Fişă de exerciţii 6

1. Alice utilizează criptosistemul Rabin cu modulul $n = 713$ şi primeşte mesajul criptat $c = 289$. Determinaţi cele 4 posibilităţi pentru mesajul în clar corespunzător.

2. Alice utilizează criptosistemul Rabin cu modulul $n = 253$.

   (a) Determinaţi cheia secretă a lui Alice.

   (b) Bob doreşte să trimită mesajul '10010110' lui Alice. Determinaţi mesajul criptat.

   (c) Decriptaţi mesajul $c = 170$ primit de Alice, ştiind că ultimii trei biţi ai mesajelor acceptabile sunt 110.

3. Alice utilizează criptosistemul RSA.

   (a) Pentru a determina cheile lui Alice alegeţi două numere prime de câte 8 biţi, p şi q, astfel încât modulul n să aibă 16 biţi, iar exponentul $e = 5$ să fie valabil.

   (b) Determinaţi cheia de decriptare.

   (c) Criptaţi mesajul 110100110110111.

4. Estimaţi numărul operaţiilor elementare necesare pentru criptarea RSA a unui mesaj de 8 biţi, cu un modul având 20 de biţi şi cu exponentul $e = 2^{16} + 1$?

5. Acelaşi mesaj m este criptat RSA şi trimis către 3 utilizatori care au cheile publice $(391, 3)$, $(55, 3)$, $(87, 3)$. Mesajele criptate obţinute sunt, respectiv, $208, 38, 32$. Determinaţi mesajul în clar M, fără a determina vreo cheie de decriptare.

6. Fie $p = 131$. Determinaţi o cheie secretă valabilă a şi o cheie publică (p, g, α) pentru schema de semnătură digitală El Gamal.

7. Alice vrea să semneze mesajul $m = 111$ cu o schemă de semnătură digitală El Gamal. Fie $p = 2237$ şi generatorul $g = 2$ al lui $\mathbb{Z}_{2237}$. Presupunem cheia secretă a lui Alice $a = 1120$. Calculaţi semnătura digitală cu $k = 2227$. Verificaţi semnătura obţinută.

8. Alice vrea să semneze mesajul $m = 111$ cu o schemă de semnătură digitală DSA. Fie $p = 2237$, $x = 2$ şi q cel mai mare număr prim care divide $p - 1$. Alice utilizează o funcţie de trunchiere cu $h(m) = 11$ şi $k = 5$. Care este semnătura digitală DSA corespunzătoare? Verificaţi această semnătură.