Test seminar grupa 333, 26 aprilie 2018

Indicatorul lui Euler şi inversul modular

- Arătaţi (folosind definiţia lui φ), că $\varphi(243) = 162$. (2 puncte)
- Calculaţi inversul lui 13 in $\mathbb{Z}_{97}$. (3 puncte)

Securitate CPA

Se consideră cifrul (Enc, Dec), unde spaţiul mesajelor M şi cel al textelor cifrate C sunt $\{0,1\}^l$, iar spaţiul cheilor este mulţimea $\{1,\ldots,l\}$. Pentru o cheie $k \in K$ şi un mesaj $m \in M$, $Enc_k(m_1,\ldots,m_l) = (m_1,\ldots,m_{k-1},\overline{m_k},\overline{m_{k+1}},\ldots,\overline{m_l})$, unde $\overline{x} = x$ xor 1.

- Scrieţi funcţia de decriptare. (2 puncte)
- Construiţi un adversar care atinge avantaj 1 într-un atac cu text clar ales. (3 puncte)

Generatoare de numere pseudoaleatoare

Fie un generator de numere pseudoaleatoare $G : \{0,1\}^l \to \{0,1\}^{2l}$ astfel încât oricare ar fi s, ultimul bit al lui $G(s)$ este xorul celorlalţi $2l-1$ biţi. Arătaţi că G nu este sigur construind un adversar care are avantaj neneglijabil în jocul de securitate. (3 puncte)

RSA

- Cheia publică (N_1, e) a lui Alice este $(p_1 * q, 3)$, iar cheia publică lui Bob este $(N_2, e) = (p_2 * q, 3)$, unde p_1, p_2, q sunt numere prime distincte foarte mari (1024 biţi fiecare). Poate Oscar să găsească factorii primi din descompunerea lui N_1 şi a lui N_2 în timp fezabil? Argumentaţi. (3 puncte)
- Se dă un sistem RSA cu cheia publică (N, e) Ştiind că de-a lungul timpului au fost transmise perechile (mesaj clar, mesaj criptat) următoare $(246, 2), (58, 3), (249, 5), (225, 13)$, puteţi decripta mesajul $c = 18$? (4 puncte)