Examen de Protocoale Criptografice

18 mai 2022

1. *RSA.* Un mesaj m modulo 91 este criptat cu cheia publica $e = 5$ si se obtine $c = 3$. Decriptati mesajul cu functia $\lambda(N)$.

2. *Elgamal* aditiv modulo $n = 100$ cu generator $g = 11$. Alice are cheia publica $h = 12$. Bob trimite mesajul criptat $(c_1, c_2) = (13, 14)$. Decriptati mesajul.

3. *Elgamal* multiplicativ modulo $p = 19$ in grupul generat de $g = 2$. Alice are cheia publica $h = 6$. Bob trimite mesajul criptat $(c_1, c_2) = (3, 4)$. Decriptati mesajul.

4. *Cipolla* Aratati ca 8 este un patrat modulo $p = 17$. Pentru $a = 1$, aratati ca $a^2 - 8$ nu este un patrat modulo 17. Folosind algoritmul lui Cipolla si $a = 1$, calculati $\sqrt{8} \bmod 17$.

5. *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 $P(\alpha) \in \mathbb{Z}_{19}$: $(10, 16)$, $(11, 0)$ si $(12, 5)$. Deduceti secretul partajat $s = P(0) \in \mathbb{Z}_{19}$.

6. *Secure Multiparty Computation peste* $\mathbb{Z}$. Valoarea secreta al lui Alice este $x_1 = 3$, valoarea secreta al lui Bob este $x_2 = 3$, si valoarea secreta al lui Cesar este $x_3 = 3$. Ei vor sa calculeze impreuna cantitatea $x_3(x_1 + x_2)$ fara a isi destainui valorile secrete. Pentru a partaja valori, ei folosesc polinoame liniare (de gradul 1). Pentru partajarile initiale, Alice foloseste $X + 3$, Bob foloseste $2X + 3$ iar Cesar foloseste $3X + 3$. Pentru a partaja inmultirile locale, Alice foloseste $3X + a$, Bob foloseste $X + b$ iar Cesar foloseste $2X + c$. Efectuati protocolul pas cu pas.

Pentru fiecare exercitiu rezolvat corect se primesc 1.5 points. Un punct este din oficiu.

Pentru invers modular corect, dar fara calculul aferent, se scad 0.375 puncte.

Pentru exponentiere modulara corecta, dar fara calculul aferent, se scad 0.375 puncte.