



## VÍDEO intypedia002es

### LECCIÓN 2: SISTEMAS DE CIFRA CON CLAVE SECRETA

#### EJERCICIOS

**AUTOR:** Fausto Montoya Vitini

Consejo Superior de Investigaciones Científicas en Madrid, España

#### EJERCICIO 1

Se desea utilizar un algoritmo para cifrar una videoconferencia (audio y video). Indique qué tipo de algoritmo de entre los siguientes resultaría inadecuado:

- a) Cifrado en flujo
- b) Cifrado en bloque
- c) Cifrado asimétrico o de clave pública
- d) Todos son inapropiados para cifrar este tipo de contenido

#### EJERCICIO 2

En los buenos algoritmos criptográficos, la seguridad del sistema debe recaer en la seguridad de la clave, debiéndose suponer conocidos el resto de los parámetros del sistema criptográfico. Esta regla de diseño se conoce como:

- a) Segunda Ley de Shannon
- b) Regla de la transparencia
- c) Principio de Kerckoffs

- d) Principio de la seguridad sin oscuridad

### **EJERCICIO 3**

En criptografía, la confusión consiste en:

- a) Enviar al atacante falsos textos para confundirlo
- b) Mezclar las letras entre sí para confundirlas
- c) Eliminar cualquier relación estadística entre el mensaje original y su texto cifrado
- d) Ocultar la relación entre el texto cifrado y la clave secreta

### **EJERCICIO 4**

En los ataques de fuerza bruta:

- a) Se prueban todas las posibles combinaciones de la clave hasta dar con la correcta
- b) Se golpea en la cabeza al emisor del mensaje hasta que revele la clave usada
- c) Se intenta descifrar el mensaje probando un máximo de 10 millones de contraseñas
- d) Se contrata mano de obra barata para que introduzcan claves tan rápidamente como puedan

### **EJERCICIO 5**

En los algoritmos de cifrado en flujo:

- a) Se cifran los mensajes bit a bit en función de los lanzamientos de un dado
- b) Se crean secuencias pseudoaleatorias con las que se mezcla el mensaje y la clave es la semilla utilizada
- c) Se crean secuencias aleatorias que son destruidas una vez que el mensaje se ha mezclado con ellas
- d) Se cifra la información en bloques de tamaño fijo, normalmente de entre 64 y 128 bits

## RESPUESTAS

1. c

2. c

3. d

4. a

5. b

---

Madrid, España, octubre de 2010

<http://www.intypedia.com>

<http://twitter.com/intypedia>

