Actividad 9: Instrucciones OpenSSL

Instrucciones

- Enviar un mail a **dedarritchon@uc.cl (mailto:dedarritchon@uc.cl)** con su llave pública.
- Yo les enviaré una pregunta encriptada con su llave pública.
- Ustedes desencriptan el mensaje usando su llave privada
- Ustedes me envían la respuesta a la pregunta encriptada con mi llave pública
- Yo desencripto la respuesta usando mi llave privada.

Comandos útiles

- **Generate Private Key:**

  `openssl genpkey -algorithm RSA -out private_key.pem -pkeyopt rsa_keygen_bits:2048`

  This generates a 2048-bit private key.

- **Extract Public Key:**

`openssl rsa -pubout -in private_key.pem -out public_key.pem`

- **Encrypt a Message Using the Public Key**

Once you have the recipient's public key, you can encrypt your message.

`echo "Secret message" | openssl rsautl -encrypt -pubin -inkey public_key.pem -out encrypt`

- **Decrypt the Message Using the Private Key**

To decrypt the message, the recipient needs to use their private key.

`openssl rsautl -decrypt -inkey private_key.pem -in encrypted_message.bin`