Muzaffarpur Institute Of Technology, Muzaffarpur

COURSE FILE
OF
INFORMATION SECURITY
(CS 061x05)

FACULTY NAME:
SAVYASACHI
ASST. PROFESSOR,
DEPARTMENT OF INFORMATION TECHNOLOGY

Institute / College Name :	Muzaffarpur Institute Of Technology, Muzaffarpur		
Program Name	**B.TECH IT**		
Course Code	IT 061x05		
Course Name	Information Security		
Lecture / Tutorial (per week):	3/0	**Course Credits**	3
Course Coordinator Name	Asst. Prof. Savyasachi		

1. **Scope and Objectives of the Course:**

The Objective is to achieve 'CIA'.

The main goal of this course is to provide you with a background, foundation, and insight into the many dimensions of information security. This knowledge will serve as basis for further deeper study into selected areas of the field, or as an important component in your further studies and involvement in computing as a whole. The primary objectives of the course are to help you:

• Understand information security's importance in our increasingly computer-driven world.

• Master the key concepts of information security and how they "work."

• Develop a "security mindset:" learn how to critically analyze situations of computer and network usage from a security perspective, identifying the salient issues, viewpoints, and trade-offs.

As a part of your general education, the course will also help you learn to:

• Clearly and coherently communicate (both verbally and in writing) about complex technical topics

.• Work and interact collaboratively in groups to examine, understand and explain key aspects of information security

.

2. **Textbooks**

- **TB1:** Information Security Principles & Practices by Mark Stamp, Wiley.

3. **Reference Books**

- **RB1:** Introduction to Computer Security by Bishop and Venkatramanayya, PearsonEducation.
- **RB2:** 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.	Meisong Wang, Charith Perera, Prem Prakash Jayaraman, Miranda Zhang, Peter Strazdins, R.K. Shyamasundar, Rajiv Ranjan, "Sensor Data Fusion in the Internet of Things, International Journal of Distributed Systems and Technologies, "International Journal of Distributed Systems and Technologies,Vol.7 1:, 2016, pp.15-22
2.	S. Bidkar, Ashwin Gumaste, P. Ghodasara, A. Kushwaha, J. Wang and A. Somani Scalable Segment Routing – A New Paradigm for Efficient Service Provider Networking using Carrier Ethernet Advances IEEE/OSA Journal of Optical Communication and Networking 7-5- 2015 445 460 A May 2015 DOI: 10.1364/JOCN.7.000445
3.	A. Mathew, P. Gokhale, T. Das and Ashwin Gumaste Application of Robust Optimization to Multi-layer High-Speed Network Design and Mobile Backhaul IEEE/OSA Journal of Optical Communication and Networking 7-4- 2015 352 - 367 367 A April 2015 DOI: 10.1364/JOCN.7.000352
4.	http://ieeexplore.ieee.org/servlet/opac?punumber=4149673
5.	Information Security and Cryptology (ISCISC), 2013 10th International ISC Conference on

6. Course Plan

Lecture Number	**Date of Lecture**	**Topics**	**Web Links for video lectures**	**Text Book / Reference Book / Other reading material**
1-10		**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=vv1ODDhXW8Q&list=PLa4KQhDlGd7SfkyvjepMFNbnBSRDYDqzd	PPTs (will provide study material to each and every student)
11-16		**SYMMETRIC KEY CRYPTO**		
		Stream Ciphers, A5/1, RC4, Block Ciphers, Fiestel Cipher, DES, Triple DES, AES.	https://www.youtube.com/watch?v=QbczPuEphUY	PPTs (will provide study material to each and every student)
17-22		**PUBLIC KEY CRYPTO**		TB1, RB1
		Knapsack, RSA, Diffie-Hellman, Uses for Public Key Crypto.	https://www.youtube.com/watch?v=TCwciYgO6zI	
23-32		**HASH FUNCTION AUTHENTICATION**		TB1, RB1,RB2
		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=9XZ45SAnJnk	
33-38		**SOFTWARE FLAWS AND MALWARE**		TB1, RB1
		Software Flaws, Malware, Miscellaneous Software-Based Attacks.	https://www.youtube.com/watch?v=l0ODBZkNpGI	
39-42		**OPERATING SYSTEM AND SECURITY**		TB1, RB1,RB2
		Operating System Security Functions, Trusted Operating System, Next Generation Secure Computing Base.	https://www.youtube.com/watch?v=gr29JiWlTH8	

1. **Evaluation Scheme:**

Component 1	Mid Semester Exam	20
Component 2	Assignment Evaluation	10
Component 3**	End Term Examination**	70

	Total	**100**

****** The End Term Comprehensive examination will be held at the end of semester. The mandatory requirement of 75% attendance in all theory classes is to be met for being eligible to appear in this component.

SYLLABUS

Topics	No of lectures	Weight age
Introduction CRYPTO BASICS : Classic Crypto, Simple Substitution Cipher,, Cryptanalysis of a simple substitution, Double Transposition Cipher, One-time Pad, Project VENONA, Codebook Cipher.	10	24
SYMMETRIC KEY CRYPTO: Stream Ciphers, A5/1, RC4, Block Ciphers, Fiestel Cipher, DES, Triple DES, AES.	6	15
PUBLIC KEY CRYPTO : Knapsack, RSA, Diffie-Hellman, Uses for Public Key Crypto.	6	15
HASH FUNCTION AUTHENTICATION: Authentication Methods, Keys versus Passwords, Biometrics, Two-Factor Authentication. **AUTHORIZATION :**Access Control Matrix, Multilevel Security Models, Firewalls, Intrusion Detection.	10	25
SOFTWARE FLAWS AND MALWARE: Software Flaws, Malware, Miscellaneous Software-Based Attacks.	6	15
OPERATING SYSTEM AND SECURITY: Operating System Security Functions Trusted Operating System, Next Generation Secure Computing Base.	4	6

This Document is approved by:

Designation	**Name**	**Signature**
Course Coordinator	Savyasachi	
H.O.D	Mr. Vijay Kumar	
Principal	Dr. J.N Jha	
Date	02-08-2018	

Evaluation and Examination Blue Print:

Internal assessment is done through quiz tests, presentations, assignments and project work. Two sets of question papers are asked from each faculty and out of these two, without the knowledge of faculty, one question paper is chosen for the concerned examination. Examination rules and regulations are uploaded on the student's portal. 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 evaluations alongwith their weightage followed by the University is given below

Sessional Test 1	10%
Sessional Test 2	10%
Sessional Test 3	10%
Assignments/Quiz Tests/Seminars	10%
End term examination	70%

(From amongst the three sessional tests best of two are considered)

Assignment I

1) **Explain Public Key Cryptography in Brief. Also Explain RSA algorithm with an example.**
2) **Explain Hill- Cipher and Play-Fair cipher with an example.**

3) **Hash Functions. In this problem we consider hash functions on a finite domain (from {0, 1} n(k) to {0, 1} m(k)).**

  a) **Preimage collision resistance != Second-preimage collision resistance. Suppose H is preimage collision resistant. Modify H to H0 (possibly with a different domain), so that the latter remains preimage collision resistant, but is not second-preimage collision resistant. (Prove these properties of H0 .)**

  b) **Second-preimage collision resistance != Preimage collision resistance. Given a CRHF H which compresses by two bits (say from n bits to n−2 bits), construct a CRHF H0 that compresses by one bit (say from n + 1 bits to n bits), such that the function f(h 0 , x) = (h 0 , h0 (x)) (where h 0 ∈ H0) is not a OWF. (In both H and H0 , collision-resistance holds when the hash function is drawn uniformly at random from the family.)**

4) **Discuss Cryptography in detail with diagram.**

Assignment II

1. **Explain Firewall in detail.**
2. **Explain IDS in detail. Also Discuss some tools of IDS.**
3. **Explain DES in Brief.**
4. **Discuss Project Venona.**

MUZAFFARPUR INSTITUTE OF TECHNOLOGY, MUZAFFARPUR

Name: Asst. Prof. SAVYASACHI

Day	I	II	III	IV		IV	V	VI
	9:00 - 10:00	10:00 – 11:00	11:00 – 12:00	12:00-01:00	1:00–2:00	02:00-03:00	03:30 – 04:00	04:00 – 05:00
Monday	IS(ME) 5th		MIS(IT) 7th		LUNCH BREAK	Test ME(IS) Test IT(MIS)		Test EE(IS)
Tuesday	IS(ME) 5th					OOP LAB (EE) 3rd		
Wednesday				IS(EE) 5th				
Thursday		MIS(IT) 7th		IS(ME) 5th		OOP LAB (EE) 3rd		
Friday	IS(EE) 5th					System Programming lab(IT) 5th		
Saturday	IS(EE) 5th			MIS(IT) 7th				

Information Security (CA35120)

CO 1. Learn the concept of Information Security.Determine which type of Biometrics Security are popular and widely used.

CO 2. Understand the model of cryptography.Learn about the policies of network security.

CO 3. Understand Cyber Law and Ethics.

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	Y			Y			Y			Y	Y	
CO2							Y					Y
CO3				Y		Y	Y		Y			