Semnaturi digitale. Aplicatii.

**Capitolul 1**

**Algoritmul RSA**

Exercitiul

**Capitolul 2**

**Semnatura ElGamal**

Exercitiul 2.3.2 Sa se semneze mesajul x = 102 cu ajutorul algoritmului ElGamal speciﬁcat de parametrii urmatori: p = 467, α = 2, cheia privata a = 127, alegand valoarea k = 213.

Rezolvare: Se calculează: β = αa mod p => β = (2127) mod 467 => β = 132

γ = αk mod p = 2213 mod 467 = 29

δ = (H(x)−aγ)k−1 mod (p−1) => δ = (102−127·29)·431 mod 466 = --1543411 mod 466 => δ = 447

Raspuns: semnatura este (γ,δ) = (29,447)

**Capitolul 3**

**Semnatura DSA**

Exercitiul:

Exercitiul 3.3.1 Sa se semneze mesajul x = 101 cu ajutorul algoritmului DSA speciﬁcat de parametrii urmatori: p = 7879, q = 101, α = 170, valoarea aleatoare utilizata k = 50, cheia secreta ﬁind a = 75. Veriﬁcati rezultatul obtinut.

Rezolvare: Se calculeaza:

γ = (αk mod p) mod q = (17050 mod 7879) mod 101 = 2518 mod 101 = 94

δ = (x + aγ)k−1 mod q = (100 + 75·94)50−1 mod 101 = 7150·50−1 mod 101 = 7150· 99 mod 101 = 42

50−1(mod 101) =−2 mod 101 = 99, ( 101 = 50·2 + 1).

Veriﬁcare:

β = αa mod p = 17075 mod 7879 = 4567

e1 = xδ−1 mod q = 100·40−1 mod 101 = 100·89 mod 101 = 0

e2 = γδ−1 mod q = 94·40−1 mod 101 = 94·89 mod 101 = 84

Se obtine: (αe1βe2 mod p) mod q = (17012 ·456784 mod 7879) mod 101 = 2518 mod 101 = 94 = γ.

Raspuns: Semnatura mesajului este (γ,δ) = (94,40);

Cheia publica este β = 4567.