Criptografie și securitate CTI

Laborator 10

Semnături digitale

1. În semnătura Textbook RSA:
   (a) Semnați mesajul $x = 14$ cu ajutorul cheii $n = 77$, $d = 13$.
   (b) Peggy publică datele $n = 221$ şi $e = 13$. Victor primeşte mesajul $m = 65$ şi semnătura $s = 182$. Este semnătura respectivă validă?
2. Folosind schema de semnătură digitală ElGamal
   (a) Să se semneze mesajul $x = 101$ cu ajutorul parametrilor următori: $p = 467, \alpha = 2$, cheia privată $a = 127$, alegând valoarea $k = 213$.
   (b) Mesajul $x = 57$ a fost semnat cu ajutorul algoritmului ElGamal specificat de parametrii următori: $p = 97, \alpha = 3, \beta = 70$, obținându-se semnătura $(\gamma, \delta) = (66, 39)$. Este aceasta o semnătură validă?
3. (a) Având acces la o mulțime de semnături digitale valide, semnate cu RSA, creați un mesaj (diferit de cele la care aveți acces deja) care are semnătura validă.
   (b) Indicați o vulnerabilitate a schemei de semnătură digitală ElGamal care poate duce la recuperarea cheii de semnare.
4. Să se semneze mesajul $x = 100$ cu ajutorul algoritmului DSA specificat de parametrii următori: $p = 7879, q = 101, \alpha = 170$, valoarea aleatoare utilizată $k = 50$, cheia secretă fiind $a = 75$.
5. Mesajul $x = 99$ a fost semnat cu ajutorul algoritmului DSA specificat de parametrii următori: $p = 7879, q = 101, \alpha = 170, \beta = 4567$, valoarea aleatoare utilizată $k = 50$ și s-a obținut semnătura $(\gamma, \delta) = (94, 78)$. Este această semnătură validă?