DSE-2C	BCS-E601A	INFORMATION SECURITY	L	C	CIA	ESE	Time for ESE
			4	4	30	70	3Hrs.
PREREQUISITES		:	NIL				
COURSE OBJECTIVES/ LEARNING OUTCOMES		:	Upon successful completion of this course, the student will be able to: • understand the basics of Information Security • know the legal, ethical and professional issues in Information Security • know the aspects of risk management • know the technological aspects of Information Security				
NOTE: The question paper shall consist of three sections (Sec.-A, Sec.-B and Sec.-C). **Sec.-A** shall contain 10 objective type questions of one mark each and student shall be required to attempt all questions. **Sec.-B** shall contain 10 short answer type questions of four marks each and student shall be required to attempt any five questions. **Sec.-C** shall contain 8 descriptive type questions of ten marks each and student shall be required to attempt any four questions. Questions shall be uniformly distributed from the entire syllabus. The previous year paper/model paper can be used as a guideline and the following syllabus should be strictly followed while setting the question paper.								

Overview of Security: Protection versus security; aspects of security–data integrity, data availability, privacy; security problems, user authentication, Orange Book. **10L**

Security Threats: Program threats, worms, viruses, Trojan horse, trap door, stack and buffer overflow; system threats- intruders; communication threats- tapping and piracy. **10L**

Cryptography: Substitution, transposition ciphers, symmetric-key algorithms-Data Encryption Standard, advanced encryption standards, public key encryption - RSA; Diffie-Hellman key exchange, ECC cryptography, Message Authentication- MAC, hash functions. **20L**

Digital signatures: Symmetric key signatures, public key signatures, message digests, public key infrastructures. **10L**

Security Mechanisms: Intrusion detection, auditing and logging, tripwire, system-call monitoring; **10L**

BOOKS RECOMMENDED :

1. W. Stallings, Cryptography and Network Security Principles and Practices, 4th Ed., Prentice-Hall of India, 2006.
2. C. Pfleeger and SL. Pfleeger, Security in Computing, 3rd Ed., Prentice-Hall of India, 2007.
3. D. Gollmann, Computer Security, John Wiley and Sons, NY, 2002.
4. J. Piwprzyk, T. Hardjono and J. Seberry, Fundamentals of Computer Security, Springer-Verlag Berlin, 2003.
5. J.M. Kizza, Computer Network Security, Springer, 2007.
6. M. Merkow and J. Breithaupt, Information Security: Principles and Practices, Pearson Education, 2006.