DARBHANGA COLLEGE OF ENGINEERING

DARBHANGA

COURSE FILE OF
INFORMATION SECURITY

(06 1805)

DEPARTMENT
OF
COMPUTER SCIENCE AND ENGINEERING

FACULTY NAME
MR. ZOHEB HASAN
(Assistant Professor)

Institute/College Name:	Darbhanga College of Engineering
Program Name:	B.Tech (CSE, 8th semester)
Course Code:	061805
Course Name:	Information security
Lecture/Tutorial(per week):	3
Course Credits:	3
Course Co-coordinator Name:	Mr. Zoheb Hasan

1. Scope and Objective of Course

The need for information security has been there since the invention of mainframe computers. Information security is one of the current key areas in which there is a demand for lot of security professionals in the government, IT industry and public sector organizations. The students taking up this course can become security professionals which includes chief information security officers, risk assessment specialists, security policy developers etc. There is also lot of research avenues in this area.

At the end of the course, students will be able to:

1. investigate, analyze and assess the security risks of organizational information
2. implement security mechanisms for software and applications
3. plan and implement corporate information security policies
4. perform security audits and maintain the security of information

2. Textbooks

1. Information Security Principles & Practices by Mark Stamp, Wiley

3. Reference Books

2. Introduction to Computer Security by Bishop and Venkatramanayya, Pearson Education.
3. Cryptography and Network Security : Principles and Practice by Stallings, PHI.

Other readings and relevant websites

S. No.	Link of journals, Magazines, websites and Research papers
1.	https://www.youtube.com/watch?v=Z6f9ckEElsU&list=PL8751DA481F0F0D17
2.	https://www.tutorialspoint.com/itil/information_security_management.htm
3.	https://www.youtube.com/watch?v=Q-HugPvA7GQ&list=PL71FE85723FD414D7
4.	https://www.youtube.com/watch?v=vv1ODDhXW8Q&list=PLQu4a1zcASnObusCkpT5j75uTcyohWSA_

Course plans

Lecture No.	Date of Lecture	Topics	Web Links for Videos Lecture	Text Books/Reference books/Reading Materials	Page No. of Text Books
1-5		**Introduction, CRYPTO BASICS** Classic Crypto, Simple Substitution Cipher,, Cryptanalysis of a simple substitution, Double Transposition Cipher, One-time Pad, Project VENONA, Codebook Cipher.	https://www.youtube.com/watch?v=otN3V0beVRo&list=PLe442drWDJIvrjZygaxbnDsvt5C7h60bI	(TB3) Cryptography and Network Security : Principles and Practice by Stallings, PHI.	28-86
6-10		**SYMMETRIC KEY CRYPTO** Stream Ciphers, A5/1, RC4, Block Ciphers, Fiestel Cipher, DES, Triple DES, AES.	https://www.youtube.com/watch?v=otN3V0beVRo&list=PLe442drWDJIvrjZygaxbnDsvt5C7h60bI	(TB3) Cryptography and Network Security : Principles and Practice by Stallings, PHI.	135-161
		Assignment-1			
11-16		**PUBLIC KEY CRYPTO** Knapsack, RSA, Diffie-Hellman, Uses for Public Key Crypto.	https://www.youtube.com/watch?v=Q-HugPvA7GQ&list=PL71FE85723FD414D7	(TB3) Cryptography and Network Security : Principles and Practice by Stallings, PHI.	268,238,290

17-26		**HASH FUNCTION** AUTHENTICATION: Authentication Methods, Keys versus Passwords, Biometrics, Two-Factor Authentication. AUTHORIZATION: Access Control Matrix, Multilevel Security Models, Firewalls, Intrusion Detection.	https://www.youtube.com/watch?v=vv1ODDhXW8Q&list=PLQu4a1zcASnObusCkpT5j75uTcyohWSA_	(TB3) Cryptography and Network Security : Principles and Practice by Stallings, PHI.	319-393 621-645
		Assignment-2			
27-32		**SOFTWARE FLAWS AND MALWARE** Software Flaws, Malware, Miscellaneous Software-Based Attacks.	https://www.youtube.com/watch?v=vv1ODDhXW8Q&list=PLQu4a1zcASnObusCkpT5j75uTcyohWSA_	(TB3) Cryptography and Network Security : Principles and Practice by Stallings, PHI.Stallings, PHI.	598-620
33-41		**OPERATING SYSTEM AND SECURITY** Operating System Security Functions, Trusted Operating System, Next Generation Secure Computing Base.	https://www.youtube.com/watch?v=Q-HugPvA7GQ&list=PL71FE85723FD414D7	(TB3) Cryptography and Network Security : Principles and Practice by Stallings, PHI.	
		Assignment-3			

Syllabus

Topics	No. of Lectures	Weightages
Introduction, CRYPTO BASICS : Classic Crypto, Simple Substitution Cipher,, Cryptanalysis of a simple substitution, Double Transposition Cipher, One-time Pad, Project VENONA, Codebook Cipher.	5	12%
SYMMETRIC KEY CRYPTO: Stream Ciphers, A5/1, RC4, Block Ciphers, Fiestel Cipher, DES, Triple DES, AES.	5	18%
PUBLIC KEY CRYPTO : Knapsack, RSA, Diffie-Hellman, Uses for Public Key Crypto	6	22%
HASH FUNCTION: **AUTHENTICATION:**Authentication Methods, Keys versus Passwords, Biometrics, and Two-FactorAuthentication. **AUTHORIZATION:**Access Control Matrix, Multilevel Security Models, Firewalls, Intrusion Detection.	10	28%
SOFTWARE FLAWS AND MALWARE: Software Flaws, Malware, Miscellaneous Software-Based Attacks.	6	8%
OPERATING SYSTEM AND SECURITY: Operating System Security Functions, Trusted Operating System, Next Generation Secure Computing Base.	9	12%

Evaluation and Examination Blue Prints:

Internal assessment is done through quiz tests, presentations, assignments and projects work. Two sets of question paper are asked from each faculty and out of these two, without the knowledge of faculty, one question paper is chose for the concerned examination. Examination rules and regulations are uploaded on the student's portals. Evaluation is a very transparent process and the answer sheets of sessional tests, internal assessment assignments are returned back to the students.

The components of evaluation along with their weightage followed by the university is given below:

Component-1	Sessional test-1	30%
	Sessional test-2	
	Sessional test-3	
Component-2	Assignments, Quiz's, Test, Seminars	10%
Component-3	End Term Examination	60%
Totals		100%

Designation	**Name**	**Signature**
Course Coordinator	Mr. Zoheb Hasan	
H.O.D	Dr._____	
Principal	Dr._____	
Date	…../…./…….	