Examen de Criptografie Aplicata

27 ianuarie 2021

1. *Elgamal* aditiv modulo $n = 400$ cu generator $g = 199$.
   (a) Alice alege cheia secreta $x = 201$. Bob alege cheia efemera $y = 203$. Calculati cheia publica a lui Alice. Aratati cum cripteaza Bob mesajul $m = 205$ si cum decripteaza Alice mesajul criptat. (3P)
   (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 $h = 3$. Bob trimite mesajul criptat $(c_1, c_2) = (4, 5)$. Decriptati mesajul. (4P)
3. *RSA.* Un mesaj m modulo 91 este criptat cu cheia publica $e = 5$ si se obtine $c = 6$. Decriptati mesajul cu functia $\varphi(N)$. (4P)
4. *RSA.* Decriptati mesajul de la Exercitiul 3 cu functia $\lambda(N)$. (4P)
5. *Goldwasser-Micali.* Un mesaj criptat modulo 2021 este format din numerele 1626, 415, 475, 441. Decriptati mesajul stiind ca $2021 = 43 \cdot 47$. (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 $(5, 18)$, $(10, 14)$ si $(18, 10)$, deduceti secretul partajat $s = P(0) \in \mathbb{Z}_{19}$. (4P)
7. *Cipolla.*
   (a) Aratati ca 6 este rest patratic modulo 19. (1P)
   (b) Gasiti radacinile patrate ale lui 6 modulo 19. In acest scop, aratati ca pentru $a = 1$, $a^2 - 6$ nu este rest patratic modulo 19 si calculati in corpul $\mathbb{F}_{19}[\sqrt{14}]$. (3P)
8. *RSA.* Un programator implementeaza decriptarea RSA pentru un client care isi genereaza singur cheile, deci cunoaste factorizarea $N = pq$ si cheia secreta d. Programatorul scrie un program avand ca input mesajul criptat c, cheia secreta d si numerele prime p si q:

$$\begin{aligned} d_1 &= d \bmod (p-1); \\ d_2 &= d \bmod (q-1); \\ m_1 &= c^{d_1} \bmod p; \\ m_2 &= c^{d_2} \bmod q; \\ t &= p^{-1} \bmod q; \\ u &= (m_2 - m_1)t \bmod q; \\ m &= m_1 + up; \end{aligned}$$

   Oare acest program calculeaza intr-adevar mesajul clar m? Demonstrati raspunsul. (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.