(Toy) RSA

1. Fie $p = 41$ şi $q = 17$ factorii modulului RSA.
   (a) Care dintre $e_1 = 32$, $e_2 = 49$, $e_3 = 5$ este un coeficient de criptare valid?
   (b) Calculaţi coeficientul de decriptare d..

2. Fie RSA cu $p = 31$, $q = 37$ şi $e = 17$ (coeficientul de criptare). Determinaţi coeficientul de decriptare d.

Sisteme asimetrice de criptare

3. Se consideră următorul sistem de criptare: (G, q, g, h) sunt parametrii publici, unde G este un grup ciclic de ordin q, g şi h doi generatori al lui G; $x = log_g h$ este cheia privată; se criptează un bit b în (c_1, c_2), astfel:
   (a) dacă $b = 0$, $y \leftarrow^R \mathbb{Z}_q$, $(c_1, c_2) = (g^y, h^y)$
   (b) dacă $b = 1$, $y, z \leftarrow^R \mathbb{Z}_q$ $y \neq z$, $(c_1, c_2) = (g^y, h^z)$

   Cerinţe:
   (a) Arătaţi că decriptarea este eficientă dacă se cunoaşte x.
   (b) Arătaţi că sistemul este CPA-sigur dacă problema DDH este dificilă.

4. Considerăm următoarea variantă a RSA Padded. Fie $|m| = n \approx |N|/2$ (mesaje de aproximativ jumătate din lungimea modulului în biţi). Se defineşte $\bar{m} = 0^k||r||00000000||m$, unde r este ales uniform aleator pe 10 bytes. Atunci $c = \bar{m}^e \mod N$. Arătaţi că sistemul astfel definit nu este CCA-sigur.

Schimb de chei

5. Alice deţine o pereche de chei (pk_A, sk_A). Bob deţine o pereche de chei (pk_B, sk_B).Cei doi doresc să stabilească o cheie secretă comună k pentru o criptare ulterioară rapidă (ex. folosind AES).
   (a) Cum procedează?
   (b) Cum procedează dacă vor să participe amandoi la alegerea cheii k (nici unul nu are încredere în celalalt că poate genera o cheie sigură)?

6. Considerăm o variantă a schimbului de chei Diffie-Hellman în care înlocuim $\cdot$ (înmulţirea) cu $+$ (adunarea) . Rămâne protocolul astfel definit sigur? Argumentaţi.

Calcule pe curbe eliptice

7. Calculaţi peste $y^2 = x^3 + 2x + 2 \mod 17$:

(a) $(6, 3) + (5, 1)$

(b) $(9, 1) + (9, 16)$

(c) $(5, 1) + (5, 1)$

Indicaţie: formulele de calcul pentru $P + Q = (x_1, y_1) + (x_2, y_2) = (x_3, y_3)$ peste $y^2 = x^3 + ax + b \mod p$:

$x_3 = s^2 - x_1 - x_2 \mod p$

$y_3 = s(x_1 - x_3) - y_1 \mod p$, unde:

$$s = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} \mod p & P \neq Q \\ \dfrac{3x_1^2 + a}{2y_1} \mod p & P = Q \end{cases}$$

8. Calculaţi toate punctele curbei eliptice $y^2 = x^3 + 2x + 1 \mod 7$