

(Toy) RSA

1. Fie $p = 41$ și $q = 17$ factorii modulului RSA.
 - (a) Care dintre $e_1 = 32$, $e_2 = 49$, $e_3 = 5$ este un coeficient de criptare valid?
 - (b) Calculați coeficientul de decriptare d .
2. Fie RSA cu $p = 31$, $q = 37$ și $e = 17$ (coeficientul de criptare). Determinați 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 și 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 $b = 0$, $y \xleftarrow{R} \mathbb{Z}_q$, $(c_1, c_2) = (g^y, h^y)$
 - (b) dacă $b = 1$, $y, z \xleftarrow{R} \mathbb{Z}_q$, $(c_1, c_2) = (g^y, h^z)$

Cerințe:

- (a) Arătați că decriptarea este eficientă dacă se cunoaște x .
 - (b) Arătați 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 biți). Se definește $\bar{m} = 0^k || r || 00000000 || m$, unde r este ales uniform aleator pe 10 bytes. Atunci $c = \bar{m}^e \pmod{N}$. Arătați că sistemul astfel definit nu este CCA-sigur.

Schimb de chei

5. Alice deține o pereche de chei (pk_A, sk_A) . Bob deține 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 (înmulțirea) cu $+$ (adunarea). Rămâne protocolul astfel definit sigur? Argumentați.

Calcul pe curbe eliptice

7. Calculați peste $y^2 = x^3 + 2x + 2 \pmod{17}$:

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

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

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

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

$$x_3 = s^2 - x_1 - x_2 \pmod{p}$$

$$y_3 = s(x_1 - x_3) - y_1 \pmod{p}, \text{ unde:}$$

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

8. Calculați toate punctele curbei eliptice $y^2 = x^3 + 2x + 1 \pmod{7}$