CONTENTS of IV054 LECTURES in 2009

Prof. Jozef Gruska, DrSc

1. Introduction to coding theory.
2. Linear codes.
3. Cyclic and convolution codes .
4. Secret-key cryptosystem - cryptomachines
5. Public-key cryptosystems: key-exchange, knapsack, RSA
6. Other public-key cryptosystems, security definitions, pseudo-random generators, hash functions
7. Digital signatures.
8. Elliptic curves cryptography, factorization.
9. Authentication, identification, secret sharing and e-business
10. Bit commitment, oblivious transfer, zero-knowledge and other crypto-protocols
11. Steganography and watermarking.
12. From crypto-theory to crypto-practice
13. Quantum cryptography