Examen de Protocoale Criptografice

8 iunie 2022

1. *Elgamal* aditiv modulo $n = 100$ cu generator $g = 33$.
   (a) Alice alege cheia secreta $x = 5$. Bob alege cheia efemera $y = 6$. Calculati cheia publica a lui Alice. Aratati cum cripteaza Bob mesajul $m = 7$ si cum decripteaza Alice mesajul criptat. (2P)
   (b) Agenta 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 $h = 13$. Bob trimite mesajul criptat $(c_1, c_2) = (15, 17)$. Decriptati mesajul. (4P)
3. *RSA.* Un mesaj m modulo 91 este criptat cu cheia publica $e = 7$ si se obtine $c = 10$. Decriptati mesajul cu functia $\lambda(N)$. (4P)
4. *Goldwasser-Micali.* Un mesaj criptat modulo 133 este format din numerele 95, 106, 38, 27. Decriptati mesajul. (4P)
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 $P(\alpha) \in \mathbb{Z}_{19}$: $(1, 9)$, $(2, 2)$ si $(3, 1)$. Deduceti secretul partajat $s = P(0) \in \mathbb{Z}_{19}$. (4P)
6. *Secure Multiparty Computation over* $\mathbb{Z}$. Valoarea secreta al lui Alice este $x_1 = 1$, valoarea secreta al lui Bob este $x_2 = 2$, si valoarea secreta al lui Cesar este $x_3 = 3$. Ei vor sa calculeze impreuna cantitatea $x_1x_2 + x_3$ fara a isi destainui valorile secrete. Pentru a partaja valori, ei folosesc polinoame liniare (de gradul 1). Pentru partajarile initiale, Alice foloseste $X + 1$, Bob foloseste $2X + 2$ iar Cesar foloseste $3X + 3$. Pentru a partaja inmultirile locale, Alice foloseste $4X + a$, Bob foloseste $5X + b$ iar Cesar foloseste $6X + c$. Efectuati protocolul pas cu pas. (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.