Planul cursului

1. Cifruri "istorice" simetrice. Substituţii monoalfabetice. Substituţii polialfabetice (Vigenère, Hill). Criptanaliza.
2. Criptosisteme "perfect sigure". Cifrul Vernam (one-time-pad). Teorema lui Shannon.
3. Criptosisteme simetrice moderne: (baby) DES, (baby) AES (ambele facultativ).
4. Criptografia cu cheie publică
   (a) logaritmul discret, atacuri (Shanks (coliziuni), Pohlig-Hellman. Pollard ρ (facultativ))
   (b) protocolul Diffie-Hellman, criptosistemul ElGamal, signatura digitală ElGamal
   (c) criptosistemul RSA, signatura digitală RSA, atacuri (asupra modulului comun, Hastad (asupra exponentului de criptare mic), Wiener (asupra exponentului de decriptare mic), atacul ciclic)
   (d) criptosistemul knapsack; criptanaliza; aplicaţii ale teoriei laticelor în criptografie.
5. Criptografie pe curbe eliptice.
6. Criptografia cuantică (doar o poveste fantastică?).

Bibliografie

1. J.Hoffstein, J.Pipher, J.Silverman, An Introduction to Mathematical Cryptography, Springer, 2008
2. S.Singh, Cartea Codurilor, Humanitas, 2005.
3. C.Gherghe, D.Popescu, Criptografie, Coduri, Algoritmi, Ed.Universităţii, 2005