T-79. 503

Foundations of Cryptology

Fall term 2003

AGENDA

Version 1 (September 10)

Week	**Topics**	**Study material** (numbers refer to textbook sections)
37	History; Background; Classical Cryptosystems; Inverting Matrices; Kasiski Method; Cryptanalysis	1.1.1 - 1.1.6; 1.2.1 – 1.2.4
38	Stream Ciphers; Linear Feedback Shift Registers; Periods of LFSR sequences	1.1.7; 1.2.5; Handout 1 - LFSRs
39	Shannon theory; Perfect Secrecy; Entropy;	2.1; 2.2; 2.3; 2.4;
40	Conditional Entropy; Secrecy Systems; Unicity Distance ; Unicity Distance – Example	2.4; 2.5; 2.6; Handout 2 – Unicity Distance
41	Diffusion and Confusion; Block cipher design criteria; Feistel cipher;DES – Description; SPN network; AES – Description;	2.7; 3.2; 3.5; 3.6; 3.7;
42	Differential Cryptanalysis; Linear Cryptanalysis; Piling-up Lemma; Non-Linearity of Boolean Functions;	3.3; 3.4; Handout 3 - Differential cryptanalysis; Handout 4 – Linear Cryptanalysis; 3.3; 3.6
43	Block cipher Modes of Operation; Hash functions; Birthday Paradox; SHA-1; HMAC	3.7; 4.1; 4.2 (intro); 4.2.2 (Birthday attack); 4.3 (intro); 4.3.2; 4.4
44	Euclid's Algorithm; Chinese Remainder Theorem; Euler Phi-Function; Structure of Finite Fields; RSA Cryptosystem	5.2; Handout 5 – More Number Theory; 5.3
45	Square and Multiply Algorithm; Quadratic residues;Jacobi Symbol; Solovay-Strassen Primality Test ;	5.3; 5.4 (only Solovay-Strassen)
46	Factoring; Attacks on RSA: known decryption exponent; small encryption exponent; Rabin Cryptosystem	5.6.1; 5.7; 5.8
47	Discrete Log Problem; ElGamal Cryptosystem; Shanks' Algorithm; Pohlig-Hellman Algorithm;	6.1; 6.2.1; 6.2.3;
48	Galois Fields; Elliptic Curves	6.4; 6.5.
49 3 Dec	No Lecture; No Exercises	
50	Digital Signature Schemes (RSA, ElGamal, DSA)	7.1; 7.2; 7.3;7.4.2