import tkinter as tk

from tkinter import simpledialog, messagebox

from sympy import primerange, is\_primitive\_root

from random import randint

# Function to find a primitive root modulo a prime number

def find\_primitive\_root(prime):

    for i in range(2, prime):

        if is\_primitive\_root(i, prime):

            return i

    return None

# Generate a list of primes from 100 to 255

primes = list(primerange(100, 256))

# Choose a prime from the list and find a primitive root for it

p = primes[randint(0, len(primes) - 1)]

g = find\_primitive\_root(p)

# If no primitive root is found, we'll pick another prime

while g is None:

    p = primes[randint(0, len(primes) - 1)]

    g = find\_primitive\_root(p)

# Function to get private key from user and calculate public key

def calculate\_keys():

    try:

        # Get private key from user

        private\_key = simpledialog.askinteger("Input", "Enter your private key (integer):",

                                              parent=root, minvalue=2, maxvalue=p-2)

        if private\_key is not None:

            # Calculate public key

            public\_key = pow(g, private\_key, p)

            # Show the calculation in the console

            print(f"Chosen prime (p): {p}")

            print(f"Primitive root (g): {g}")

            print(f"Your private key: {private\_key}")

            print(f"Your public key (g^private\_key mod p): {public\_key}")

            # Display the public key to the user

            messagebox.showinfo("Public Key", f"Your public key is: {public\_key}")

    except Exception as e:

        messagebox.showerror("Error", f"An error occurred: {e}")

# Initialize the main application window

root = tk.Tk()

root.title("Diffie-Hellman Key Exchange")

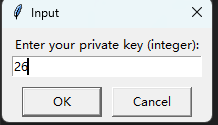
# Button to trigger the calculation

calculate\_button = tk.Button(root, text="Select Private Key", command=calculate\_keys)

calculate\_button.pack(pady=20)

# Start the GUI event loop

root.mainloop()





输出：

Chosen prime (p): 127

Primitive root (g): 3

Your private key: 26

Your public key (g^private\_key mod p): 82

可以调整prime