



DD2449, Foundations of Cryptography, 2008

Topics of lectures combined with some reading pointers for Stinson, edition 3.

1 Lectures as they happened

- 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), information theoretic security. Cryptanalysis of Vigenère (1.2.3) and transposition, Start of entropy.
- F3** Relation of entropy to encoding length. Proof of some of its properties (2.4-2.5). Clear text redundancy as a key factor for attacking encryption (2.8).
- F4** DES, definition and properties (3.5). Modes of block ciphers (3.7).
- F5** Linear cryptanalysis (3.3), finite fields (6.4), Euclidean algorithm for inverses in finite fields and modular arithmetic (5.2.1).
- F6** AES, formal description and discussions (3.6).
- F7** Primality testing (Miller-Rabin), Fermat's theorem, RSA (5.2-5.3).
- F8** Attacks on RSA (5.6-5.7), Chinese remainder theorem (5.2.2), introduction to the discrete logarithm problem (6.2), Diffie-Hellman key exchange (11.2).
- F9** El-Gamal (6.1) encryption, algorithms for discrete logarithms (6.2). Preliminary discussion of hash functions, collision probability (4.1).
- F10** Pollard rho-method for attacking hash-algorithms. General facts about hash-algorithms (4.1-4.2), SHA-1 (4.3.2)
- F11** MACs (4.4-4.5), digital signatures with RSA (7.1-7.2, 7.4.2), Started discussing Schnorr identification.
- F12** Schnorr identification (9.4) and signatures (7.4.1), zero-knowledge (9.4).
- F13** Elliptic curves (6.5).
- F14** Pseudorandom generators (1.2.5), (8)
- F15** A guest lecture by Mats Näslund, Ericsson.