



VÍDEO intypedia003es

LECCIÓN 3: SISTEMAS DE CIFRA CON CLAVE PÚBLICA

EJERCICIOS

AUTOR: Gonzalo Álvarez Marañón

Consejo Superior de Investigaciones Científicas en Madrid, España

EJERCICIO 1

En la criptografía de clave pública:

- a) Todo el mundo puede descifrar mensajes cifrados con la clave pública, pero sólo el poseedor de la clave privada puede descifrar mensajes cifrados usando la clave privada.
- b) Todo el mundo puede descifrar mensajes cifrados con la clave privada, pero sólo el poseedor de la clave privada puede descifrar mensajes cifrados usando la clave pública.
- c) Todo el mundo puede cifrar mensajes usando la clave pública y luego descifrarlos usando la misma clave pública.
- d) Sólo el poseedor de la clave privada puede cifrar mensajes con ella y luego descifrarlos usando la misma clave privada.

EJERCICIO 2

Para firmar un mensaje usando criptografía de clave pública:

- a) Se cifra el mensaje usando la clave pública.
- b) Se cifra el mensaje usando una clave secreta (de criptografía simétrica) cifrada a su vez con la clave pública del destinatario.
- c) Se cifra un resumen del mensaje usando la clave privada.

- d) Se cifra la firma manuscrita escaneada y se añade al mensaje.

EJERCICIO 3

Para acordar de forma segura, eficiente y escalable una clave secreta como las usadas en criptografía simétrica:

- a) Se llama por teléfono, preferiblemente por Skype para mayor seguridad, al destinatario del mensaje y se le revela la clave secreta que se usará para cifrar el mensaje.
- b) Se le envía la clave secreta por correo electrónico, o por chat, o por Twitter, o por Facebook o por cualquier otro medio online de gran velocidad.
- c) Se le envía la clave secreta en una memoria USB utilizando un servicio de Courier.
- d) Se cifra con la clave pública del destinatario.

EJERCICIO 4

En los algoritmos de clave pública:

- a) El conocimiento de la clave pública no permite obtener ninguna información sobre la correspondiente clave privada ni descifrar el texto cifrado con dicha clave pública.
- b) El conocimiento de la clave pública permite deducir la correspondiente clave privada siempre que se conozca el tipo de problema en el que se basa el algoritmo.
- c) El conocimiento de la clave pública permite descifrar el texto con ella cifrado siempre que se conozca el tipo de problema en el que se basa el algoritmo.
- d) El conocimiento de la clave pública equivale a haber roto el algoritmo, por lo que esa clave debería descartarse y crear una nueva.

EJERCICIO 5

El ataque del hombre en el medio consiste en:

- a) Interceptar todos los mensajes enviados entre emisor y receptor, haciéndoles creer que se comunican directamente, cuando en realidad todos los mensajes son leídos y manipulados por el atacante.
- b) Situarse entre el emisor y el receptor y hacerse pasar por un conocido para engañarles con el fin de que revelen confiadamente las claves privadas.
- c) Interceptar las claves públicas intercambiadas entre emisor y receptor.
- d) Robar la clave privada del receptor de los mensajes cifrados con su clave pública para situarse entre emisor y receptor y poder así descifrar todos los mensajes que se le envían cifrados con su clave pública.

RESPUESTAS

1. b
2. c
3. d
4. a
5. a

Madrid, España, diciembre de 2010

<http://www.intypedia.com>

<http://twitter.com/intypedia>

