T-79. 503 Foundations of Cryptology

AGENDA Fall 2004

Version1 (16-9-2004)

Week	**Topics**	**Study material** (numbers refer to textbook sections)
38	History; Background; Classical Cryptosystems; Inverting Matrices; Kasiski Method;	1.1.1 - 1.1.6; 1.2.1 – 1.2.4
39	Stream Ciphers; Linear Feedback Shift Registers; Periods of LFSR sequences	1.1.7; 1.2.5; Handout 1 - LFSRs
40	Linear Complexity; Berlekamp-Massey algorithm; Shannon theory; Perfect Secrecy;	Handout 2 – Linear Complexity 2.1; 2.2; 2.3;
41	Entropy; Conditional Entropy; Secrecy Systems; Unicity Distance; Diffusion and Confusion; Block cipher design criteria;	2.4; 2.5; 2.6; 2.7;
42	Feistel cipher;DES – Description; SPN network; AES – Description; Block cipher Modes of Operation;	3.2; 3.5; 3.6; 3.7;
43	Euclid's Algorithm; Chinese Remainder Theorem; Euler Phi-Function; Structure of Finite Fields; Boolean functions; Algebraic normal form	5.2; 6.4; Handout 3 (Euler Phi-function and Boolean functions)
44	Nonlinearity of Boolean functions; Linear Cryptanalysis; Differential Cryptanalysis; Rijndael (AES) S-box	Handout 3; 3.3; 3.4; 3.6.1
45 Room change T2 -> T5	Hash functions; Birthday Paradox; SHA-1; HMAC	4.1; 4.2 (intro); 4.2.2 (Birthday attack); 4.3 (intro); 4.3.2; 4.4
46	RSA Cryptosystem; Square and Multiply Algorithm; Quadratic residues;Jacobi Symbol; Solovay-Strassen Primality Test	5.3; 5.4 (only Solovay-Strassen)
47	Factoring; Attacks on RSA: known decryption exponent; small encryption exponent; Rabin Cryptosystem	5.6.1; 5.7; 5.8
48	Discrete Log Problem; ElGamal Cryptosystem; Shanks' Algorithm; Pohlig-Hellman Algorithm;	6.1; 6.2.1; 6.2.3;
49	Elliptic Curves; Digital Signature Schemes (RSA, ElGamal, DSA)	6.5. 7.1; 7.2; 7.3;7.4.2
50 9 Dec	No lectures. Only one exercise group: 16-18	