Course EE720: Introduction to Number Theory and Cryptography

Instructor: Virendra Sule
vrs@ee.iitb.ac.in

January 7, 2016

Course plan

- Offered Spring 2014-15.
- Open to: 3rd, 4th year UG/DD and M. Tech./Ph.D.

Topics planned to be covered

1. Introduction to requirements and functionalities of cryptography. One way and trapdoor one way functions. Symmetric and public key crptography. Applications of cryptography and real world constraints and scope. Cryptanalysis and evaluation of strength of cryptographic primitives. Conceptual formulation of cryptographic schemes.

2. Basic background of finite fields, modular arithmetic and computations. Algorithms for solving Boolean systems and systems of equations over finite fields (optional). Basic probabilistic analysis, birthday paradox, perfect secrecy.

3. Block and stream ciphers, AES, e-stream ciphers. Cipher algotihm design considerations. Results on feedback shift register sequences. Hash functions. MACs. Key management.

4. Elements of number theory: Euclidean division to Chinese Reminder theorem, groups, Lagrange, Fermat and Euler theorems, Euler function.

5. Construction of Public key primitives: RSA, Diffie Hellman, El Gammal. Hash functions and signatures. Elliptic curves and their application in cryptography. Methods of RSA factorization and discrete log computation over prime fields.

6. Algorithms for arithmetic: large integer multiplication and division, modular arithmetic, finite field arithmetic (optional). Elliptic curve arithmetic and elliptic curve cryptography (basic illustrative examples).

7. (If time permits): Introduction to Quantum cryptography.

A limited list of references is given below. For further information and clarification you may contact the instructor.

References

[1] Simon Singh, Code Breakers, Fourth Estate Publishers, London, 1999.

[2] Waade Trape and Lawrence Washington, Introduction to cryptography and coding theory. Pearson 2006.

[3] Johanne Buchmann, Introduction to cryptography, Springer, 2006.

[4] Serge Vaudeney, Classical introduction to cyptography, Springer, 2006.

[5] Bruce Schneier, Applied Cryptography, John Wiley, 2002.

[6] A. Menezes, van Oorschot, Vanstone, Handbook of applied cryptography, CRC Press 1997.

[7] Christof Paar, Jan Pelzl. Understanding Cryptography. Springer 2010.