Temă

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.

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.

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.

4. Alice alege numărul prim p = 21739, generatorul g = 7 și cheia secretă a = 15140.

(2) $m = 11111$ RSA

$Ke = (n = 28829, e)$

$S = m^e \pmod n = 11111^e \pmod{28829}$

$n = 28829$

$\sqrt{28829} \mid 169$

1

188

156

3229

2961

268

$26 \cdot 6 = 156$

$329 \cdot 9 = 2961$

$t = 170 \Rightarrow 170^2 - n = 28900 - 28829 = 71$

$t = 171 \Rightarrow 29241 - 28829 = 412$

$t = 172 \Rightarrow 773$

$t = 173 \Rightarrow 1100 = 11 \cdot 10^2 \overset{S^2}{\Rightarrow} 10\sqrt{11} = S$

$n = (173 - 10\sqrt{11})(173 + 10\sqrt{11})$

(3) $p=1223$, $q=1987$, $K_e=(n=pq=2430101, e=948047)$

$m=1070777$ (public) $\Rightarrow$ semnătura?

$S = m^d \pmod n$

$de \equiv 1 \pmod{\varphi(n)}$

$\varphi(n)=(p-1)(q-1) = 1222 \cdot 1986 = 2426.892$

$d = e^{-1} \pmod{\varphi(n)} = 948047^{-1} \pmod{2.426.892}$

$2.426.892 = 2 \cdot 948.047 + 530.798 \Rightarrow X_{530798} = X_{2426892} - 2 \cdot X_{948047} =$

$= (1,0) - 2(0,1) = (1,-2)$

$948047 = 1 \cdot 530798 + 453249 \Rightarrow X_{453249} = (0,1) - (1,-2) = (1,3)$

$530798 = 1 \cdot 453249 + 77549 \Rightarrow X_{77549} = (1,-2) - (1,3) = (0,-5)$

$453249 = 5 \cdot 77549 + 65354 \Rightarrow X_{65354} = (1,3) - 5 \cdot (0,-5) = (1,28)$

$77.549 = 1 \cdot 65.354 + 12195 \Rightarrow X_{12195} = (0,-5) - (1,28) = (-1,-32)$

$65354 = 5 \cdot 12195 + 4379 \Rightarrow X_{4379} = (1,28) - 5(-1,-32) = (6,188)$

$12195 = 2 \cdot 4379 + 3437 \Rightarrow X_{3437} = (-1,-32) - 2(6,188) = (-13,-408)$

$4379 = 1 \cdot 3437 + 942 \Rightarrow X_{942} = (6,188) - (-13,-408) = (19,596)$

$3437 = 3 \cdot 942 + 611 \Rightarrow X_{611} = (-13,-408) - 3(19,596) = (-70,-2196)$

$942 = 1 \cdot 611 + 331 \Rightarrow X_{331} = (19,596) - (-70,-2196) = (89,2792)$

$611 = 1 \cdot 331 + 280 \Rightarrow X_{280} = (-70,-2196) - 189,2792) = (-259,-4988)$

$331 = 1 \cdot 280 + 51 \Rightarrow X_{51} = (89,2792) - (-259,-4988) = (348,7780)$

$280 = 5 \cdot 51 + 25 \Rightarrow X_{25} = (-259,-4988) - 5 \cdot (348,7780) = (-1999,-43888)$

$51 = 2 \cdot 25 + 1 \Rightarrow X_1 = X_{51} - 2 \cdot X_{25} = (348,7780) - 2 \cdot (-1999,-43888) =$

$= (4346, 95556)$

$\Rightarrow d$

$S = m^d \pmod n = 1070777^{95556} \pmod{2430101} =$

$= 66406$