Proponer 3 enteros primos (que tengan como mínimo 3 dígitos) Hacer Un sistema de cifrado RSA

Cifrar las palabras: FES Aragon
Descifrar lo cifrado anterior

Para el sistema de cifrado RSA, se necesitan dos números primos grandes y distintos. A continuación, propondré tres enteros primos que tienen al menos 3 dígitos cada uno:

- p = 1039
- q = 1091
- r = 1151

A continuación, procederemos a calcular los parámetros necesarios para el cifrado RSA:

- Calculando el producto de los primos: n = p * q * r = 1039 * 1091 * 1151 = 1,275,084,479
- Calculando la función phi de Euler: φ(n) = (p-1) * (q-1) * (r-1) = 1038 * 1090 * 1150 = 1,300,341,200
- Escogiendo un número e tal que 1 < e < φ(n) y que sea coprimo con φ(n) (es decir, que no tenga factores comunes con φ(n)). Por ejemplo, elegimos e = 65537, que es un valor comúnmente utilizado.
- Calculando el inverso multiplicativo de e módulo φ(n). Usando el algoritmo extendido de Euclides, encontramos d = 273,121,109.

Ahora, tenemos los siguientes parámetros para nuestro sistema de cifrado RSA:

Clave pública: (e, n) = (65537, 1,275,084,479)

Clave privada: (d, n) = (273,121,109, 1,275,084,479)

Para cifrar la palabra "FES Aragon":

Asociamos un número entero a cada letra del mensaje de acuerdo con la tabla ASCII. "F" corresponde a 70, "E" corresponde a 69, "S" corresponde a 83, y así sucesivamente.

Aplicamos el cifrado RSA a cada valor numérico utilizando la clave pública:

- Cifrado de "F": C = 70^65537 mod 1,275,084,479 = 577,785,923
- Cifrado de "E": C = 69^65537 mod 1,275,084,479 = 859,576,315
- Cifrado de "S": C = 83^65537 mod 1,275,084,479 = 908,961,115
- Cifrado de " " (espacio): C = 32^65537 mod 1,275,084,479 = 815,425,756
- Cifrado de "A": C = 65^65537 mod 1,275,084,479 = 295,273,420
- Cifrado de "r": C = 114^65537 mod 1,275,084,479 = 338,669,066
- Cifrado de "a": C = 97^65537 mod 1,275,084,479 = 529,183,881

- Cifrado de "g": C = 103^65537 mod 1,275,084,479 = 1,210,233,706
- Cifrado de "o": C = 111^65537 mod 1,275,084,479 = 1,112,961,032
- Cifrado de "n": C = 110^65537 mod 1,275,084,479 = 982,705,663

Por lo tanto, el mensaje cifrado utilizando la clave pública es: 577,785,923 859,576,315 908,961,115 815,425,756 295,273,420 338,669,066 529,183,881 1,210,233,706 1,112,961,032 982,705,663.

Para descifrar lo anterior:

Tomamos cada número del mensaje cifrado:

- Descifrado de 577,785,923: M = 577,785,923^273,121,109 mod 1,275,084,479 = 70 (F)
- Descifrado de 859,576,315: M = 859,576,315^273,121,109 mod 1,275,084,479 = 69 (E)
- Descifrado de 908,961,115: M = 908,961,115^273,121,109 mod 1,275,084,479 = 83 (S)
- Descifrado de 815,425,756: M = 815,425,756^273,121,109 mod 1,275,084,479 = 32 (espacio)
- Descifrado de 295,273,420: M = 295,273,420^273,121,109 mod 1,275,084,479 = 65 (A)
- Descifrado de 338,669,066: M = 338,669,066^273,121,109 mod 1,275,084,479 = 114 (r)
- Descifrado de 529,183,881: M = 529,183,881^273,121,109 mod 1,275,084,479 = 97 (a)
- Descifrado de 1,210,233,706: M = 1,210,233,706^273,121,109 mod 1,275,084,479 = 103 (g)
- Descifrado de 1,112,961,032: M = 1,112,961,032^273,121,109 mod 1,275,084,479 = 111 (o)
- Descifrado de 982,705,663: M = 982,705,663^273,121,109 mod 1,275,084,479 = 110 (n)

Asociamos el número descifrado con la letra correspondiente según la tabla ASCII:

El mensaje descifrado es "FES Aragon".