KUNGL TEKNISKA HÖGSKOLAN
Datavetenskap och kommunikation
Johan Håstad

9 mars 2007

2D1449, Foundations of Cryptography, 2007

Plan of lectures combined to some reading pointers for Stinson, edition 3.

Note that we are currently behind in the lectures, in fact essentially two lectures already. This implies that some topics will be skipped.

1 Lectures in the past

F1 Overview. Classical cryptography, simple substitution (1.1.2), Vigenère (1.1.4), Transposition (1.1.6), One time Tape (1.1.7,2.3), Geheim-Schreiber (handout).

F2 Security of OTT (2.3), cryptanalysis of Viginère (1.2.3).

F3 Entropy (2.4-2.6).

F4 DES (3.5)

F5 Properties of DES, linear and differential cryptanalysis (3.3-3.4).

F6 Modes of block ciphers (3.7), finite fields (6.4).

F7 AES (3.6)

F8 Primality testing (Miller-Rabin), Fermat's theorem, initial RSA (5.2-5.3).

F9 RSA, attacks on RSA (5.6-5.7).

F10 El-Gamal (6.1) encryption and Diffie-Hellman key exchange (11.2) , algorithms for discrete logarithms (6.2).

F11 Hashing algorithms (4.1-4.2), SHA-1 (4.3.2), Digital signatures with RSA (7.1-7.2, 7.4.2), key distribution, (10.2) Schnorr identification (9.4).

F12 Schnorr identification (9.4) and signatures (7.4.1), zero-knowledge (9.4).

F13 Elliptic curves (6.5).

F14 A guest lecture by Mats Näslund, Ericsson.

F15 A guest lecture by Lennart Brynielsson, TSA with some discussion of real uses of cryptography and pseudo-random generators (1.1.7, 8.1-8.2).