DISKREČIOJI MATEMATIKA
Kriptologija *Paskaitų kurso programa*

1. Kriptologija, kriptografija, kriptoanalizė: kas tai yra
2. Kriptografinės sistemos
3. Kriptografinės sistemos slaptumo matas
4. Simetrinės kriptografinės sistemos
   4.1 Cezario ir Vižene šifrai
   4.2 Kasiskio ir Frydmano testai
   4.3 Vienkartinio rakto sistema
5. Algoritmų sudėtingumo problema
   5.1 Polinominio laiko algoritmai
   5.2 NP problemos
6. Vienakryptės funkcijos
7. Asimetrinės kriptografinės sistemos
   7.1 Lucifer kriptosistema
   7.2 Kriptosistema be raktų
   7.3 Viešo rakto kriptosistemos
      7.3.1 RSA
      7.3.2 Merkle-Hellman'o ("kuprinės") kriptosistema
8. Elektroninis parašas

Literatūra

1. Beutelspacher A. Kryptologie, *Braunschweig: Vieweg*, 1994.
2. Koblitz N. A course in Number theory and Cryptography, *Springer Verlag*, 1987.
3. Koblitz N. Algebraic Aspects of Cryptography, *Springer Verlag*, 1998.
4. Stakėnas V. Informacijos kodavimas, *Vilnius: Vilniaus universitetas*, 1996.
5. Welsh D. Codes and Cryptography, *Oxford: Clarendon Press*, 1988.

Sudarė: A. Mačiulis