Secret messages with public and private keys instructions

Introduction:

Welcome to the secret messages workout where you will learn about public and private key encryption. When transmitting messages across the Internet, there's a possibility they may be intercepted by a man-in-the-middle attack. To counteract this, encryption algorithms were created to make reading messages much more difficult for attackers.

What is public key cryptography?

This is also known as asymmetric key cryptography. Public key cryptography uses two keys to encrypt a plain text message. When generating a key pair, a public key is usually given out to the public while the private key is kept by the person who created it. People with the public key are only able to encrypt messages while the owner with the private key can decrypt them. This type of cryptography is really good for ensuring security but may be a little slower than private key cryptography. Examples of algorithms that use this are **RSA(Rivest-Shamir-Adleman)** and **DSA (Digital Signature Algorithm)**.

What is private key cryptography?

This is also known as symmetric key cryptography. Only one key is used to cipher and decipher codes. The great thing about this method is that it's quite fast while still maintaining a good degree of security. Perhaps the big disadvantage with this method is that all parties must exchange the key for decrypting and encrypting messages. This makes the likelihood of the key falling into the wrong hands a much bigger problem. Some of the algorithms that utilize this include **AES (Advanced Encryption Standard)**, **DES(Data Encryption Standard)**, and **RC4 (Rivest Cipher 4)**. Out of the three mentioned algorithms, AES is considered to be the most secure and is approved and used by government organizations like the NSA for top secret information.

Logging onto your computer:

- Use the generated username and password to login through Guacamole

Your mission:

- Once logged in, you should see a program called Kleopatra.
- Using this program, generate a new key pair.
- Once you’ve done that, create a message in a text editor like notepad.
- With Kleopatra, encrypt the message with the public key. **Do not encrypt the file itself.**
- After encrypting, decrypt it using your private key.