IMBUNATATIREA ALGORITMILOR DE CRIPTARE

LUMINITA SCRIPCARIU si PETRUT DUMA

Confidentialitatea informatiilor transmise intr-un sistem de comunicatii digitale este asiguratä folosind diferiti algoritmi de criptare. Permutarea simbolurilor se poate efectua mat eficient folosind familii de functii polinomiale inversabile cu coeficienti din diverse câmpuri Galois, in locul tabelelor de permutare impuse. Generarea cheilor de criptare se poate realiza fara periodicitate folosind generatoare numerice haotice, de tipul sistemului lui Baptista. Imbunatatirea celur doua elemente ale criptosistemului cresc robustetea oricarui algoritm de criptare cunoscut.