



C.P. 16 – 162, 062510 – BUCUREȘTI

tel. 021.4113617, fax 021.4114280

e-mail. [office@matrixrom.ro](mailto:office@matrixrom.ro), [www.matrixrom.ro](http://www.matrixrom.ro)

## **Criptografie si securitatea informatiei. Aplicatii**

Capitolul 1. Sistemul de cifrare Cezar

Capitolul 2. Metoda substitutiei

Capitolul 3. Sistemul de cifrare Playfair

Capitolul 4. Sistemul de cifrare Hill

Capitolul 5. Sisteme de cifrare polialfabetice

Capitolul 6. Metoda transpozitiei

Capitolul 7. Sisteme mixte

Capitolul 8. Generatoare pseudoaleatoare

Capitolul 9. Calcule in corpuri Galois

Capitolul 10. Algoritmul RIJNDAEL - Standardul AES

Capitolul 11. Criptanaliza cifrurilor bloc

Capitolul 12. Lema chinezeasca a resturilor

Capitolul 13. Sistemul de cifrare Merkle-Hellman

Capitolul 14. Sistemul de cifrare RSA

Capitolul 15. Sistemul de cifrare ElGamal

Capitolul 16. Aritmetica pe curbe eliptice

Capitolul 17. Sistemul de cifrare ElGamal bazat pe curbe eliptice

Capitolul 18. Sistemul de cifrare Menezes-Vanstone

Capitolul 19. Semnatura ElGamal

Capitolul 20. Semnatura DSA

Capitolul 21. Protocolul Diffie-Hellman de stabilire a cheilor

Capitolul 22. Sistemul Shamir de partajare a secretelor

Capitolul 23. Canale subliminale

Capitolul 24. Principii criptografice

Capitolul 25. Atacuri in mediul de implementare

Capitolul 26. Resurse software

Capitolul 27. Teste grila