Estructuras Discretas II

Docente: Carlo Corrales Delgado

Actividad

Ejercicios de RSA, Firma digital, Elgamal

Escuela:

Ciencia de la computación (Primer año)

Alumno:

Josue Gabriel Sumare Uscca

RSA, El gamal, Firma Digital

1)

a) $N = 5 \cdot 7 = 35$

$\varphi(35) = \varphi(5) \cdot \varphi(7) = 4 \cdot 6 = 24$

$d \cdot e \bmod \varphi(35) = 1 \Rightarrow 11 \cdot e \bmod 24 = 1$

$\Rightarrow e = 11$

$C = 2^{11} \bmod 35$; $C = 18$ cifrado de $M = 2$

$M = 18^{11} \bmod 35$; $M = 2$ descifrado C

b) $N = 3 \cdot 11 = 33$

$\varphi(33) = \varphi(3) \cdot \varphi(11) = 2 \cdot 10 = 20$

$d \cdot e \bmod \varphi(33) = 1 \Rightarrow 7 \cdot d \bmod 20 = 1 \Rightarrow$

$d = 3$

$C = 5^{7} \bmod 33$; $C = 14$ cifrado de $M = 5$

$M = 14^{3} \bmod 33$; $M = 5$ descifrado de C

c) $N = 5 \cdot 11 = 55$

$\varphi(55) = \varphi(5) \cdot \varphi(11) = 4 \cdot 10 = 40$

$d \cdot e \bmod \varphi(55) = 1 \Rightarrow 7 \cdot d \bmod 40 = 1 \Rightarrow$

$d = 23$

$C = 10^{7} \bmod 55 \Rightarrow C = 10$ cifrado de 10

$M = 35^{23} \bmod 55 \Rightarrow M = 30$ cifrado de 35

d) $N = 7 \cdot 13 = 91$

$\varphi(91) = \varphi(7) \cdot \varphi(13) = 6 \cdot 12 = 72$

$d \cdot e \bmod \varphi(91) = 1 \Rightarrow 11 \cdot e \bmod 72 = 1 \Rightarrow e = 59$

$C = 3^{59} \bmod 91$; $C = 61$ cifrado de 31

$M = 41^{11} \bmod 91$; $M = 20$ descifrado de 41

2) ⓐ 1) La fortaleza está en la factorización de números grandes.

2) La longitud de las claves son de 1024 y 2048 bits

3) Los números primos p y q, secretos, constituyen la complejidad del método, Conocidos p y q es fácil calcular d a partir de e, mientras que la complejidad de Factorizar N es el orden de e(ln(N)) ln ln (N)) 1/2.

ⓑ Clave Pública de Laura = e

$d = 7 \quad ; \quad e.d \equiv 1 \bmod \phi(N)$

$\phi(55) = \phi(5.11) = 4.10 = 40$

$7.e = 1 \bmod 40 \Rightarrow mcd(7, 40) = 1$

Teorema de Euler

$a^{-1} = a^{\phi(n)-1} \bmod n \Rightarrow \phi(n) = \phi(40) =$

$\phi(23) \cdot \phi(5) = (23-22).4 = 16$

$e = d^{-1} = d^{\phi(40)-1} = 7^{15} \bmod 40 = (7^2)^7.$

$7 \bmod 40 = 9^7 . 7 = (9^2)^3 . 9.7 = 81^3.$

$63 \bmod 40 = 63 \bmod 40 = 23 \Rightarrow e = 3$

$M = 10 \Rightarrow C = M^e (\bmod N) = 10^{23} \bmod 55$

Cifrar

$10^2 (\bmod 55) = -10 \Rightarrow 10^3 (\bmod 55) = -10 \cdot 10$
$= -100 \bmod 55 = 10 ,$

$\Rightarrow 10^{23} = (10^3)^7 . 10^2 (\bmod 55) = 10^7 . 10^2 = 10^9 \bmod 55$

$= (10^3)^3 \bmod 55 = 10$

Rpta: Al observar que el cifrado y descifrado son lo mismo no es una buena elección.

(3) • Primero debemos calcular la clave privada de Alicia:

$\phi(NA) = 2 \cdot 10 = 20 \quad eA \cdot dA \equiv 1 \bmod \phi(NA))$

$dA \cdot 7 = 1 \bmod 20$

$dA = 3$

• Alicia va descifrando letra a letra el mensaje.

$26^3 \pmod{33} = 20 = T$

$2^3 \pmod{33} = 8 = I$

$15^3 \pmod{33} = 9 = J$

• Calculando la clave privada de Benito

$\phi(NB) = 2 \cdot 12 = 24$

$eB \cdot dB = 1 \pmod{\phi(NB)})$

$dB \cdot 5 = 1 \bmod 24$

$dB = 5$

• Benito con su clave privada descifra letra a letra el mensaje de Alicia

$22^5 \pmod{39} = 16 \to P$

$8^5 \pmod{39} = 8 \to I$

$10^5 \pmod{39} = 4 \to E$