MINIMIZAREA CORELAȚIILOR ÎN ŞIRURILE DE DATE CRIPTATE

LUMINIȚA SCRIPCARIU şi PETRUȚ DUMA

Confidențialitatea şi secretul informații1or transmise prin rețelele de calculatoare sunt asigurate pe baza algoritmilor de criptare. Proprietățile de corelație ale secvențe1or criptate pot fi exploatate în diverse atacuri criptografice pentru deducerea cheilor de criptare. Reducerea corelațiilor din şirurile de date criptate constituie principiul de optimizare a algoritmilor de criptare. În această lucrare sunt prezentați şi ana1izați algoritmii de criptare clasici RSA şi AES, precum şi un algoritm de criptare propriu, denumit algoritmul GLIM, bazat pe structuri de date mari, multidimensionale. Simulările pe calculator au permis deducerea valorilor medii şi standard ale gradului de încredere oferit de textul criptat prin cei trei algoritmi, ca o măsură a corelațiilor existente în acesta. Compararea valorilor obținute a scos în evidență performanțele diferite dar comparabile ale acestor algoritmi şi posibilitatea de optimizare a lor în vederea reducerii corelațiilor dintre secvența originală şi cea criptată. prin folosirea structurilor de date multidimensionale.