Criptografie-Tema10

guzurazvan

May 2024

1. Pentru a semna mesajul m = 343 folosind o schemă de semnătură digitală DSA, Alice alege p = 48731, q = 443 și x = 7. Cheia secretă a lui Alice este a = 242. (a) Determinați cheia publică a lui Alice. (b) Pentru semnătura digitală, Alice alege k = 427, fără a folosi o funcție de trunchiere. Determinați semnătura digitală și verificați autenticitatea acesteia.

a)
$q = 7^{(48731-1)/443}(mod 48731) = 7^{110}(mod 48731) = 5260(mod 48731)$
$\alpha = 5260^{242}(mod 48731) = 3438$

2. Pentru o semnătură RSA, Alice folosește cheia publică
Ke = (n = 28829, e), cu e cel mai mic posibil exponent. Determinați semnătura folosită de Alice pentru a semna mesajul public m = 11111.

m = 11111 Ke = (n = 28829, e)
$S = m^e(mod n) = 11111^e(mod 28829)$
$n = 28829$
$\left[\sqrt{(28829)}\right] = 169$
$t = 170 \Rightarrow 170^2 - n = 28900 - 28829 = 71$
$t = 171 \Rightarrow 171^2 - n = 29241 - 28829 = 412$
$t = 172 \Rightarrow 172^2 - n = 29584 - 28829 = 755$
$t = 173 \Rightarrow 173^2 - n = 29929 - 28829 = 1100$
...
$t = 177 \Rightarrow 177^2 - n = 31329 - 28829 = 2500 = 50^2$
$\Rightarrow S^2 = 50^2$
$\Rightarrow S = 50$
$n = (177 - 50)(177 + 50) = 227 \cdot 127$
$\phi(n) = 226 \cdot 126$

3. Alice alege două numere prime p = 1223 și q = 1987 și face publică cheia Ke = (n = p · q = 2430101, e = 948047).

Determinați semnătura pe care trebuie să o atașeze Alice mesajului public m = 1070777.

p = 1223, q = 1987, Ke = (n = p · q = 2430101, e = 948047).
m = 1070777

$S = m^e(modn)$
$de = 1(mod\phi(n))$
$\phi(n) = (p-1)(q-1) = 1222 \cdot 1986 = 2426892$
$d = e^{-1}(mod\phi(n)) = 948047^{-1}(mod2426892)$
$2426892 = 2 \cdot 948047 + 530798$
$\Rightarrow x_{530798} = x_{2426892} - 2 \cdot x_{948047} = (1,0) - 2 \cdot (0,1) = (1,-2)$
$948047 = 1 \cdot 530798 + 453249 \Rightarrow x_{453249} = (0,1) - (1,-2) = (1,3)$
$530798 = 1 \cdot 453249 + 77549 \Rightarrow x_{77549} = (1,-2) - (1,3) = (0,-5)$
$453249 = 5 \cdot 77549 + 65354 \Rightarrow x_{65354} = (1,3) - 5 \cdot (0,-5) = (1,28)$
$77549 = 1 \cdot 65354 + 12195 \Rightarrow x_{12195} = (0,-5) - (1,28) = (-1,32)$
$65354 = 5 \cdot 12195 + 4379 \Rightarrow x_{4379} = (1,28) - 5 \cdot (-1,-32) = (6,188)$
$12195 = 2 \cdot 4379 + 3437 \Rightarrow x_{3437} = (-1,-32) - 2 \cdot (6,188) = (-13,-408)$
$4379 = 1 \cdot 3437 + 942 \Rightarrow x_{942} = (6,188) - (-13,-408) = (19,596)$
$3437 = 3 \cdot 942 + 611 \Rightarrow x_{611} = (-13,-408) - 3 \cdot (19,596) = (-70,-2196)$
$942 = 1 \cdot 611 + 331 \Rightarrow x_{331} = (19,596) - (-70,-2196) = (89,2792)$
$611 = 1 \cdot 311 + 280 \Rightarrow x_{280} = (-70,-2196) - (89,2792) = (-259,-4988)$
$331 = 1 \cdot 280 + 51 \Rightarrow x_{51} = (89,2792) - (-259,-4988) = (348,7780)$
$280 = 5 \cdot 51 + 25 \Rightarrow x_{25} = (-259,-4988) - 5 \cdot (348,7780) = (-1999,-43888)$
$51 = 2 \cdot 25 + 1 \Rightarrow x_1 = (348,7780) - 2 \cdot (-1999,-43888) = (4346,95556)$
$\Rightarrow d = 95556$
$S = m^d(modn) = 1070777^{95556}(mod2430101) = 66406(mod2430101)$