Academic Course Description

BHARATH UNIVERSITY
Faculty of Engineering and Technology
Department of Electronics and Communication Engineering

BEC012 Cryptography and Network Security

Sixth Semester, 2015-16 (Even Semester)

Course (catalog) description

To impart knowledge on Encryption techniques ,Key Management which include Elliptic Curve Architecture, introduces the Authentication requirements ,Authentication functions , Authentication code
Authentication Applications and prominence given to cover the importance of the Network Security,
System Level Security.

Compulsory/Elective course : Compulsory for ECE students

Credit hours : 3 credits

Course Coordinator : Ms. RAJI PANDURANGAN Asst. Professor

Instructors :

Name of the instructor	Class handling	Office location	Office phone	Email (domain:@ bharathuniv.ac.in	Consultation
Ms.RAJI PANDURANGAN	Third year ECE	SA003		Raji.ece@bharathuniv.ac.in	12.30-1.30PM
Ms. S.Arul Selvi	Third year ECE	SA003		arulselvi.ece@bharathuniv.ac.in	12.30-1.30PM

Relationship to other courses:

Pre –requisites : BEC604 Communication Engineering – II,
BEC601Computer Communication and Networks

Assumed knowledge : The students will have a mathematics background obtained at a high school (or equivalent) level. In particular, working knowledge of basic mathematics including factorization, Euclidean Algorithm technique, Modular Arithmetic's are assumed.

Following courses : BEC002 Integrated Service Digital Network,
BEC007 Digital Image Processing,
BCS 701 Grid and Cloud Computing,
BET008 Wireless Networks

Syllabus Contents

UNIT I INTRODUCTION **9 HOURS**

OSI Security Architecture - Classical Encryption techniques – Cipher Principles – Data Encryption Standard – Block Cipher Design Principles and Modes of Operation - Evaluation criteria for AES – AES Cipher – Triple DES – Placement of Encryption Function – Traffic Confidentiality

UNIT II PUBLIC KEY CRYPTOGRAPHY **9 HOURS**

Key Management - Diffie-Hellman key Exchange – Elliptic Curve Architecture and Cryptography - Introduction to Number Theory – Confidentiality using Symmetric Encryption – Public Key Cryptography and RSA.

UNIT III AUTHENTICATION AND HASH FUNCTION **9 HOURS**

Authentication requirements – Authentication functions – Message Authentication Codes – Hash Functions – Security of Hash Functions and MACs – MD5 message Digest algorithm - Secure Hash Algorithm – RIPEMD – HMAC Digital Signatures – Authentication Protocols – Digital Signature Standard.

UNIT IV NETWORK SECURITY **9 HOURS**

Authentication Applications: Kerberos – X.509 Authentication Service – Electronic Mail Security – PGP – S/MIME – IP Security – Web Security.

UNIT V SYSTEM LEVEL SECURITY **9 HOURS**

Intrusion detection – password management – Viruses and related Threats – Virus Counter measures – Firewall Design Principles – Trusted Systems.

TOTAL 45 HOURS

Text book(s) and/or required materials

T1. William Stallings, Cryptography and Network Security, 6th Edition, Pearson Education, March 2013.

T2. Charlie Kaufman, Radia Perlman and Mike Speciner, "Network Security", Prentice Hall of India,2002.

Refrence Books:

R1 Behrouz A. Ferouzan, "Cryptography & Network Security", Tata Mc Graw Hill, 2007.

R2 Charles Pfleeger, "Security in Computing", 4th Edition, Prentice Hall of India, 2006.

R3 Ulysess Black, "Internet Security Protocols", Pearson Education Asia, 2000.

R4 Charlie Kaufman and Radia Perlman, Mike Speciner, "Network Security, Second Edition, Private Communication in Public World", PHI 2002.

R5 Bruce Schneier and Neils Ferguson, "Practical Cryptography", First Edition, Wiley Dream tech India Pvt Ltd, 2003.

R6 www.ics.uci.edu/~stasio/spring04/ics180.html

Computer usage: Nil

Professional component

General	-	0%
Basic Sciences	-	0%
Engineering sciences & Technical arts	-	40%
Professional subject	-	60%

Broad area: Cryptography and Network Security | Digital Image Processing |Cloud Computing |Wireless Networks | Computer Networks |

Test Schedule

S. No.	Test	Tentative Date	Portions	Duration
1	Cycle Test-1	February 2nd week	Session 1 to 14	2 Periods
2	Cycle Test-2	March 2nd week	Session 15 to 28	2 Periods
3	Model Test	April 3rd week	Session 1 to 45	3 Hrs
4	University Examination	TBA	All sessions / Units	3 Hrs.

Mapping of Instructional Objectives with Program Outcome

To learn various encryption techniques, understand the concept of Public key cryptography, study about message authentication and hash functions and to impart knowledge on Network security . This course emphasizes:	Correlates to program outcome		
	H	**M**	**L**
1. Classify the symmetric encryption techniques.	a,h	c,e,f,g,i	k
2. Illustrate various Public key cryptographic techniques.	c,g,j	a	B,i
3. Evaluate the authentication and hash algorithms.	b,k	a,c,d,g,h,i	-
4. Discuss authentication applications	b,c	a,e,i,k	-
5. Summarize the intrusion detection and its solutions to overcome the attacks.	_	b,e,f,g,i	-
6. Basic concepts of system level security	f	d,e,g	-

H: high correlation, M: medium correlation, L: low correlation

Draft Lecture Schedule

Session	Topics	Problem solving (Yes/No)	Text / Chapter
UNIT I	**INTRODUCTION**		
1.	OSI architecture	No	[T1] Chapter -1,2,3,5 [R1]Chapter-6,7
2.	Symmetric ciphers	Yes	
3.	Block cipher design	No	
4.	Modes of operation	No	
5.	Evaluation criteria AES	No	
6.	AES cipher	No	
7.	Triple DES	No	
8.	Placement of encryption	Yes	
9.	Traffic confidentiality	No	
UNIT II	**PUBLIC KEY CRYPTOGRAPHY**		
10.	Key management	No	[T1] Chapter -8,9,10 [T2]Chapter 7 [R1]Chapter-8,9
11.	Diffie Helman	Yes	
12.	Elliptic Curve	Yes	
13.	Elliptic curve	Yes	
14.	Number theory	Yes	
15.	Confidentiality –symmetric	Yes	
16.	Public key cryptography	Yes	
17.	RSA	No	
18.	RSA problems	Yes	
UNIT III	**AUTHENTICATION AND HASH FUNCTION**		
19.	Authentication	No	[T1] Chapter - 11,12,13, [T2]Chapter 2,3,5 [R1]Chapter-11,12,13
20.	Authentication requirement	No	
21.	Authentication functions	No	
22.	Message Authentication	No	
23.	Hash function	Yes	
24.	Security of Hash Function, Secure hash Algorithm	Yes	
25.	MAC, MD5 Algorithm	No	
26.	HMAC Digital Signature	No	

27.	Authentication Protocol	No	
	UNIT IV NETWORK SECURITY		
28.	Authentication application	No	[T1] Chapter - 14,15,16,17, [T2]Chapter 13,14
29.	Kerberos	No	
30.	X.509 authentication services	No	
31.	Electronic mail security	No	
32.	PGP	No	
33.	S/MIME	No	
34.	IP security	No	
35.	Web security	No	
36.	Internet security	No	
	UNIT V SYSTEM LEVEL SECURITY		
37.	Intrusion detection	No	[T1] Chapter -18,19,20
38.	Viruses	No	
39.	Viruses and related treats	No	
40.	Virus counter measures	No	
41.	Virus counter measures	No	
42.	Fire wall design	No	
43.	Fire wall design	No	
44.	Fire wall principle	No	
45.	Trusted system	No	

Teaching Strategies

The teaching in this course aims at establishing a good fundamental understanding of the areas covered using:

- Formal face-to-face lectures
- Tutorials, which allow for exercises in problem solving and allow time for students to resolve problems in understanding of lecture material.
- Laboratory sessions, which support the formal lecture material and also provide the student with practical construction, measurement and debugging skills.
- Small periodic quizzes, to enable you to assess your understanding of the concepts.

Evaluation Strategies

Cycle Test – I	-	10%
Cycle Test – II	-	10%
Model Test	-	25%
Attendance	-	5%
Final exam	-	50%

Prepared by: Raji Pandurangan Assistant professor , Department of ECE **Dated : 5 -11-2016**

Addendum

ABET Outcomes expected of graduates of B.Tech / ECE / program by the time that they graduate:

(a) an ability to apply knowledge of mathematics, science, and engineering fundamentals.
(b) an ability to identify, formulate, and solve engineering problems
(c) an ability to design a system, component, or process to meet desired needs within realistic constraints such as economic, environmental, social, political, ethical, health and safety, manufacturability, and sustainability
(d) an ability to design and conduct experiments, as well as to analyze and interpret data
(e) an ability to use the techniques, skills, and modern engineering tools necessary for engineering practice
(f) an ability to apply reasoning informed by a knowledge of contemporary issues
(g) an ability to broaden the education necessary to understand the impact of engineering solutions in a global, economic, environmental, and societal context
(h) an ability in understanding of professional and ethical responsibility and apply them in engineering practices
(i) an ability to function on multidisciplinary teams
(j) an ability to communicate effectively with the engineering community and with society at large
(k) an ability in understanding of the engineering and management principles and apply them in Project and finance management as a leader and a member in a team.

Program Educational Objectives

PEO1: To provide strong foundation in mathematical, scientific and engineering fundamentals necessary to analyze, formulate and solve engineering problems in the field of Electronics And Communication Engineering.

PEO2: To enhance the skills and experience in defining problems in Electronics And Communication Engineering design and implement, analyzing the experimental evaluations, and finally making appropriate decisions.

PEO3: To enhance their skills and embrace new Electronics And Communication Engineering Technologies through self-directed professional development and post-graduate training or education.

PEO4: To provide training for developing soft skills such as proficiency in many languages, technical communication, verbal, logical, analytical, comprehension, team building, inter personal relationship, group discussion and leadership skill to become a better professional.

PEO5: Apply the ethical and social aspects of modern communication technologies to the design, development, and usage of electronics engineering.

Course Teacher	Signature
Ms. RAJI PANDURANGAN	
MS.S.ARUL SELVI	

Course Coordinator	Academic Coordinator	Professor In-Charge	HOD/ECE
(Ms.Raji Pandurangan)	( )	(Dr.)	(Dr.M.Sundararajan)