Casos prácticos

RSA

Telefónica EDUCACIÓN DIGITAL

Casos prácticos

genRSA: http://www.criptored.upm.es/software/sw_m001d.htm

Fortaleza de cifrados: http://www.criptored.upm.es/software/sw_m001e.htm

LegionRSA: http://www.criptored.upm.es/software/sw_m001o.htm

1 | Generación de claves RSA (0,3 puntos)

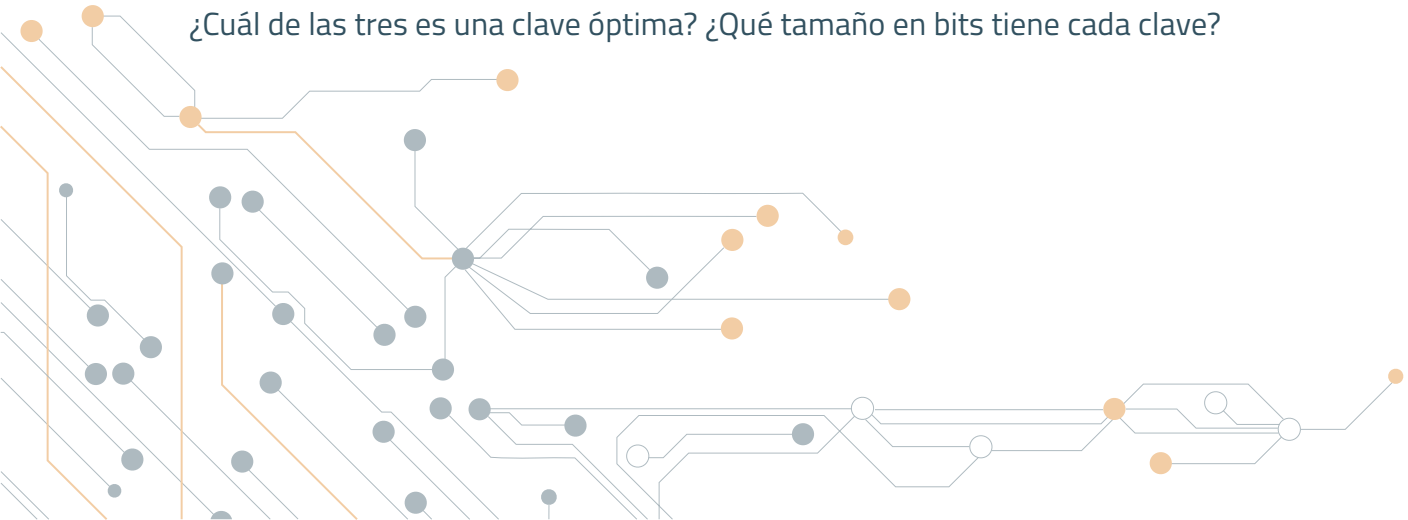
Genera estas tres claves RSA y apunta el número de CPP y NNC.

Clave 1 (decimal): p = 191, q = 211, e = 41.

Clave 2 (hexadecimal): p = C41B0847, q = E25582BF, e = 38B1.

Clave 3 (hexadecimal): p = FCAD34577963E341, q = BF0C9F869FD5E149, e = 0F4D

¿Cuál de las tres es una clave óptima? ¿Qué tamaño en bits tiene cada clave?



2 | Cifrado y descifrado RSA (0,4 puntos)

Con la clave óptima del ejercicio anterior, cifra el valor secreto N = D75A (como la clave se ha creado en formato hexadecimal, la entrada será también en hexadecimal). Convirtiendo valores a decimales con la calculadora de Windows, comprueba con el software Fortaleza de Cifrados que la cifra es correcta.

3 | Ataque por paradoja del cumpleaños a RSA (0,3 puntos)

Se conoce el módulo RSA de una clave de 60 bits es 975.489.807.177.105.347, con e = 65.537. Realiza un ataque por paradoja del cumpleaños y encuentra la clave privada d = 785.786.010.365.481.473. ¿Cuánto tarda el ataque? Comprueba con Fortaleza de Cifrados que es la clave correcta cifrando el número 1.234 con la clave pública y luego descifrando el criptograma con la clave privada.

Telefónica EDUCACIÓN DIGITAL