

Comprehensive exam Cryptography

Syllabus Mathematical foundations; radix representation, and its generalizations, algorithms for basic operations, congruences, discrete logarithm, operations with residue classes. The greatest common divisor, prime factorization, lattices, the LLL algorithm. Elliptic curves over finite fields, the discrete elliptic logarithm. Algorithms for symmetric and asymmetric encryption. Algoritmusok: szimmetrikus és aszimmetrikus titkosítás. Basic properties of the DES, AES, RSA, ElGamal and the elliptic curve cryptography. Authentication, digital signature, secret sharing and key exchange. Formal verification of protocols Public key infrastructure. Post-quantum cryptography

- Bibliography**
1. Attila Pethő, *Algebraische Algorithmen*, Vieweg Verlag, 1999.
 2. Johannes Buchmann, *Introduction to cryptography*. Second edition. Undergraduate Texts in Mathematics. *Springer-Verlag, New York*, 2004.
 3. H. Cohen and G. Frey Eds.: *Handbook of Elliptic and Hyperelliptic Curve Cryptography*, Chapman & Hall/CRC, 2005.
 4. D. Hankerson, A. Menezes and S. Vanstone, *Guide to Elliptic Curve Cryptography*, Springer, 2005.
 5. D.J. Bernstein, J. Buchmann and E. Dahmen, Eds.: *Post-quantum cryptography*, Springer, 2009.