VÍDEO intypedia008es

LECCIÓN 8: PROTOCOLO DE REPARTO DE SECRETOS

EJERCICIOS

AUTOR: Dr. Luis Hernández Encinas

Consejo Superior de Investigaciones Científicas en Madrid, España

EJERCICIO 1

En todos los protocolos de reparto de secretos:

a) A partir del secreto original se obtiene un número determinado de sombras, todas ellas del mismo tamaño.

b) El secreto que se desea proteger se divide en un número fijo de partes, todas del mismo tamaño que el del secreto.

c) El secreto, que siempre es un número, se escribe en binario y se divide en tantas partes como se haya decidido de antemano.

d) A partir del secreto se obtiene un número fijo de sombras, cada una de las cuales es de un tamaño diferente.

EJERCICIO 2

En un protocolo de reparto de secretos:

a) Hacen falta, siempre, todas las sombras para recuperar el secreto.

b) Con la mitad de las sombras es posible, en todos los casos, recuperar el secreto.

c) El número de sombras necesario para recuperar un secreto depende de los parámetros establecidos en el protocolo.

d) No se puede recuperar el secreto a no ser que se disponga de la clave utilizada para ocultarlo.

EJERCICIO 3

En los esquemas umbrales (*k*, *n*) de reparto de secretos, para recuperar el secreto original:

a) Se requieren tantas sombras como el valor de *n*.

b) Se precisan exactamente *k* sombras.

c) Hacen falta *k*–1 sombras y con menos ya no se puede recuperar.

d) No importa el número de sombras siempre que sea mayor que *n*–*k*.

EJERCICIO 4

En los protocolos umbrales (*k*, *n*) de reparto de secretos en los que se usa el método de interpolación Lagrange:

a) Se usa un polinomio de grado *k*.

b) El secreto se oculta como un coeficiente cualquiera de un polinomio de grado *n*.

c) El término independiente del polinomio coincide con el secreto a ocultar.

d) De usan dos polinomios, uno para ocultar el secreto y otro para recuperarlo.

EJERCICIO 5

Para recuperar el polinomio en los protocolos del Ejercicio 4:

a) Es preciso conocer tantos puntos como sombras se hayan definido en el protocolo.

b) Basta con conocer *k* puntos para obtener el polinomio y así, el secreto.

c) No se puede recuperar el polinomio a no ser que se conozcan exactamente *n*–*k*+1 puntos.

d) Hace falta conocer 3 polinomios auxiliares y no menos.

RESPUESTAS

1. a

2. c

3. b

4. c

5. b

Madrid, España, Junio de 2011

http://www.intypedia.com

http://twitter.com/intypedia