CRYPT4YOU

DOCUMENTO ANEXO A LA LECCIÓN 6

DEL CURSO "EL ALGORITMO RSA"

EJERCICIOS Y PRÁCTICAS PROPUESTOS Y RESUELTOS

Autor: Dr. Jorge Ramió Aguirre
Fecha de publicación: 13 de junio de 2012
http://www.criptored.upm.es/crypt4you/temas/RSA/leccion6/leccion06.html

TABLA DE CONTENIDOS

LECCIÓN 6. RSA Y EL TEOREMA CHINO DEL RESTO

Apartado 6.2. Definición del teorema chino del resto y su uso en RSA

ejercicioRSA6.2.1

Ejercicio 1

Conociendo que el teorema chino del resto se expresa como:

Si $x \equiv x_1 \bmod p$

$x \equiv x_2 \bmod q$

Entonces $x = [x_1 * q * (q^{-1} \bmod q) + x_2 * p * (p^{-1} \bmod p)] \bmod n$

Para el módulo n = 7.171 compuesto por el producto de los primos p = 71 y q = 101, usa la ecuación del teorema chino del resto y encuentra el valor de x que cumple con las siguientes congruencias:

$x \equiv 32 \bmod 71$

$x \equiv 84 \bmod 101$

Solución:

x_1 = **32**; x_2 = **84**; p = **71**; q = **101**; n = 7.171

$q^{-1} \bmod q$ = inv (q, p) mod q = inv (101, 71) mod 101 = inv (30, 71) mod 101 = 45 mod 101 = **45**

Nota: inv (101, 71) mod 101 = inv (30, 71) mod 101 porque 101 mod 71 = 30

$p^{-1} \bmod p$ = inv (p, q) mod p = inv (71, 101) mod 71 = 37 mod 71 = **37**

Luego:

x = [32 * 101 * 45 + 84 *71 * 37] mod 7.171

x = [145.440 + 220.668] mod 7.171 = 366.108 mod 7.171 = **387**

Efectivamente, se comprueba fácilmente que:

$387 \equiv 32 \bmod 71$ Es decir, 387 mod 71 = 32

$387 \equiv 84 \bmod 101$ Es decir, 387 mod 101 = 84

Ejercicio 2

Resuelve ahora el valor de x para estos dos casos

a) $x \equiv 12 \bmod 19$ $x \equiv 25 \bmod 31$

b) $x \equiv 40 \bmod 2001$ $x \equiv 100 \bmod 2011$

ejercicioRSA6.2.2

Aplicando la propiedad $r \equiv t \bmod \phi(p) \Rightarrow a^r \equiv a^t \bmod p$, calcula $2^{3.104} \bmod 101$ y saca conclusiones de lo observado.

Solución

Comprobado que 101 es número primo y que mcd (2, 101) = 1, aplicando la propiedad indicada tenemos:

$\phi(101) = 100$
$3.104 \equiv 4 \bmod 100$

Luego:

$2^{3.104} \equiv 2^4 \equiv 16 \bmod 101$

Por tanto, la propiedad anterior nos permite reducir significativamente el número de potencias a calcular.

ejercicioRSA6.2.3

Para obtener x mod n, con n = p * q, a partir de $x_1 \equiv x \bmod p$ y $x_2 \equiv x \bmod q$, se hace:

$x = x_1 + h * p$, donde $h = [(x_2 - x_1)(p^{-1} \bmod q)] \bmod q$ (fórmula de Garner)

Demuestra que la fórmula de Garner es correcta.

Demostración

Basta comprobar que cuando hacemos x mod p y x mod q, para $x = x_1 + h * p$, obtenemos x_1 y x_2 respectivamente.

Primera ecuación:

$x \bmod p = (x_1 + h * p) \bmod p = x_1 \bmod p + h * p \bmod p$

$= x_1 \bmod p$ (pues $h * p \bmod p = 0$)

Luego $x_1 \bmod p = x_1$

Segunda ecuación:

$x \bmod q = (x_1 + h * p) \bmod q$

$= x_1 \bmod q + h * p \bmod q$

$= x_1 \bmod q + p\ [(x_2 - x_1)(p^{-1} \bmod q)] \bmod q$

$= x_1 \bmod q + \{(p \bmod q)\ [(x_2 - x_1) \bmod q]\ (p^{-1} \bmod q)]\} \bmod q$

$= x_1 \bmod q + [(x_2 - x_1) \bmod q] \bmod q$ (porque $(p \bmod q)\ (p^{-1} \bmod q) = 1$)

$= x_1 \bmod q + x_2 \bmod q - x_1 \bmod q$

$= x_2 \bmod q = x_2$

LECCIÓN 6. RSA Y EL TEOREMA CHINO DEL RESTO

Apartado 6.3. Aplicación del TRC en el descifrado RSA

prácticaRSA6.3.1

Para las siguientes claves, descifra el criptograma C utilizando el teorema chino del resto.
SW genRSA: http://www.criptored.upm.es/software/sw_m001d.htm
SW Fortaleza de Cifrados: http://www.criptored.upm.es/software/sw_m001e.htm
SW dec4hex: http://www.criptored.upm.es/software/sw_m051b.htm

Clave RSA1: p = 223, q = 251, e = 131, C = 44.683
Clave RSA2: p = 23.357, q = 29.759, e = 4321, C = 487.735.883
Clave RSA3: p = 18EE7F9, q = 1DB117F, e = 5FB9, C = 2E1EEB6C98D7B (M en decimal)