Caso práctico final

Criptografía

Telefónica EDUCACIÓN DIGITAL

Caso práctico final

En una vuelta del algoritmo criptográfico DES se tiene como entrada a las cajas S el texto hexadecimal FABADAFABADA.

Se pide:

a. Encontrar la salida de las cajas y mostrar toda la cadena de bits resultantes de la operación de las cajas S en esa vuelta en octetos.

b. ¿Cuántas operaciones habría que realizar como máximo para romper la caja S7 en esa vuelta? ¿Cuántas operaciones habría que realizar como máximo para romper las 8 cajas de esa vuelta? ¿Y cuántas operaciones habría que realizar como máximo para romper las cajas S de un bloque de cifra del DES?

Siendo $\varphi(n)$ la función de Euler, con los números p = 5, q = 20 y el producto n = p·q, elige la(s) afirmación(es) correcta(s):

a. Las claves RSA se calcularán en un cuerpo con módulo n
b. $\varphi(n) = (p - 1)\cdot(q - 1) = (5 - 1)(20 - 1) = 4 \cdot 19 = 76$
c. El algoritmo RSA se basa en la dificultad de factorizar números primos.

¿Cuál de las siguientes opciones es más eficiente? Justifica tu respuesta.

a.

$C = M^e \bmod n$

$C^1 = C^d \bmod n$

b.

$C = M^d \bmod n$

$C^1 = C^e \bmod n$

Explica, con tus propias palabras, qué es, qué características tiene y qué aplicaciones prácticas puede tener una función hash. Además, menciona las funciones hash que conozcas.

Telefónica

EDUCACIÓN DIGITAL