Course Outline: CSE-502: Cryptography
Department of Comp. Science and Engineering
East West University, Dhaka, Bangladesh

Instructor: Md. Shamsujjoha
M.S. and B.Sc.in Computer Science and Engineering, University of Dhaka,
Dhaka-1000 Bangladesh
Senior Lecturer, Department of Computer Science and Engineering, &
Assistant Proctor, East West University

Office: Room: 646, Phone: +8809666775577, Ext. 107
Email: msj@ewubd.edu, dishacse@yahoo.com, shamsujjoha.cse@gmail.com
Personal Web: http://www.ewubd.edu/~msj

Course Files: http://groups.yahoo.com/group/cse_msj/files

❖ CSE-502

Class Routine and Office Hour

Day	11:50-01:20	01:30-03:00	03:10-04:40	04:50-06:20
Sunday	CSE 245 (4) Room: 217	Office Hour Room: 646	CSE 245 (2) Room: 110	CSE 245 (3) Room: 637
Monday	CSE 245 (3) Room: 212	Office Hour Room: 646	CSE 245 (1) Room: AB2 (302)	CSE 245 (2) Room: 637
Tuesday	CSE 245 (4) Room: 533	Office Hour Room: 646	Office Hour Room: 646	CSE 245 (1) Room: 637
Wednesday	CSE 245 (3) Room: 212	Office Hour Room: A.P.R	CSE 245 (1) Room: AB2 (302)	CSE 245 (4) Room: 637
Thursday	Office Hour Room: A.P.R	Office Hour Room: A.P.R	CSE 245 (2) Room: 110	Office Hour Room: A.P.R
Saturday	CSE 502 Room: 646			

Course Description: This course introduces basic concepts in cryptography and computer security and discusses both their theoretical foundations and practical applications. Various threats, attacks and countermeasures including cryptosystems, cryptographic protocols and secure systems/networks will be addressed. After completing this course the student should be able to:

1. Understand the fundamentals of Cryptography
2. Acquire knowledge on standard algorithms used to provide confidentiality, integrity and authenticity.
3. Understand the various key distribution and management schemes.
4. Understand how to deploy encryption techniques to secure data in transit across data networks
5. Design security applications in the field of Information technology

Syllabus: A rigorous introduction to the design of cryptosystem and to cryptanalysis. Topic include cryptanalysis of classical cryptosystems; theoretical analysis of one-way functions; DES and differential cryptanalysis, the RSA cryptosystem, ELGamal, elliptic, hyper-elliptic, and hidden monomial cryptosystems, attacks on signature schemes, identification schemes and authentication codes; secret sharing and zero knowledge.

Text Book:

- William Stallings: Cryptography and Network Security, Pearson 8th or later edition.

Reference Materials:

- Behrouz A. Forouzan: Data communications and networking, 5th or later edition
- J. Katz and Y. Lindell: Introduction to Modern Cryptography, 2nd or later edition
- .

Mark Distribution:

Participation in the course	5%
Assignments	10%
Case Study	10%
Quiz	10%
Presentation	15%
Term I Exam	15%
Term II Term Exam	15%
Final Exam	20%

*The above mark distribution can be change up to ±5% (for each field).

Exam Dates:

Exam Name	Both Sections
Mid Term 1	07.02.2018
Mid Term 2	07.03.2018
Final	11.04.2018

Special Instructions:

- All mobile phones MUST be turned to silent. There is zero tolerance for cheating at EWU. Students caught with cheat sheets in their possession, whether used or not used, &/or copying from cheat sheets, writing on the palm of hand, back of calculators, chairs or nearby walls, etc. would be treated as cheating in the exam hall. The only penalty for cheating is expulsion from EWU. **For plagiarism, the grade will be automatically become zero for that exam/assignment**. There will be **NO make-up examinations for Quiz Exam in any case**. Make up exam can only be considered for the midterms in case of emergency, you MUST either inform me or the department secretary within 24 hours of the exam time. Failure to do so will mean that you are trying to take UNFAIR advantage and you will be automatically disqualified.