Second semester 2016-17 02.08.2016

Course Handout Part II

In addition to the Part-I (General Handout) for all courses appended to the timetable, this portion gives further specific details regarding the course.

Course No.: BITS F463

Course Title: Cryptography

Instructor: Ashutosh Bhatia

Email: ashutosh.bhatia@pilani.bits-pilani.ac.in

Description: This course is an introduction to the basic theory and practice of cryptographic techniques used in computer security. We will cover topics such as encryption (secret-key and public-key), message integrity, digital signatures, user authentication, key management, cryptographic hashing, Network security protocols (SSL, IPsec), public-key infrastructure, digital rights management, and a bit of advancement in modern cryptology such as Identity Based Encryption, Steganography and Watermarking, Quantum Cryptographic and Zero-Knowledge protocols.

Prerequisites: The course is self-contained, however a basic understanding of probability theory, information theory, complexity theory and modular arithmetic from number theory will be helpful. The course is intended for advanced undergraduates and master students.

Course Objectives: Lectures deal with the basic methods to solve three key problems of the transmission of information. All three problems are of large practical importance and their solutions are based on elegant theoretical results. On successful completion of the course students should be able to: understand basic principles and results of the theory of secure communication; know principles and problems of basic cryptosystems for encryption (both secret and public key), digital signing and authentication; know methods to create core cryptographic protocols primitives; analyze and practically use simple cryptosystems; be experienced in methods of quantum cryptography and steganography

Text Book:

[T1] B.A. Forouzan, D. Mukhopadhyay, Cryptography and Network Security, 2nd Edition, 2011, Mcgraw Hill Education.

[T2] Bruce Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, Second Edition 1995, John Wiley & Sons

Reference Books:

[R1] Douglas R. Stinson, "Cryptography Theory and Practice", Chapman & Hall/CRC, Third Edition, 2006.

[R2] A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996. Available online at: http://cacr.uwaterloo.ca/hac/

[R3] S.Goldwasser, M. Bellare, Lecture Notes on Cryptography, 2008. Available online at: https://cseweb.ucsd.edu/~mihir/papers/gb.pdf

[R4] O. Goldreich, Foundations of Cryptography Volume 1: Basic Tools, Cambridge University Press, 2004. Available online at: http://www.wisdom.weizmann.ac.il/~oded/foc-drafts.html

[R5] O. Goldreich, Foundations of Cryptography Volume 2: Basic Applications, Cambridge University Press, 2004. Available online at: http://www.wisdom.weizmann.ac.il/~oded/ focdrafts.html

[R6] W. Stallings, Cryptography and Network Security: Principles and Practice, 6th Edition, 2014, Pearson.

[R7] Cryptography – 1, an online course on "Coursera", Taught By: Prof. Dan Boneh, Dept. of Computer Science and Electrical Engineering, Stanford University. URL: https://www.coursera.org/learn/crypto

[R8] https://en.wikibooks.org/wiki/High_School_Mathematics_Extensions/Discrete_Probability

Lecture Plan

Faculty: Prof. Ashutosh Bhatia Hrs:40

Lecture #	Topics to be covered	Reading
Module 1: Introduction to Cryptography		
1	Introduction	Lecture Slides
2	History of Cryptography	Lecture Slides
3	Some Simple Crypto Systems – 1 : Shift Cipher, Substitution Cipher, Affine Cipher	R1.1.1
4	Some Simple Crypto Systems – 2 : Vigenere Cipher, Hill Cipher, Permutation Cipher	R1.1.1
Module 2: Mathematical Foundation - 1		
5	Probability Theory, Randomized Algorithm, Property of XOR, Birthday Paradox	R8
6	Background on Functions	R2.1.3
7	Number Theory: Integer Arithmetic, Modular Arithmetic	T1.2.1, T1.2.2
8	Linear Congruence	T1.2.4
9	Algebraic Structures, Finite Fields	T1.4
10	Polynomial Arithmetic	T1.4
Module 3: Classical Crypto Systems		
11	Information Theoretic Security, The One Time Pad	
12	Shanon's Theory	R1.2
13	Stream Ciphers and Pseudo Random Number Generators	T2.16

14	Attacks on Stream Ciphers and One Time Pad	Lectures Slides
15	Semantic Security	Lectures Slides
Module 4: Symmetric Key Encryption		
15	Data Encryption Standard (DES) - 1	T1.6
16	Data Encryption Standard (DES) – 2	T1.6
17	Combining Block Ciphers: Double Encryption, Triple Encryption	T2.15
18	Modes of Block Ciphers - 1 (ECB, CBC)	T2.9
19	Modes of Block Ciphers - 2 (CFB, OFB, CTR)	T2.9
20	Advanced Encryption Standard (AES) – 1	T1.7
21	Advanced Encryption Standard (AES) – 2	T1.7
Module 5: Mathematical Foundation - 2		
23	Prime Numbers, Fermet's Little Theorem, Euler Theorem, Chinese Remainder Theorem,	T1.9.1-9.3
24	Primality Testing, Factorization	T1.9.4
35	Discrete Logarithms	
Module 6: Asymmetric Key Encryption		
26	Intro to Public-Key Crypto, RSA	T1.10.1-2
27	Discrete Logarithm Based Cryptosystems: ElGamal	T1.10.4
28	Elliptic Curve cryptography, Digital Signatures	
Module 7: Data Integrity, Authentication		
29	Message Integrity	T1.11.1
30	Message Authentication, Message Authentication Codes (MACs)	T1.11.3
31	Cryptographic Hash Functions	T1.12
32	Authenticated Encryption: Hash Functions and MACs, Zero Knowledge Proof	
Module 8: Modern Trends in Cryptography		
33	Identity Based Encryption	Lecture Slides
34	Quantum Cryptographic Protocols	Lecture Slides
35	Steganography and Watermarking	Lecture Slides
Module 9: Cryptographic Protocols		
36	Protocol Building Blocks	T2.2
37	Basic Protocols 1 - Key Exchange, Authentication, Authentication and Key Exchange	T2.3
38	Basic Protocols 2 - Formal Analysis of Authentication and Key-Exchange Protocols	T2.3
39	Intermediate Protocols 1 - : Timestamping Services, Subliminal Channel	T2.4
40	Intermediate Protocols 2 - : Undeniable Digital Signatures, Designated Confirmer Signatures	T2.4

Malpractice Regulations: The following regulations are supplementary to BITS-wide policies regarding malpractices:

1. Any student or team of students involved/found involved in malpractices in working out assignments / projects will be awarded a zero for that assignment / project and will be blacklisted.
2. Any student or team of students found repeatedly – more than once across all courses – involved in malpractices will be reported to the Disciplinary Committee for further action. This will be in addition to the sanction mentioned above.
3. A malpractice - in this context - will include, but not be limited to:
   - Submitting some other student's / team's solution(s) as one's own;
   - Copying some other student's / team's data or code or other forms of a solution;
   - Seeing some other student's / team's data or code or other forms of a solution;
   - Permitting some other student / team to see or copy or submit one's own solution;
   - or other equivalent forms of plagiarism wherein the student or team does not work out the solution and use some other solution or part thereof (such as downloading it from the LAN or the Web).
4. The degree of malpractice (the size of the solution involved or the number of students involved) will not be considered toward mitigating evidence. Failure on the part of instructor(s) to detect malpractice at or before the time of evaluation may not prevent sanctions based on later evidence.
5. In this context, a malpractice does NOT include the following:
   a. Asking help from a third person doubts, as long as there is no overt or covert intend/attempt to positively contribute towards the solution of Assignment/Project.
   b. Pointing out compilation errors. (As long as there is no active contribution to the semantics of the code.)

Either case, the fact that help was sought must be acknowledged while submitting the work

Date: 20/07/2016
Instructor-In-Charge
BITS F463