

## Examen de Protocoale Criptografice

17 mai 2024

1. *RSA*. Un mesaj  $m$  modulo 55 este criptat cu cheia publică  $e = 7$  și se obține  $c = 3$ . Decriptati mesajul cu funcția  $\lambda(N)$ .
2. *Elgamal* aditiv modulo  $n = 120$  cu generator  $g = 11$ . Alice are cheia publică  $h = 12$ . Bob trimite mesajul criptat  $(c_1, c_2) = (13, 14)$ . Decriptati mesajul.
3. *Elgamal* multiplicativ modulo  $p = 19$  în grupul generat de  $g = 2$ . Alice are cheia publică  $h = 6$ . Bob trimite mesajul criptat  $(c_1, c_2) = (7, 8)$ . Decriptati mesajul.
4. *Corpuri finite* Arătați că polinomul  $x^3 + x + 1$  este ireductibil peste corpul  $\mathbb{F}_2$ . Fie  $\omega$  o rădăcină a acestui polinom. Calculați elementul  $(\omega^2 + \omega)^{-1}$  în  $\mathbb{F}_8 = \mathbb{F}_2[\omega]$ .
5. *Shamir Secret Sharing*. Fie  $P \in \mathbb{Z}_{19}[X]$  un polinom de gradul 2. Se consideră următoarele perechi  $(\alpha, P(\alpha))$  unde  $\alpha \in \mathbb{Z}_{19} \setminus \{0\}$  și  $P(\alpha) \in \mathbb{Z}_{19}$ :  $(1, 6)$ ,  $(3, 15)$  și  $(6, 7)$ . Deduceți secretul partajat  $s = P(0) \in \mathbb{Z}_{19}$ .
6. *Secure Multiparty Computation* peste  $\mathbb{Z}$ . Valoarea secretă al lui Alice este  $x_1 = 1$ , valoarea secretă al lui Bob este  $x_2 = 4$  și valoarea secretă al lui Cesar este  $x_3 = 8$ . Ei vor să calculeze împreună cantitatea  $x_3(x_1 + x_2)$  fără a își destăinui valorile secrete. Pentru a partaja valori, ei folosesc polinoame liniare (de gradul 1). Pentru partajările inițiale, Alice folosește  $X + 1$ , Bob folosește  $2X + 4$  iar Cesar folosește  $3X + 8$ . Pentru a partaja înmulțirile locale, Alice folosește  $3X + a$ , Bob folosește  $X + b$  iar Cesar folosește  $2X + c$ . Efectuați protocolul pas cu pas.

Pentru fiecare exercițiu rezolvat corect se primesc 1,5 puncte. Un punct este din oficiu.

Pentru un invers modular corect, dar fără calculul aferent, se scad 0,375 puncte.

Pentru o exponențiere modulară corectă, dar fără calculul aferent, se scad 0,375 puncte.