Casos prácticos

Cifrado en bloque AES

Telefónica EDUCACIÓN DIGITAL

Casos prácticos

Software: AESPhere: http://www.criptored.upm.es/software/sw_m001p.htm

1 | Cifrado con clave de 128 y 256 bits modo CBC

Se cifra el texto que se indica con la siguiente clave de 128 bits usando el vector inicial IV.

Mensaje: El algoritmo AES es el actual estándar mundial de cifra simétrica.

Clave 128 bits: 0123456789ABCDEFFEDCBA9876543210

IV: AAAA0000FFFF3333BBBB5555DDDD8888

Pregunta 2.1.1. Muestra los dos criptogramas en hexadecimal que has obtenido.

Pregunta 2.1.2. Justifica el relleno que verás en el texto en claro al cifrar.

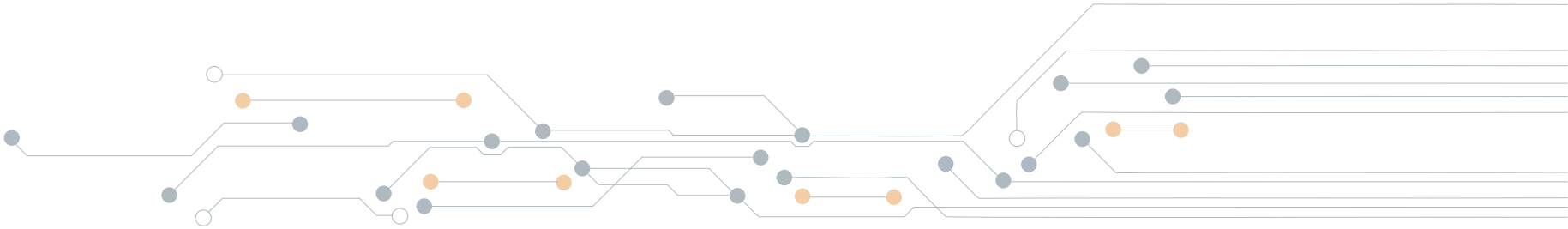
2 | Descifrado AES modo ECB

Recibes el siguiente criptograma en formato base 64, además de la clave de 128 bits que se indica.

C = ohju+ZJvzeMI53whWdOFvighAeEeHD1ok1AkFiQsz+KYeYSVPk5yuK0a3Ikf9FqpXXIUUtA9DKE2a9PNWfSUUQ==

K = ACABADAACABADAACABADAACABADAACAB

Pregunta 2.2.1. ¿Cuál era el mensaje?



Telefónica EDUCACIÓN DIGITAL