KUNGL TEKNISKA HÖGSKOLAN

Datavetenskap och kommunikation
Johan Håstad

11 mars 2009

DD2449, Foundations of Cryptography, 2009

As topics are planned in detail pointers to relevant chapters in Stinson (edition 3) get more detailed.

1 Lectures that have taken place

F1 Overview of course. Classical cryptography: Simple Substitution (1.1.2), Ceasar Shift (1.1.1), OneTimeTapes (1.1.7), Vigenère (1.1.4), Transposition (1.1.6, but we used other definition), Geheim-Schreiber (handout).

F2 Discussion of security. Information theoretic security of OTT (2.3), cryptanalysis of Vigenère (2.3).

F3 Entropy, definition and basic properties (2.4-2.5)

F4 Entropy finished. Definition of DES (3.5), priciples and modes for block ciphers (3.7).

F5 Futher discussion of DES including linear cryptanalysis (3.5). Start of finite fields.

F6 Finite fields (6.4) and efficient modular arithmetic, including division (5.2.1) major part of AES (3.6).

F7 AES completed. The idea of public key encryption, Fermat's theorem (5.1-5.2).

F8 Primality testing, Fermat's little theorem, RSA (chapter 5).

F9 RSA complete, quick discussion of factoring (5.6), some attacks (5.7). Mentioned power and timing attacks. Introduction to the discrete logarithm problem.

F10 The discrete logarithm problem, Diffie-Hellman key exchange, El-Gamal encryption (chapter 6.1,6.2). Baby-step, giant step algorithm.

F11 Hash functions. The birthday paradox, general theory and Merkle-Damgård construction (4.1, 4.3). Message Authentication codes (MACs, 4.4, 4.5). Introduction to signatures (7.1).

F12 RSA signatures (7.2), Schnorr identification (9.4) and zero-knowledge (chapter 9,4).

F13 Schnorr signatures (7.4.1) completeted and Elliptic curves (chapter 6.5).

F14 Pseudorandom generators, Linear Congruential Generators (chapter 8.1,8.2), Linear Feedback Shift Registers (1.2).

F15 A guest lecture by Mats Näslund, Ericsson.