

**Birla Institute of Technology & Science, Pilani**  
**Distance Learning Programmes Division**  
**Second Semester 2005-2006**

**Course Handout**

**Course No.** : SS ZG513

**Course Title** : Network Security

*Course Email Address: [sszg513@dlpd.bits-pilani.ac.in](mailto:sszg513@dlpd.bits-pilani.ac.in)*

**Course Description**

The primary goal of the course is to introduce the student to system and application design aspects of network security including cryptographic, systemic and computational security aspects of the network / internetwork systems.

**Scope and Objectives**

The course covers fundamental aspects of security in a modern networked environment with the focus on system design aspects and cryptography in the specific context of network / internetwork security. It also dwells into basics of cryptographic techniques, algorithms and protocols required to achieve these properties; computational issues in implementing cryptographic protocols and algorithms; and system/application design issues in building secure networked systems.

**Prescribed Text Book**

T1 Bruce Schneier: [Applied Cryptography](#), Wiley Student Edition, 2<sup>nd</sup> Edition, Singapore, 1996.

**Reference Books**

- R1 Alfred Menezes, Paul van Oorschot, and Scott Vanstone: **Handbook of Applied Cryptography**. CRC Press, NY.
- R2 William Stallings: **Cryptography and Network Security**. 4<sup>th</sup> Edition. Prentice-Hall, Englewood Cliffs, 2006.
- R3 C.Kauffman, R.Pearlman and M.Spenser: **Network Security**, Second Edition, Prentice Hall, Englewood Cliffs, 2002.
- R4 S.Bellovin and W.Chesvick: **Internet Security and Firewalls**, Second Edition, Addison-Wesley, Reading, 1998.

**Additional Reading Material**

A1 Rahul Banerjee: **Lecture Notes on Network Security**, Electronic Read-only edition to be available just before Mid-Sem Test at the URL: <http://discovery.bits-pilani.ac.in/rahu/NetSec/>  
Lecture slides shall be also made available from time to time at this course page.

### Plan of Self Study

Week No.	Topic(s)	Chapter Reference
1	Introduction & Foundation	T1:1, Lecture notes
2	Cryptography Theory and Related Mathematics	T1:11
3	Symmetric Key Encryption Mechanisms <DES>	T1:12, Lecture notes
4	Block Cipher Design Principles	T1: 13.8, 13.9, 14.3, 14.8 - 14.12, Lecture notes
5	One Way hash Functions & Modes of Operation	T1: 9.3, 9.6, 18.1, 18.4, 18.5 -18.7, 18.10 – 18.14
6	Introduction Public Key Encryption Schemes	T1: 19.1-19.3,19.8, Lecture notes
7	Key Management & Key Exchange Mechanisms	T1:7, 8, 22.1, 22.3, 22.5,22.7, Lecture notes
8	Case Study 1: <ul style="list-style-type: none"> <li>▪ Firewalls</li> <li>▪ Intrusion Detection Systems</li> <li>▪ Introduction to VPNs</li> </ul>	T1: 2, Lecture notes
<b>Syllabus for Mid-Semester Test (Closed Book): Topics in Week No. 1 to 8</b>		
9	Digital Signatures	T1: 20, Lecture notes
10	Intermediate Protocols	T1: 4.1- 4.8, 4.10, 4.13,4.14
11	Zero Knowledge Protocols	T1: 5
12	Case Study 2: <ul style="list-style-type: none"> <li>▪ Kerberos</li> <li>▪ Email Security</li> </ul>	T1: 24.5,24.10-24.12, Lecture notes
13	Theory of Random and Pseudo Random Numbers	T1: 16,17, Lecture Notes
14	Secret Sharing Mechanisms	T1: 23.1-2.3, 23.7, 23.11, 23.12, 23.14, 23.16, Lecture notes
15	Cryptographic Design & Usage of Algorithms	T1: 10, Lecture notes
16	Case Study 3: <ul style="list-style-type: none"> <li>▪ Secure Elections</li> <li>▪ Digital Cash</li> </ul>	T1: 6, Lecture notes
<b>Syllabus for Comprehensive Exam (Open Book): All topics given in Plan of Self Study</b>		

### Evaluation Scheme :

EC No	Component & Nature	Duration	Weightage	Date, Time	To be given & evaluated by
1.	Mid-Semester Test (Closed Book)	2 hrs	40%	04/02/2006 (FN) 10 AM – 12 Noon	Instructor
2.	Compre. Exam (Open Book)	3 hrs	60%	01/04/2006 (FN) 9 AM – 12 Noon	Instructor

### Note :

It shall be the responsibility of the individual student to be regular in maintaining the self study schedule as given in the course handout, attend the online/on demand lectures as per details that would be put up in the BITS DLP website <http://www.bits-pilani.ac.in/dlp-home/> or <http://202.54.26.115/bits/portal/dlpd/> and take the prescribed components of the evaluation such as mid semester test, comprehensive examination as per scheduled dates in the course handout. If the student is unable to appear for the regular test/examination due to genuine exigencies, the student must refer to the procedure for applying for make-up test/examination, which will be available through the **Important Information** link on the [BITS DLP website](#).