

# Examen de Criptografie Avansata

4 iunie 2021

1. *Elgamal* aditiv modulo  $n = 63$  cu generator  $g = 16$ .
  - (a) Alice alege cheia secreta  $x = 5$ . Bob alege cheia efemera  $y = 7$ . Calculati cheia publica a lui Alice. Aratati cum cripteaza Bob mesajul  $m = 9$  si cum decripteaza Alice mesajul criptat. (2P)
  - (b) Agentia Eva calculeaza  $g^{-1} \bmod n$  si gaseste cheia secreta a lui Alice folosind cheia ei publica. Efectuati calculele. (2P)
2. *Elgamal* multiplicativ modulo  $p = 19$  in grupul generat de  $g = 2$ . Alice are cheia publica  $h = 9$ . Bob trimite mesajul criptat  $(c_1, c_2) = (10, 11)$ . Decriptati mesajul. (4P)
3. *RSA*. Un mesaj  $m$  modulo 91 este criptat cu cheia publica  $e = 5$  si se obtine  $c = 5$ . Decriptati mesajul cu functia  $\mu(N)$ . (4P)
4. *RSA*. Decriptati mesajul de la Exerciitiul 3 cu functia  $\lambda(N)$ . (4P)
5. *Goldwasser-Micali*. Un mesaj criptat modulo 77 este format din numerele 23, 53, 36, 41. Decriptati mesajul. (4P)
6. *Shamir Secret Sharing*. Fie  $P \in \mathbb{Z}_{19}[X]$  un polinom de grad 2. Se considera urmatoarele perechi  $(\alpha, P(\alpha))$  unde  $\alpha \in \mathbb{Z}_{19} \setminus \{0\}$  si  $P(\alpha) \in \mathbb{Z}_{19}$ . Daca trei perechi sunt  $(1, 11)$ ,  $(2, 13)$  si  $(3, 16)$ , deduceti secretul partajat  $s = P(0) \in \mathbb{Z}_{19}$ . (4P)
7. *Cipolla*.
  - (a) Aratati ca 7 este rest patrat modulo 19. (1P)
  - (b) Gasiti radacinile patrute ale lui 7 modulo 19. In acest scop, aratati ca pentru  $a = 1$ ,  $a^2 - 7$  nu este rest patrat modulo 19 si calculati in corpul  $\mathbb{F}_{19}[\sqrt{13}]$ . (3P)
8. *Inele*. Un inel comutativ are exact 3 elemente multiplicativ inversabile. Numarul elementelor multiplicativ neinversabile este strict mai mic decat 5. Aratati ca inelul este corpul cu 4 elemente  $\mathbb{F}_4$ . *Indicatie: elementele inversabile formeaza un grup multiplicativ si elementul  $-1$  este element in acest grup.* (4P)

Pentru fiecare subiect rezolvat corect se acorda 4 puncte.

Fiecare invers modular fara calcul se penalizeaza cu 1 punct.

Fiecare exponentiere modulara fara calcul se penalizeaza cu 1 punct.