Test seminar grupa 334, 24 aprilie 2018

Indicatorul lui Euler

Arătaţi (folosind definiţia lui φ), că $\varphi(p^5) = p^4 \cdot (p-1)$ oricare ar fi un număr prim p. (1 punct)

Securitate CPA

Se consideră cifrul $(Enc,\ Dec)$, unde spaţiul mesajelor M şi cel al textelor cifrate C sunt $\{0,1\}^l$, iar spaţiul cheilor K este mulţimea permutărilor mulţimii $\{0,1,\ldots,l-1\}$. Pentru $k \in K$ şi $m \in M$, $Enc_k(m) = m[k[0]]\ldots m[k[l-1]]$, adică funcţia de cripare permută biţii lui m in funcţie de permutarea k.

- 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

1.

Fie un generator de numere pseudoaleatoare $G : \{0,1\}^l \to \{0,1\}^{2l}$ astfel încât ultimii 3 biţi ai lui $G(s)$ sunt mereu 0 oricare ar fi $s \in \{0,1\}^l$.

- Arătaţi că G nu este sigur. (3 puncte)
- Daţi exemplu de un test statistic de verificare a aleatorismului care va fi trecut de G (dacă l este suficient de mare), deşi G nu este sigur din punct de vedere matematic. Argumentaţi. (1 punct)

2.

Fie A o matrice publică de dimensiune $m \times n$ cu elemente din $\{0,1\}$ şi $m > n$. Se consideră generatorul de numere pseudoaleatoare $G : \{0,1\}^n \to \{0,1\}^m$ astfel încât $G(s) = A \cdot s \bmod 2$. Arătaţi că G nu este sigur oricare ar fi matricea A. (4 puncte)

RSA

Se consideră sistemul RSA cu modulul de criptare $n = p \cdot q$ unde p şi q sunt două numere prime impare astfel încât $|p-q| < n^{1/4}$. Notăm cu $A = \frac{p+q}{2}$ media aritmetică a numerelor p şi q şi cu $G = \sqrt{p \cdot q}$ media lor geometrică.

- Arătaţi că $A \geq G$ şi A este număr natural. (1 punct)
- Arătaţi că $A - G < 1$. (3 puncte)
- Argumentaţi de ce alegerea numerelor prime p şi q conduce la un sistem RSA vulnerabil. (2 puncte)