Applied Cryptography (CS6530)

Jan - April 2018

Chester Rebeiro, IIT Madras

Schedule

Quiz and End Sem Schedule	**Grading Policy**
Quiz 1 : 16/2/2018 (8:00 - 9:00 AM) **Quiz 2** : 6/3/2018 (8:00 - 9:00 AM) **EndSem** : 8/5/2018 (9:00 - 10:00 AM)	Tutorials: 20 Quiz 1: 20 Quiz 2: 20 Project: 20 Endsem: 20
Attendance requirements as per Institute norms	

Class	Coverage
[1] 17/1/2018 (W)	Introduction to the course
[2] 18/1/2018 (Th)	**Classical Cryptography** cryptosystems (P,C,K,E,D), attack models
[3] 19/1/2018 (Fr)	shift cipher, substitution cipher, polyalphabetic ciphers, vigenere cipher,
[4] 23/1/2018 (Tu)	Modular arithmetic; Hill Cipher
[5] 24/1/2018 (W)	permutation cipher, block cipher (introduction), stream cipher (introduction), introduction to perfect secrecy
[6] 25/1/2018 (Th)	**Perfect secrecy** Perfect secrecy apriori and aposteriori probabilities, Shannon's theory

[7] 30/1/2018 (Tu)	Tutorial 1 (Classical Cryptography)
[8] 31/1/2018 (W)	One time pad, entropy
[9] 1/2/2018 (Th)	Huffman Coding, Language redundancy, Unicity distance
[10] 2/2/2018 (F)	**Block Ciphers** Product Ciphers, Iterative ciphers, Block Ciphers Introduction
[11] 6/2/2018 (Tu)	Tutorial 2 (Perfect Secrecy)
[12] 7/2/2018 (W)	s-boxes and diffusion layers.
[13] 8/2/2018 (Th)	SPN Networks, Feistel ciphers, Linear Cryptanalysis
[14] 9/2/2018 (F)	Linear Cryptanalysis
[15] 13/2/2018 (Tu)	Linear Cryptanalysis and Differential Cryptanalysis
[16] 15/2/2018 (Th)	DES, Modes of Operation
[17] 16/2/2018 (F)	Quiz 1 (syllabus till differential cryptanalysis)
[18] 20/2/2018 (Tu)	Modes of Operation; SBox Design
[19] 21/2/2018 (W)	SBox design
[20] 22/2/2018 (Th)	Finite fields
[21] 23/2/2018 (Fr)	Finite Fields (Quiz 1 answer scripts distributed)
[22] 27/2/2018 (Tu)	Tutorial 3 (DES, Finite fields, modes of operation)
[23] 28/2/2018 (W)	AES Encryption and Decryption
[24] 1/3/2018 (Th)	AES Implementation Aspects (Composite field Implementation of SBoxes)
[25] 6/3/2018 (Tu)	AES Bitslice implementation and T-Table implementation
[26] 7/3/2018 (W)	Attacks on AES (Square Attack / Related Key Attack); Hash functions
[27] 8/3/2018 (Th)	**Hash functions** the RO model, hash function security problems
[28] 9/3/2018 (F)	Security proofs in the RO model; Iterated hash functions
[29] 13/3/2018 (Tu)	Cache Timing Attacks on AES (Tutorial 4, take home)

[30] 14/3/2018 (W)	Merkle Damgard Construction; Collisions in MD5
[31] 15/3/2018 (Th)	MAC
[32] 16/3/2018 (F)	**Public Key Ciphers** Number Theory (Extended Euclidean Algorithm and CRT)
[33] 20/3/2018 (Tu)	Tutorial 5 on hash functions
[34] 21/3/2018 (W)	Introduction to PKC and RSA
[35] 22/3/2018 (Th)	RSA introduction, multi-precision arithmetic
[36] 23/3/2018 (Fr)	Montgomery multiplication and the montgomery ladder
[37] 26/3/2018 (M)	Primality testing algorithms : Fermat's based and Miller-Rabin
[38] 27/3/2018 (Tu)	Solvay Strassen; Factorization Algorithms (Pollard p - 1)
[39] 28/3/2018 (W)	Pollard RHO algorithm
[40] 3/4/2018 (Tu)	Tutorial 6 (Public Key ciphers)
[41] 4/4/2018 (W)	Dixons Random Squares; Backdoor attack
[42] 5/4/2018 (Th)	Backdoor attacks
[43] 6/4/2018 (F)	Quiz 2 (AES, modes of operation, Hash functions, Public key ciphers till Pollard Rho)
[44] 10/4/2018 (Tu)	Backdoor attacks, discrete log problem
[45] 11/4/2018 (W)	ElGamal, DiffieHellman, Shank's algorithm Elliptic Curve Crypto
[46] 12/4/2018 (Th)	**Elliptic Curve Cryptography** Weierstrass equation, point doubling, point addition and scalar multiplier
[47] 13/4/2018 (F)	ECC projective coordinates, ECC encryption and key exchange
[48] 17/4/2018 (Tu)	**Digital Signatures** Introduction, difference with MAC; RSA Digital signatures
[49] 18/4/2018 (W)	Elgamal signatures,
[50] 19/4/2018 (Th)	**Bitcoin and Blockchain**
[51] 20/4/2018 (F)	Bitcoin and Blockchain

[52] 24/4/2018 (Tu)	Invited talk from IBM Research (Non-interactive zero knowledge proofs)
[53] 25/4/2018 (W)	Assignment Evaluation
[54] 26/4/2018 (Th)	Assignment Evaluation
[55] 27/4/2018 (Fr)	Tutorial 7: ecc, bitcoin, signatures
8/5/2018 (Tu) 9:00AM	End Sem (syllabus from RSA (RSA included))