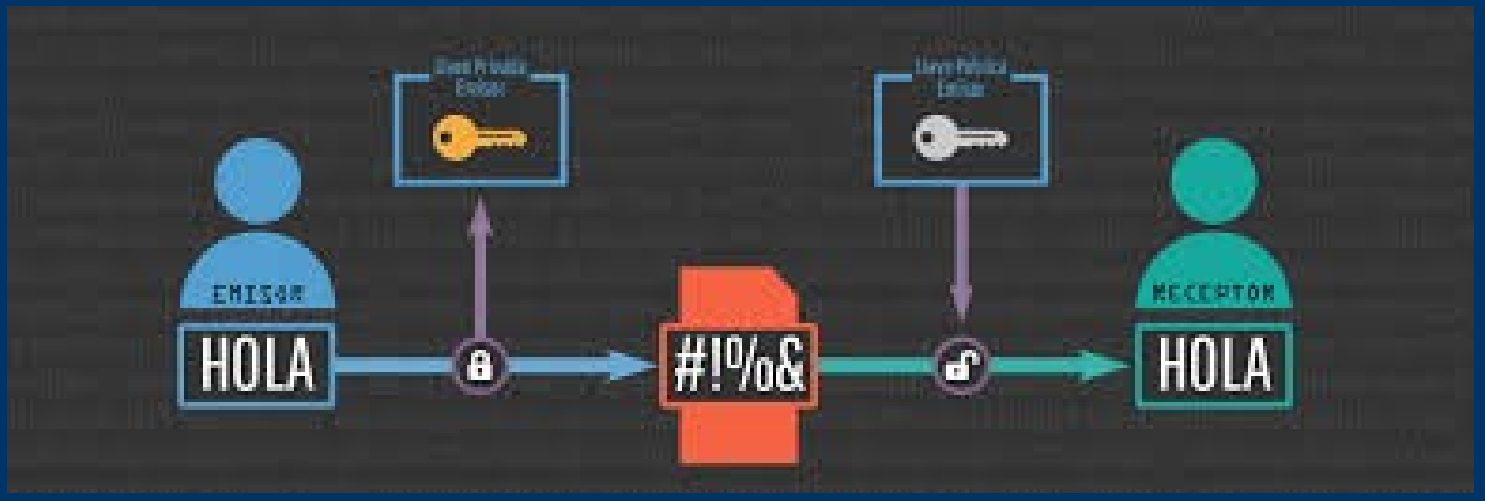
SEGURIDAD INFORMÁTICA
TEMA 1 – SEGURIDAD ACTIVA



ÍNDICE

- Criptografía
- No repudio

Criptografía

La criptografía en general tiene 3 objetivos:

- Integridad

  Demostrar que el mensaje no ha sido modificado, ni accidental ni deliberadamente.

- Confidencialidad

  Hacer que el mensaje sea ilegible para nadie, salvo el destinatario previsto.

- No repudio

  Poder demostrar que el mensaje proviene del remitente declarado.

Criptografía

No repudio

- Necesitamos verificar que el mensaje proviene del remitente declarado.
- Por ejemplo si Raúl nos envía un mensaje, vamos a verificar que el nos lo envía.
- La criptografía asimétrica de clave pública también se ocupa de solucionar el problema de la autenticidad.
- Necesitamos tener su clave pública.

Criptografía

No repudio

- Ejemplo:

  Yo soy Raúl y le quiero mandar un mensaje a Ernesto.

- Creo un mensaje y lo firmo con mi clave privada
- El mensaje encriptado se lo envío a Ernesto encriptado con su clave pública.
- Ernesto recibe el mensaje + la firma.
- El mensaje lo desencripta con su clave privada
- La firma la verifica con mi clave pública.

Criptografía

No repudio

Cifrado asimétrico

- Creamos un mensaje

  echo "La temporada ciclista se acaba pronto" > message.txt

- Ahora firmamos el mensaje con la clave privada de Raúl

  openssl dgst -sha256 -sign raul_private.pem -out message.txt.signed message.txt

- Encriptamos el mensaje con la clave pública de Ernesto

  openssl pkeyutl -encrypt -inkey ernesto_public.pem -pubin -in cosas_importantes.txt -out acosas_importantes.txt.enc

Criptografía

No repudio

Cifrado asimétrico

- Creamos un mensaje

  echo "La temporada ciclista se acaba pronto" > message.txt

- Ernesto recibe el mensaje y desencripta con su clave privada

  openssl pkeyutl -decrypt -inkey ernesto_private.pem -in cosas_importantes.txt.enc -out cosas_importantes.txt

- Ernesto verifica el mensaje con la firma y con la clave pública de Raúl

  openssl dgst -verify raul_public.pem -signature cosas_importantes.txt.signed cosas_importantes.txt

Criptografía

No repudio

Cifrado asimétrico

- Creamos un mensaje

  echo "La temporada ciclista se acaba pronto" > message.txt

- La firma sirve porque cualquiera te puede mandar un mensaje porque tiene tu clave pública