

Examen de Protocoale Criptografice

20 mai 2021

1. *Elgamal* aditiv modulo $n = 100$ cu generator $g = 51$.
 - (a) Alice alege cheia secreta $x = 49$. Bob alege cheia efemera $y = 47$. Calculati cheia publica a lui Alice. Aratati cum cripteaza Bob mesajul $m = 45$ 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 $h = 5$. Bob trimite mesajul criptat $(c_1, c_2) = (6, 7)$. Decriptati mesajul. (4P)
3. *RSA*. Un mesaj m modulo 91 este criptat cu cheia publica $e = 7$ si se obtine $c = 8$. Decriptati mesajul cu functia $\lambda(N)$. (4P)
4. *Goldwasser-Micali*. Un mesaj criptat modulo 77 este format din numerele 58, 71, 55, 17. 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 $P(\alpha) \in \mathbb{Z}_{19}$. Daca trei perechi sunt $(1, 6)$, $(2, 14)$ si $(3, 7)$, deduceti secretul partajat $s = P(0) \in \mathbb{Z}_{19}$. (4P)
6. *Secure Multiparty Computation over \mathbb{Z}* . Valoarea secreta al lui Alice este $x_1 = 10$, valoarea secreta al lui Bob este $x_2 = 11$, si valoarea secreta al lui Cesar este $x_3 = 12$. 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 factorul liniar 13, Bob foloseste factorul liniar 14 iar Cesar foloseste factorul liniar 15. Pentru a partaja inmultirile locale, Alice foloseste factorul liniar 16, Bob foloseste factorul liniar 17 iar Cesar foloseste factorul liniar 18. Efectuati protocolul pas cu pas.

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.