CC5301

COMUNICACION ENCUBIERTA

Andrés Calderón Roberto Rivera

¿QUÉ ES?

• Intercambio de información oculto

• El mensaje se esconde en algún

objeto

• ¿Se está comunicando algo?



REQUERIMIENTOS

APLICACIÓN DE COMUNICACIÓN ENCUBIERTA

COMUNICACIÓN CONFIDENCIAL E ÍNTEGRA

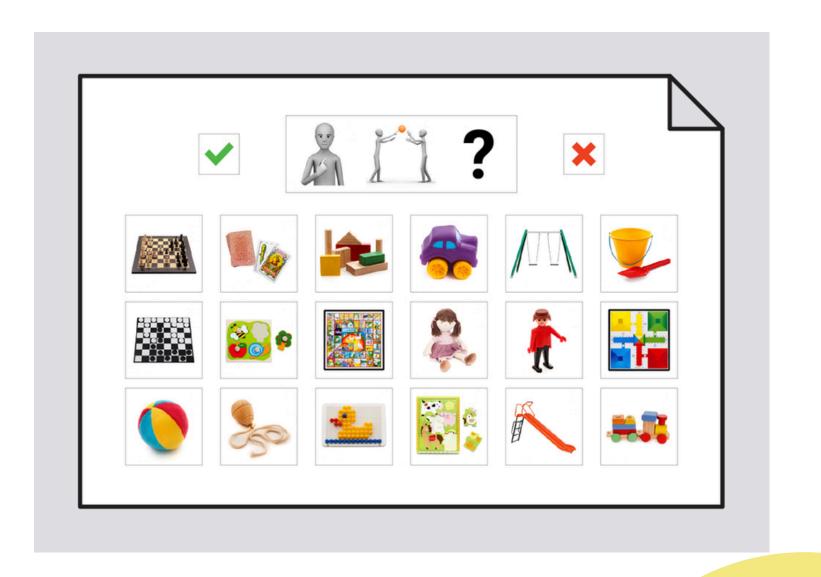
ADVERSARIO NO
SABE SI HAY
MENSAJE SECRETO

¿ESTEGANOGRAFÍA?

SOLUCIÓN







IMPLEMENTACIÓN

Usuario/a se registra

Se generan sus claves pública y privada Se generan sus claves pública y privada

2

Envía una imagen a otro usuario con un mensaje adjunto

3

Usuario/a se registra

2

Se generan sus claves pública y privada 3

Envía una imagen a otro usuario con un mensaje adjunto

4

Se encripta y añade un MAC al mensaje Se generan sus claves pública y privada

Envía una imagen a otro usuario con un mensaje adjunto

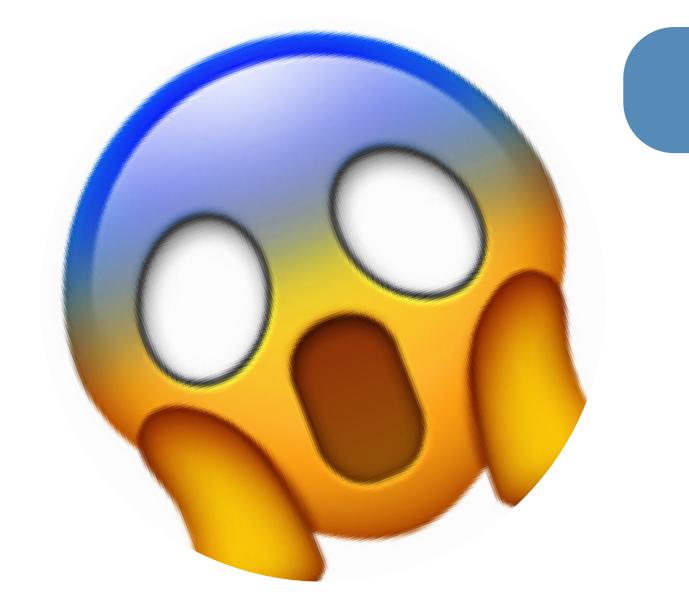
3

5

2

Este mensaje es ocultado en la imagen Se encripta y

añade un MAC al mensaje



ESPEREMOS QUE SALGA BIEN...

DEMO EN VIVO

CONCLUSIÓN

- Se logró solucionar el problema
- Desafíos: diseño del sistema, aplicación funcional
- Todavía hay oportunidades de mejora

iMUCHAS! GRACIAS!

¿PREGUNTAS?