T-79. 5501 Cryptology

AGENDA Fall 2005

September 2, 2005

Week	**Topics**	**Study material** (numbers refer to textbook sections)
37	Shannon's theory; Perfect Secrecy; Entropy; Conditional Entropy;	2.1 -2.5
38	Unicity Distance; Diffusion and Confusion; Block cipher design criteria; Stream cipher design criteria; Modular Arithmetic; Euclid's algorithm, Chinese Remainder Theorem; Euler Phi-Function	2.6 – 2.7; Lecture notes 1.1; 5.2
39	Structure of Finite Fields; Linear Feedback Shift Registers; Periods of LFSR sequences; Linear Complexity; Berlekamp-Massey algorithm	6.4; Lecture notes
40	Boolean functions; Algebraic normal form; Nonlinearity of Boolean functions; Bent functions; Correlation properties of stream ciphers;	Lecture notes
41	Linear Cryptanalysis of block ciphers	3.1 - 3.3
42	Differential Cryptanalysis; Rijndael (AES) S-box	3.4 - 3.6
44	RSA Cryptosystem; Square and Multiply Algorithm; Quadratic residues;Jacobi Symbol;	5.3
45	Solovay-Strassen Primality Test; Miller-Rabin Primality Test; Square roots; Factoring	5.4 – 5.6
46	Attacks on RSA: known decryption exponent; small encryption exponent; Rabin Cryptosystem	5.7 – 5.8
47	Discrete Log Problem; Shanks' Algorithm; Pohlig-Hellman Algorithm; Elliptic Curves;	6.1; 6.2; 6.5
48	ElGamal Cryptosystem; Diffie-Hellman key exchange; Digital Signature Schemes (RSA, ElGamal, DSA)	6.1; 7.1 – 7.4