Institute / College Name :	Bakhtiyarpur College of Engineering, Bakhtiyarpur		
Program Name	**B.TECH (CSE)**		
Academic Year	**2020-21**		
Course Code	**051718**		
Course Name	**Cryptography**		
Semester	**7th**		
Lecture / Tutorial (per week):	**3/0**	**Course Credits**	**3**
Course Coordinator Name	Asst. Prof. Bhawana Singh		

Course Description

- In today's cyber world, it is important for engineers to understand and appreciate computer/information security as it has become an essential aspect of our day life.
- This course provides students with concepts of computer security, cryptography, digital money, secure protocols, intrusion detection and other security techniques.
- This course develops a workable knowledge of mathematics used in cryptology.
- The course emphasizes to give a basic understanding of previous attacks on cryptosystem with the aim of preventing future attacks.
- The cryptanalysis part will help in understanding the challenges for cybersecurity.
- Upon the completion of this course, students should be able to explain, appreciate, employ, design and implement appropriate security technologies and policies to protect computers and digital information.

Course Objectives

- To explain the areas of Cryptography and Cryptanalysis.
- To implement different cryptographic techniques for securing a message over insecure channel.
- To select methods about how to maintain the Confidentiality, Integrity and Availability of a data.
- To interpret various protocols for network security against the threats in the networks.

Course Outcomes

After successful completion of the course, the learners would be able to

- support security of the data and system over the network using various cryptographic techniques.
- Implement various networking protocols.
- Conclude authentication protocols required for threat free message over the network.
- Explore in the emerging areas of cryptography and network security.

051718 CRYPTOGRAPHY

L–T–P : 3–0–0 **Credit : 3**

1. Introduction : The OSI Security Architecture, Security attack, Security Services, Security Mechanism, A model for Network Security. **Lecture : 4**

2. Symmetric Cipher : Classical Encryption Techniques, Symmetric Cipher Model, Block Cipher Principles, DES, Cryptanalysis, Block Cipher Design Principle, The Euclidean Algorithm, Finite field of Form GP(p), Advance Encryption Standard (AES), AES Cipher, Multiple Encryption and Triple DES, Stream, Placement of Encryption Function, Traffic Confidentiality, Key Distribution, Random number generation.

Lecture : 15

3. Public Key Encryption and Hash Function : Fermat's & Euler's Theorems, The Chinese Remainder Theorem, RSA Algorithm, Diffie-Hellman Key Exchange, Elliptic Curve Cryptography, Message authentication code, Security of Hash Functions and MAACs, Secure Hash algorithm, Whirlpool, HMAC, CMAC, Digital Signature.

Lecture : 12

4. Network Security Applications : Kerberos, X.509 Authentication Service, S/MIME, IP Security Architecture, Encapsulating Security Payload, Secure Socket Layer (SSL), Transport layer security, Secure Electronic Transaction.

Lecture : 6

5. System Security: Intrusion detection, Password Management, Virus countermeasure, Denial of Service Attack, Firewall design principles, Trusted System.

Lecture : 6

Text Book : System Security

1. Cryptography and Network Security : Principle and Practice, 4e by William Stalling, Pearson Education/PHI.

Reference Books :

1. Beginning Cryptography with Java by David Hook, Wiley Dreamtech.
2. Modern Cryptography Theory & Practices by Wenbo Mao, Pearson Education.
3. Cryptography for Database and Internet Application by Nick Galbreath, Wiley Dreamtech.
4. Network Security : Private Communication in a Public World, 2e, by Charlie Kaufman, Radia Perlman and Mike Speciner, Pearson Education..

Bakhtiyarpur College of Engineering, Bakhtiyarpur

Branch - CSE 7th Sem **Effective From:- 01.08.2020**

Days	Branch	1st Period	2nd Period	3rd Period	4th Period	1:20-2:10	5th Period	6th Period	7th Period
		10:00-10:50	10:50-11:40	11:40-12:30	12:30-1:20		2:10-03:00	03:00-3:50	3:50-04:40
Mon	CSE		PROJECT			RECESS	AI	DC	ELECTIVE I
Tue	CSE		DC LAB				ELECTIVE I	AI	DC
Wed	CSE	CISCO TRAINING					ELECTIVE III	ELECTIVE I	ELECTIVE II
Thu	CSE		AI LAB				ELECTIVE II	ELECTIVE III	AI
Fri	CSE		PROJECT				DC	ELECTIVE II	ELECTIVE III
Sat	CSE	SPOKEN TUTORIAL					WEEKLY MEETING		

Sl. No.	Sub. Code	Subject Name	Faculty Name
1	AI	Artificial Intelligence	Prof. Shahab Saquib
2	DC	Distributed Computing	Prof. Ajeet Kumar
3	ELECTIVE I	Fundamental of Data Communication	Prof. Rajeev Ranjan
4	ELECTIVE II	Cryptography	Prof. Bhawana Singh
5	ELECTIVE III	Computer Graphics	Prof. Sashi Raj
6	PROJECT	Project I	Prof. Sashi Raj

COURSE PLAN	
Semester	7th
Course Code	051718
Course Credit	3
Course Name	Cryptography
Branches	Computer Science and Engineering
Course Coordinator	***Bhawana Singh***
Date	28.07.2020

Part-A		Lecture Plan	
Sl. No.		Topic Name	Periods
1		**Introduction**	
	1.1	The OSI Security Architecture, Security attack	1
	1.2	Security Services, Security Mechanism	2
	1.3	A model for Network Security	1
Assignment 1			
2		**Symmetric Cipher**	
	2.1	Classical Encryption Techniques	1
	2.2	Symmetric Cipher Model, Block Cipher Principles	2
	2.3	DES, Cryptanalysis	2
	2.4	Block Cipher Design Principles	1
	2.5	The Euclidean Algorithm	1
	2.6	Finite field of Form GP(p)	1
	2.7	Advance Encryption Standard (AES), AES Cipher	1
	2.8	Multiple Encryption and Triple DES	1
	2.9	Stream, Placement of Encryption Function	2
	2.10	Traffic confidentiality	1
	2.11	Key distribution	1
	2.12	Random number generation	1
Assignment 2			
3		**Public Key Encryption and Hash Function**	
	3.1	Fermat’s & Euler’s Theorems	1
	3.2	The Chinese Remainder Theorem	1
	3.3	RSA Algorithm	1
	3.4	Diffie-Hellman Key Exchange	1
	3.5	Elliptic Curve Cryptography	1
	3.6	Message authentication code	1
	3.7	Security of Hash Functions and MAACs	1
	3.8	Secure Hash algorithm	1

	3.9	Whirlpool	**1**
	3.10	HMAC	**1**
	3.11	HMAC	**1**
	3.12	Digital Signature	**1**
Assignment 3			
4		**Network Security Applications**	
	4.1	Kerberos, X.509 Authentication Service	**2**
	4.2	S/MIME, IP Security Architecture	**2**
	4.3	Encapsulating Security Payload, Secure Socket Layer (SSL)	**1**
	4.4	Transport layer security, Secure Electronic Transaction	**1**
Assignment 4			
5		**System Security**	
	5.1	Intrusion detection, Password Management	**2**
	5.2	Virus countermeasure, Denial of Service Attack	**2**
	5.3	Firewall design principles	**1**
	5.4	Trusted System	**1**
Assignment 5			
TOTAL			**43**

PART B	**Assignment Numbers**	**Module**
1	Assignment 1	1
2	Assignment 2	2
3	Assignment 3	3
4	Assignment 4	4
5	Assignment 5	5

. Web Link for video lectures

Module	**Web Link for video lectures**
Module 1	https://nptel.ac.in/courses/106/105/106105162/#
Module 2	
Module 3	
Module 4	
Module 5	

Other reading and relevant websites

S.No.	Link of Journals, Magazines, websites and Research Papers
1.	Crypto Glossary and Dictionary of Technical Cryptography
2.	A Course in Cryptography by Raphael Pass & Abhi Shelat – offered at Cornell in the form of lecture notes.
3.	Overview and Applications of Cryptology by the CrypTool Team; PDF; 3.8 MB. July 2008
4.	http://ieeexplore.ieee.org/servlet/opac?punumber=4149673
5.	Information Security and Cryptology (ISCISC), 2013 10th International ISC Conference on
6.	A multi-classifier network-based **crypto** ransomware detection system: a case study of Locky ransomware AO Almashhadani, M Kaiiali, S Sezer, P O'Kane - **Ieee** Access, **2019** - ieeexplore.**ieee**.org
7.	Combination of steganography and **cryptography**: A short survey MS Taha, MSM Rahim, SA Lafta… - IOP conference …, **2019** - iopscience.iop.org
8.	A **survey** on various **cryptography** techniques VK Mitali, A Sharma - International Journal of Emerging Trends & …, 2014 - academia.edu

Evaluation Scheme:

Component 1	Mid Semester Exam	20
Component 2	Assignment Evaluation	5
Component 3	Attendance	5
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.

This Document is approved by:

Designation	**Name**	**Signature**
Course Coordinator	Bhawana Singh	
H.O.D	Mr. Shahab Saquib	
Principal	Dr. Kumar Surendra	
Date	28.07.2020	

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 along with their weightage followed by the University is given below

Mid Term exam	20%
Assignments/Quiz Tests/Seminars	5%
Attendance	5%
End term examination	70%