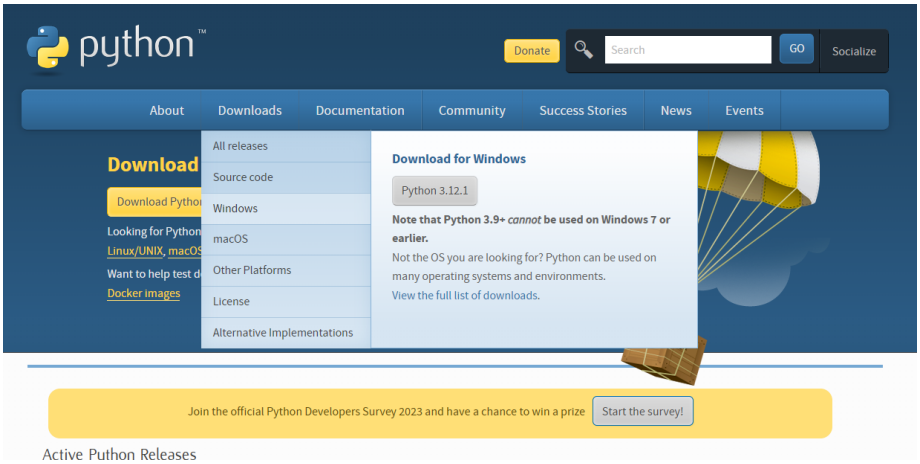

Figura 6: página de descarga de Python

Posteriormente saldrá una lista de versiones, debemos escoger la versión de Python 3.10.11 de abril 5 de 2023, (ir a la parte inferior de la página o buscarlo con el Finder) y descargar el paquete llamado Windows installer (64-bit) como se aprecia en la figura 7.

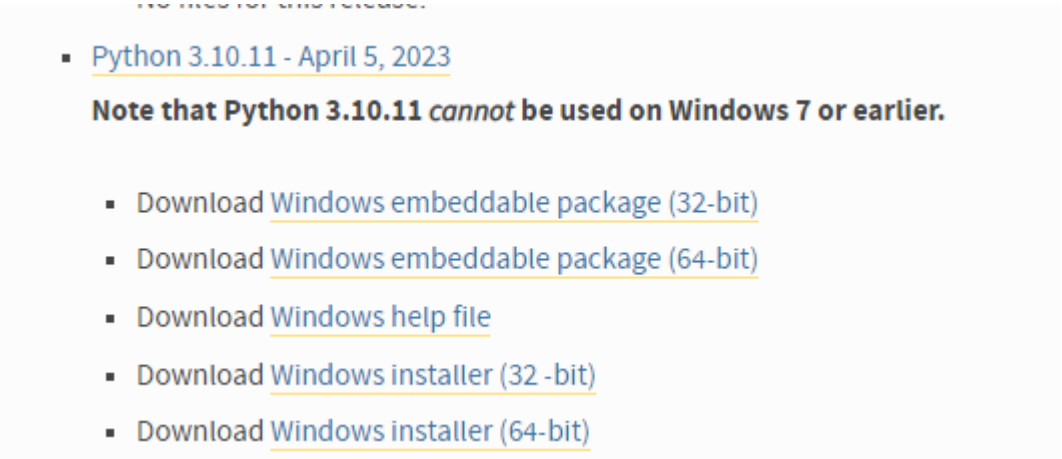

Figura 7: Versiones disponibles de Python y la versión a descargar.

En la primera etapa de la instalación, se debe marcar la casilla Add Python.exe to path como se ve en la figura 8. Y luego hacer clic en el botón con el texto (en azul) de Install now

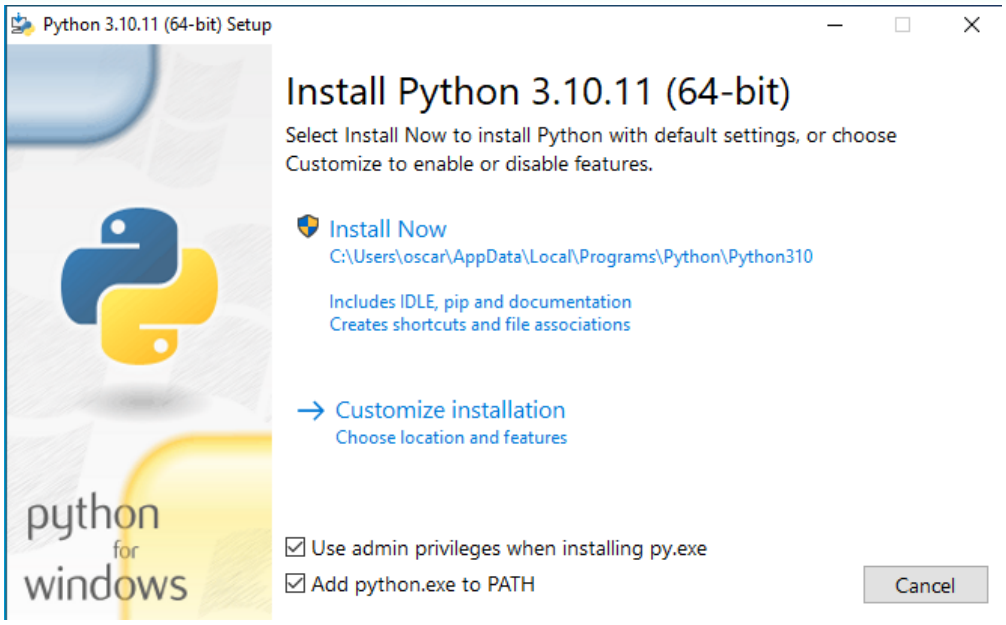

Figura 8: instalación de Python

Al terminar hacer clic en cerrar y ya se encontrará el intérprete instalado (figura 9)

Es **importante en este paso reiniciar** el computador para poder continuar sin problemas.

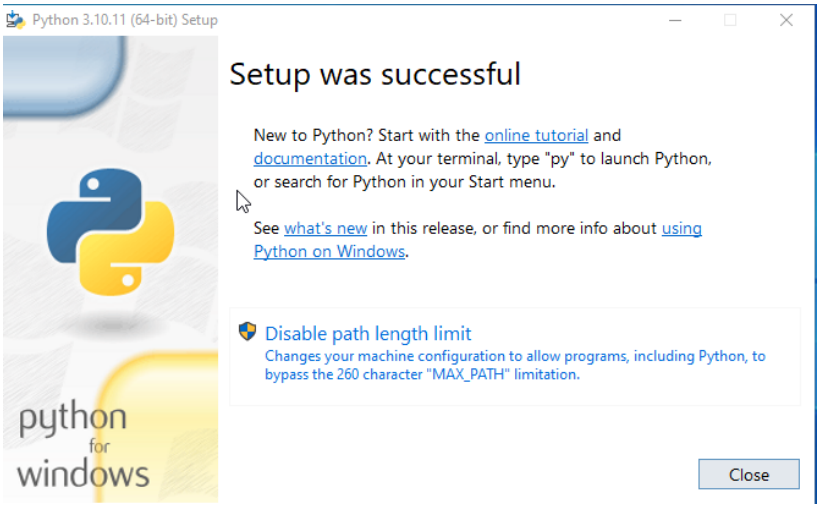

Figura 9, instalación finalizada

Para validar la instalación, se debe abrir el programa instalado visual studio code y hacer clic en el menú file y luego en new text file

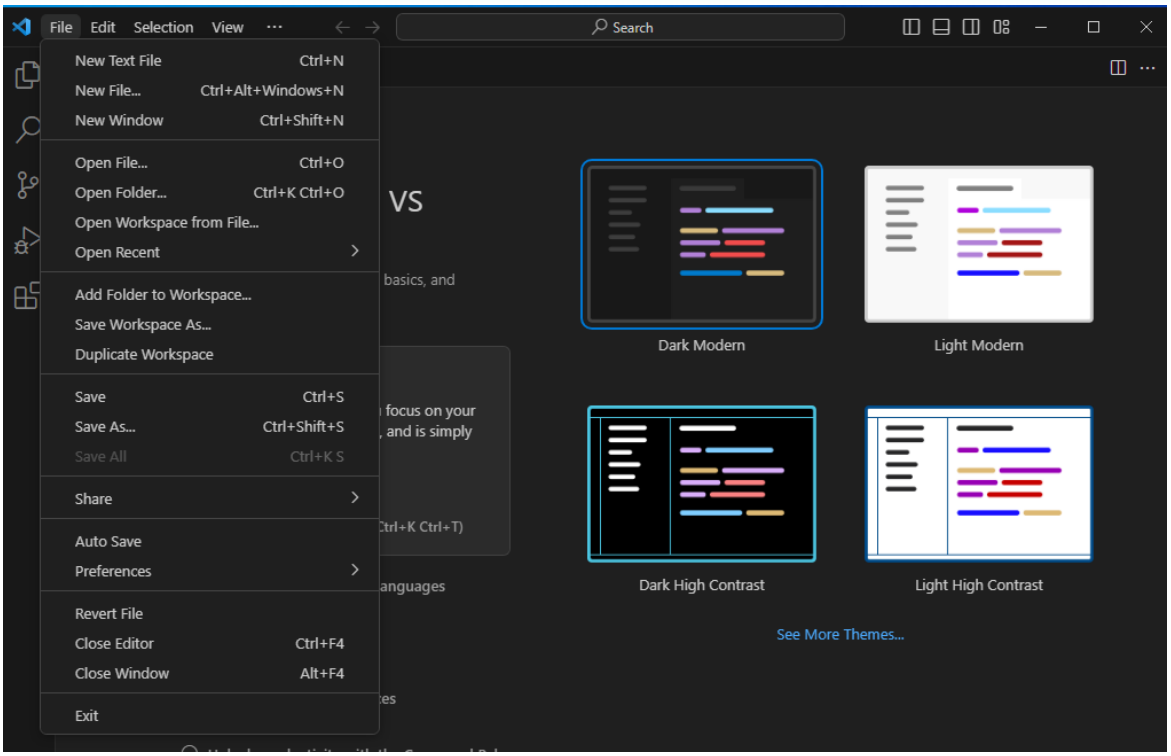

Figura 10: Creando un archivo de Python en visual studio code.

Al crear el archivo, vamos a darle clic en file -> save as y nombrar el archivo como prueba1.py De preferencia guardar en el escritorio para facilitar el proceso. Es importante que la extensión del archivo sea .py para que visual studio code asocie el archivo con el intérprete de python. El resultado se aprecia en la figura 11.

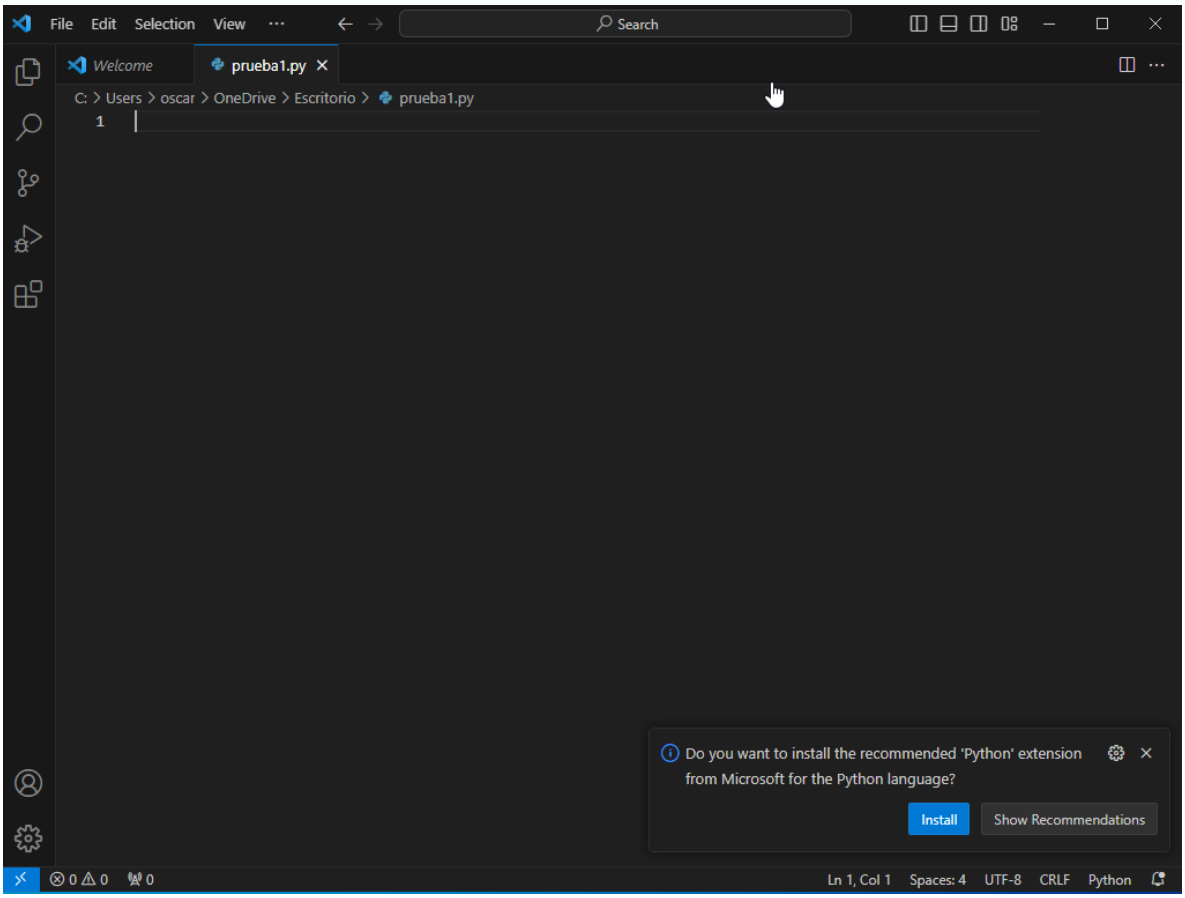

Figura 11: Guardando el script de pruebas

En la figura 11 se ve un recuadro en la parte inferior que sugiere instalar las extensiones de Python, vamos a hacer clic en install (botón azul). Para tener soporte a las funciones automáticas de ayuda para programar en Python.

En caso de que la ventana no aparezca o se haya desaparecido, también se puede ir al panel izquierdo de íconos y seleccionar el último(extensiones) allí se debe buscar Python y se realiza la instalación del plugin como se ve en la figura 12.

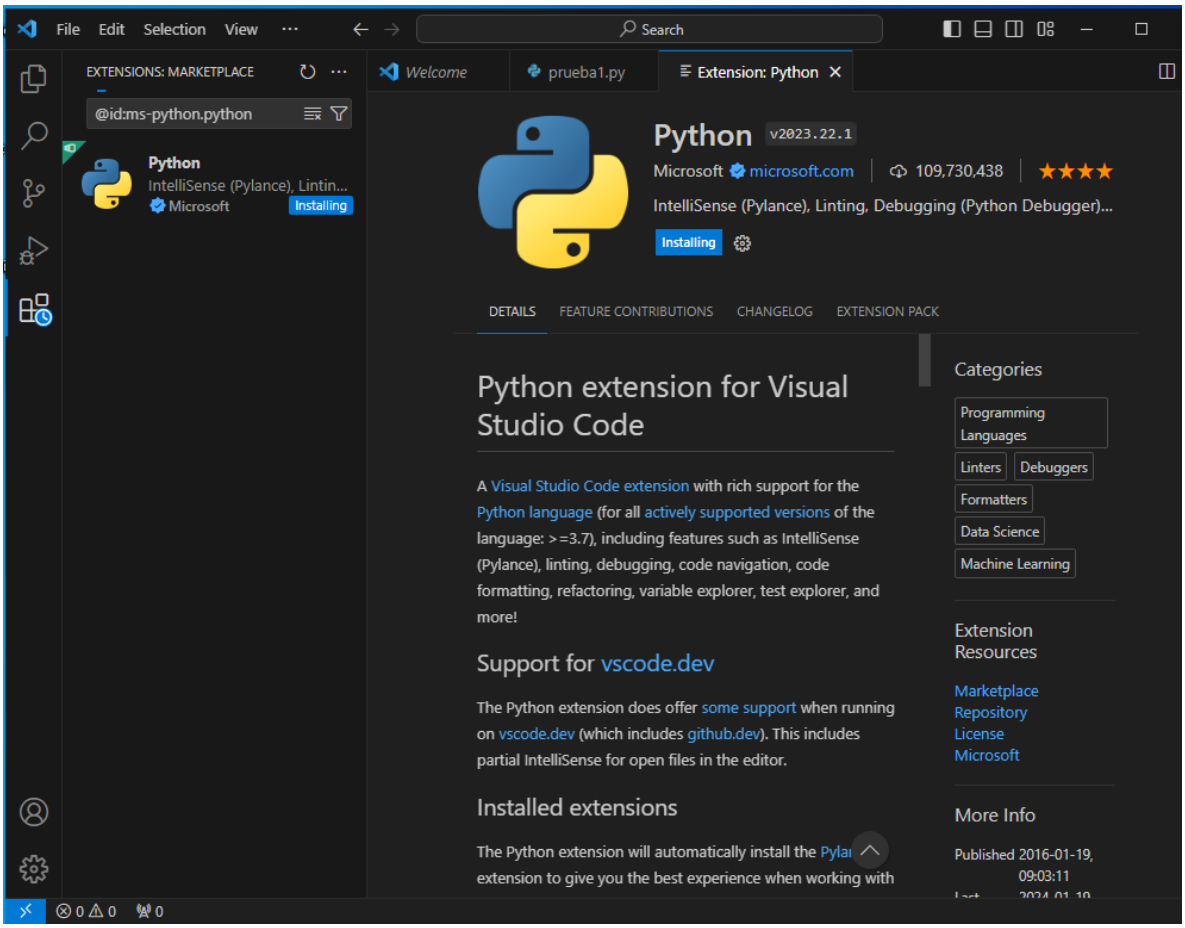

Figura 12 instalación del plugin de Python.

En el editor de texto (archivo prueba1.py) escribir: print(“hola mundo”) y luego procederemos a ejecutar el código con el botón triangular en el panel derecho superior. (figura 13).

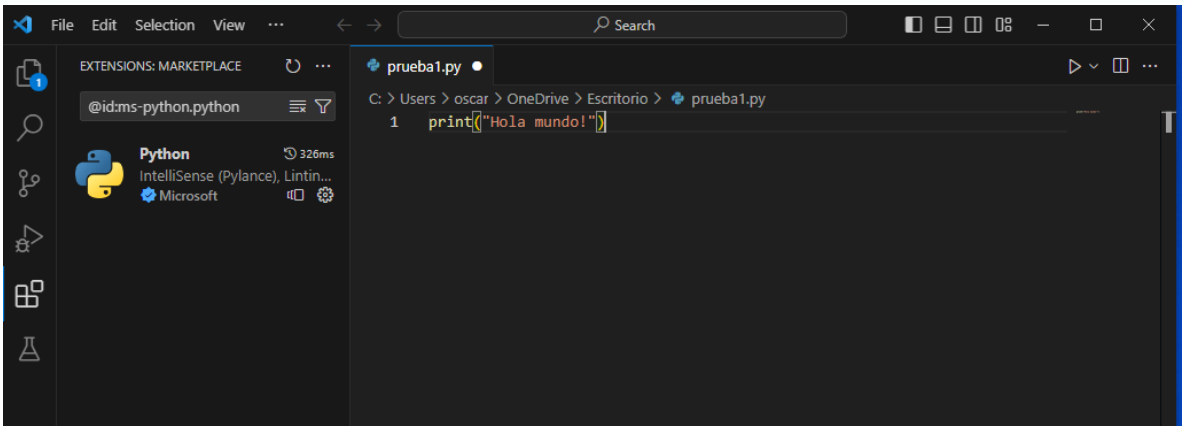

Figura 13: ejecución del primer programa.

Al hacer clic en el botón marcado en la figura 13, se apreciará un panel inferior (terminal) en donde se ve el resultado del programa, en este caso el programa muestra por consola el texto “hola mundo” (figura 14).

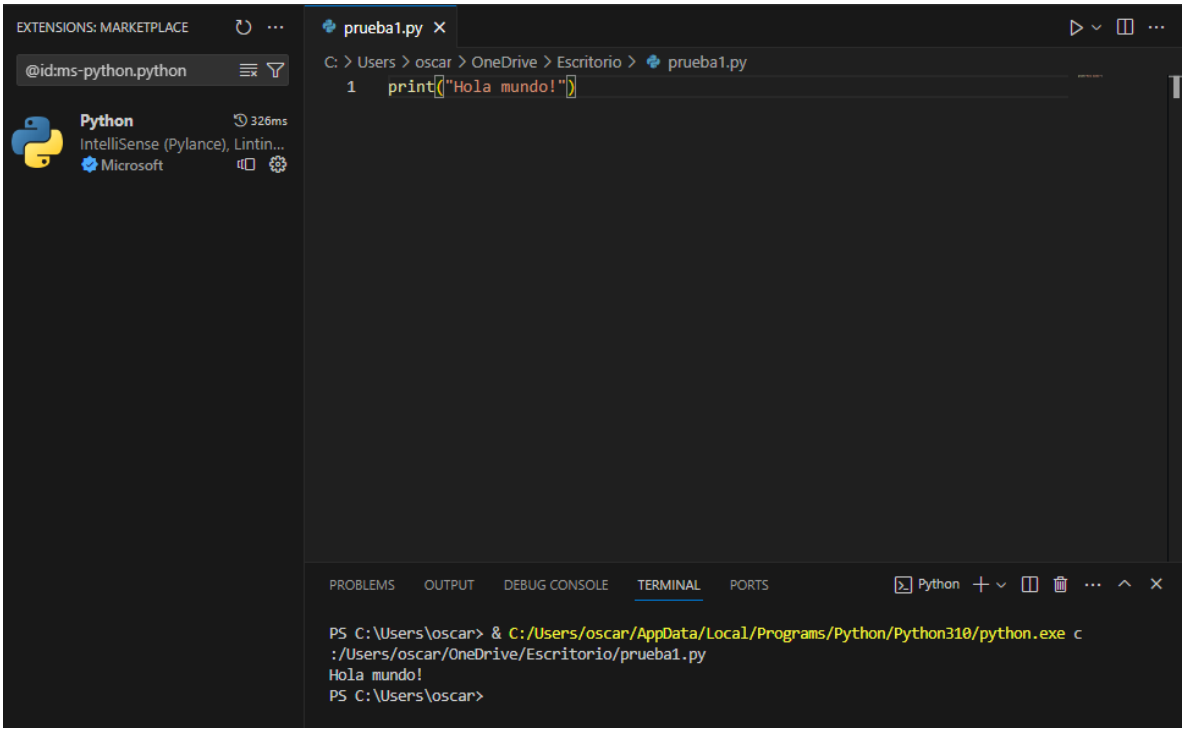

Figura 14: resultado

A continuación, se instalarán algunas librerías necesarias para el análisis de datos como son numpy, pandas y matplotlib. Tal instalación se realiza con el gestor de paquetes de Python llamado Pip, la instalación de un paquete requiere saber el nombre del paquete y escribir en la terminal: pip install (nombre del paquete).

Por ejemplo, para instalar las librerías podemos escribir en la terminal y ejecutar los siguientes comandos:

pip install numpy pandas

tal como se muestra en la figura 15.

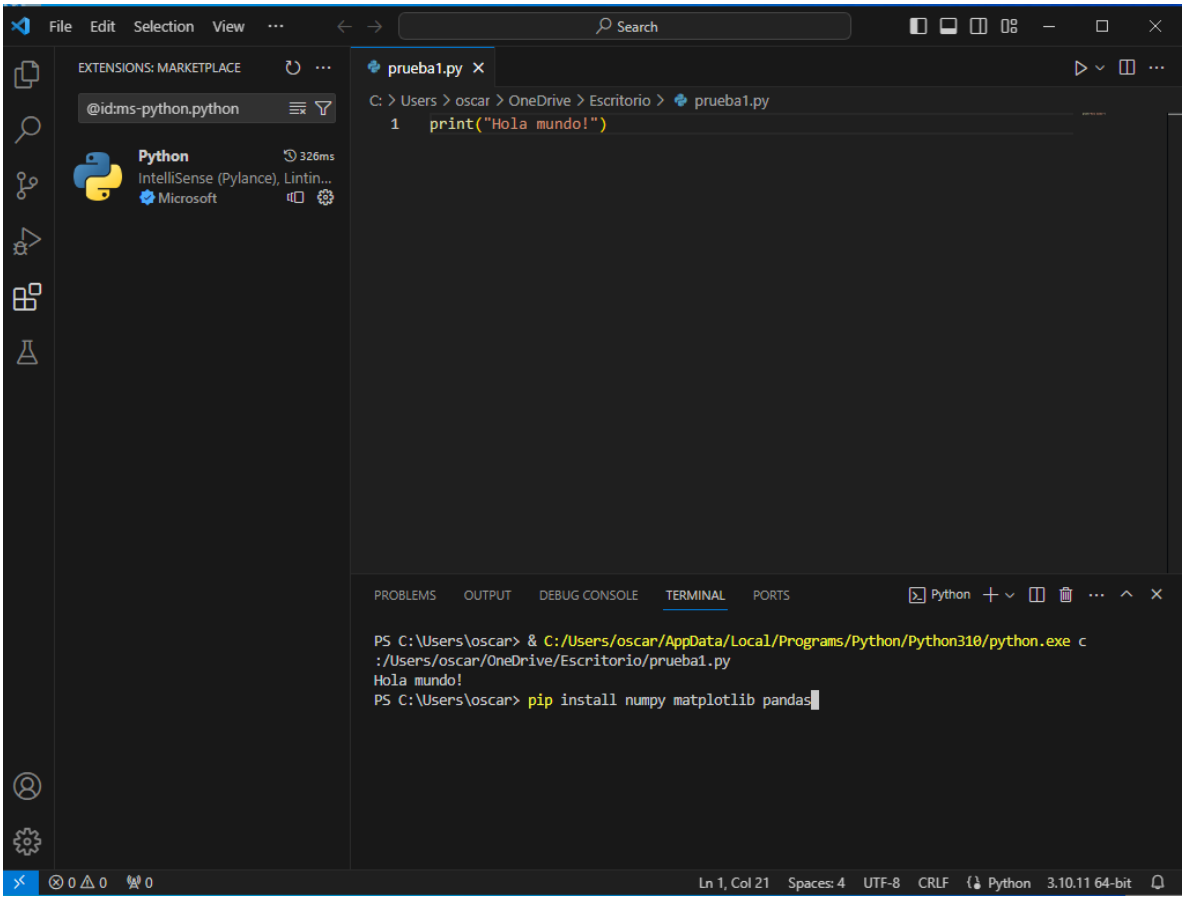

Figura 15 instalación de librerías

El gestor de paquetes pip es una herramienta esencial en el ecosistema de Python, diseñada para facilitar la instalación, actualización y gestión de paquetes y bibliotecas. Utilizado desde la línea de comandos, pip simplifica el proceso de manejar dependencias en proyectos Python. Puedes instalar un paquete específico con el simple comando pip install nombre_del_paquete, lo que descargará e instalará automáticamente la última versión disponible. Además, pip permite gestionar versiones específicas de los paquetes y puede trabajar en conjunto con archivos de requisitos para reproducir exactamente el entorno de desarrollo.

Para finalizar, se validará que las librerías funcionen importándolas al proyecto. Para importarlas basta con escribir antes de la línea escrita las siguientes instrucciones

import pandas

import numpy

luego de escritas, hacer clic en el botón triangular (botón RUN o ejecutar programa) y en la consola se debe seguir viendo el mismo mensaje de hola mundo como en la figura 16. En caso de alguna falla, ejecutar el comando de actualizar pip en la consola:

python.exe -m pip install –upgrade pip

posteriormente instalar de nuevo las librerías y ejecutar el comando RUN

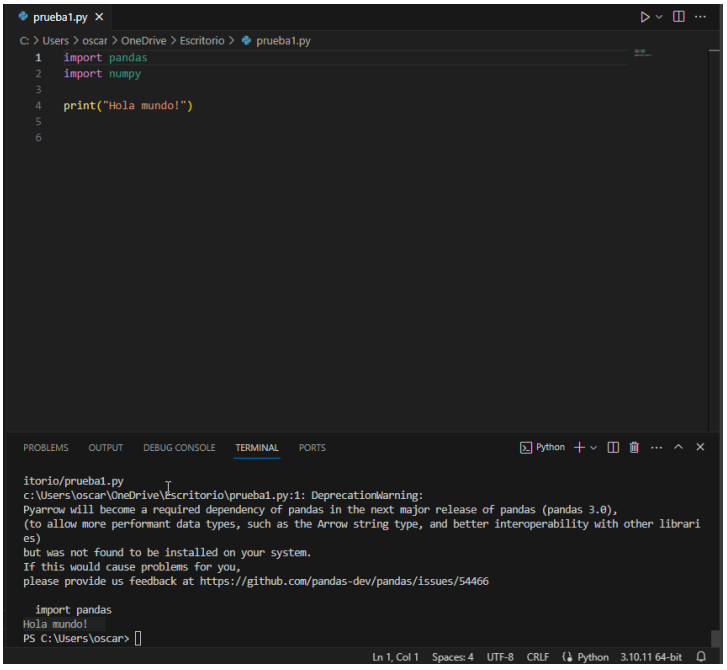

Figura 16: librerías instaladas y funcionando

La criptografía es la forma en la que se puede ocultar el significado de un mensaje a todos los posibles lectores, con excepción del destinatario. Para que el mensaje se pueda ocultar, se necesita que sea transformado de su forma original a una variación. A este proceso se le llama cifrado.

Al proceso inverso que consiste en tomar la información alterada y recuperar el mensaje original se le conoce como descifrar.

En la ciberseguridad, se requiere constantemente de aplicar ambos procesos, para esto existen muchos algoritmos que pueden cifrar y descifrar mensajes. Según el algoritmo el proceso puede ser más rápido, pero en ocasiones un poco mas inseguro, o más lento, pero mucho más seguro. Al escoger un algoritmo de cifrado se debe tener en cuenta el tiempo que se tardarán los paquetes en ser procesados y el nivel de seguridad que ofrece el algoritmo ante posibles ataques.

Los métodos de cifrado han ido evolucionando conforme avanzan las capacidades de computación humana y los avances en áreas como la matemática.

Para facilitar los procesos de cifrado y descifrado, debe usarse una clave de cifrado secreto, que es similar al caso visto de la escítala en donde la clave era una vara de madera con un grosor específico.

Existen dos tipos de claves de cifrado: claves simétricas y claves asimétricas