FR. Conceicao Rodrigues College Of Engineering

Father Agnel Ashram, Bandstand, Bandra-west, Mumbai-50

Department of Computer Engineering

Course Name : Cryptography and System Security

Teaching Scheme : Lectures- 4 Hrs/Week

Examination Scheme :

Tests : - 20 Marks

End Sem Exam – 80 Marks

Academic Year : 2019-20

Class: T.E. (Computer) (semester VI)

Faculty : Sunil Chaudhari

PAC Members: **HOD :**

Course Outcomes & Assessment Plan

Subject: Cryptography and System Security (CSC604) **Credits-4**

Syllabus:

Module No	Unit No	Detailed Content
1	**Introduction & Number Theory**	
	1.1	Security Goals, Services, Mechanisms and attacks, The OSI security architecture, Network security model, Classical Encryption techniques, Symmetric cipher model, mono-alphabetic and poly-alphabetic substitution techniques: Vigenere cipher, playfair cipher, Hill cipher, transposition techniques: keyed and keyless transposition ciphers, steganography.

	1.2	Modular Arithmetic and Number Theory:- Euclid‘s algorithm-–Prime numbers-Fermat‘s and Euler‘s theorem- Testing for primality -The Chinese remainder theorem, Discrete logarithms.
2		**Symmetric and Asymmetric key Cryptography and key Management**
	2.1	Block cipher principles, block cipher modes of operation, DES, Double DES, Triple DES, Advanced Encryption Standard (AES), Stream Ciphers: RC5 algorithm.
	2.2	Public key cryptography: Principles of public key cryptosystems-The RSA algorithm, The knapsack algorithm, ElGamal Algorithm.
	2.3	Key management techniques: using symmetric and asymmetric algorithms and trusted third party. Diffie Hellman Key exchange algorithm.
3		**Hashes, Message Digests and Digital Certificates**
	3.1	Cryptographic hash functions, Properties of secure hash function, MD5, SHA-1, MAC, HMAC, CMAC.
	3.2	Digital Certificate: X.509, PKI
4		**Authentication Protocols & Digital signature schemes**
	4.1	User Authentication and Entity Authentication, One-way and mutual authentication schemes, Needham Schroeder Authentication protocol, Kerberos Authentication protocol.
	4.2	Digital Signature Schemes – RSA, EIGamal and Schnorr signature schemes.
		Network Security and Applications
5	**5.1**	Network security basics: TCP/IP vulnerabilities (Layer wise), Packet Sniffing, ARP spoofing, port scanning, IP spoofing, TCP syn flood, DNS Spoofing.
	5.2	Denial of Service: Classic DOS attacks, Source Address spoofing, ICMP flood, SYN flood, UDP flood, Distributed Denial of Service, Defenses against Denial of Service Attacks.
	5.3	Internet Security Protocols: SSL, IPSEC, Secure Email: PGP, Firewalls, IDS and types, Honey pots 5.3
6		**System Security**
	6.1	Software Vulnerabilities: Buffer Overflow, Format string, cross-site

		scripting, SQL injection, Malware: Viruses, Worms, Trojans, Logic Bomb, Bots, Rootkits. 6.1

1. **Course Outcomes:**

Upon completion of this course students will be able to:

Sr. No.	*Course Outcome Statement*
CSC604.1	Illustrate different cryptosystems from an application viewpoint. **(Analysis)**
CSC604.2	Analyze and evaluate the authentication and hashing algorithms. **(Analysis**)
CSC604.3	Identify different attacks on networks and analyze the performance of security protocols. **(B3-Apply)**

Mapping of CO and PO/PSO

Program Outcomes (POs)

Engineering Graduates will be able to

1. **Engineering knowledge:** Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems.
2. **Problem analysis:** Identify, formulate, review research literature, and analyze complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.
3. **Design/Development of solutions:** Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for public health and safety, and the cultural, societal, and environmental considerations.
4. **Conduct investigations of complex problems:** Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.
5. **Modern tool usage:** Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modeling of complex engineering activities with an understanding of the limitations.
6. **The engineer and society:** Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering practice.
7. **Environment and sustainability:** Understand the impact of the professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and the need for sustainable development.
8. **Ethics:** Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice.
9. **Individual and team work:** Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.

10. **Communication:** Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.
11. **Project Management and finance:** Demonstrate knowledge and understanding of the engineering and management principles and apply these to one's work, as a member and leader in a team, to manage projects and in multidisciplinary environments.
12. **Life-long learning:** Recognized the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.

(A) Program Specific Outcomes (PSOs)

Student will have ability to

1. Apply fundamental computer science knowledge to solve real world problems.
2. Design and implement software systems of varying complexity in multidisciplinary scenarios that meet specified requirements with appropriate consideration to architectural, algorithmic and security aspects.

Relationship of course outcomes with program outcomes: Indicate 1 (low importance), 2 (Moderate Importance) or 3 (High Importance) in respective mapping cell.

	PO1 (Engg Know)	PO2 (Ana)	PO3 (De sign)	PO4 (inve stiga)	PO5 (tools)	PO6 (engg Soci)	PO7 (Env)	PO8 (Eth)	PO9 (ind Team)	PO10 (comm.)	PO11 (PM)	PO12 (life Long)
CSC604.1	3	1	2									
CSC604.2	3	2			2							
CSC604.3	3	2			3	2						3
Total	9	5	2		5	2						3
Course To PO	3	2.5	2		1	2						3

CO	PSO1	PSO2
CSC604.1	3	2
CSC604.2	3	2
CSC604.3	3	2
Total	9	6
Course to PSO	3	2

CO Assessment Tools:

CSC604.1: **Direct Methods(80%):** Test 1 + Quiz +UniExamTh+ UniExamOral+ Labs

CO1dm = 0.2T1+.15A+0.15Q+0.15UTh+0.15UOr+0.2Lab

InDirect Methods(20%): Course exit survey

CO1idm

CSC302.1 = 0.8*CO1dm + 0.2* CO1idm

Direct Method	Weightage	Target	Marks
Test1	0.2	65% of students will minimum score 60% marks	20
Assignment	0.15	70% of students will minimum score 70% marks	
Quiz 1,2,3,4(NPTEL Course on Cryptography and Network Security)	0.15	65% of students will minimum score 60% marks	20
University Exam	0.15	60% of students will minimum score 50% marks	80
Oral Exam	0.15	60% of students will minimum score 70% marks	25
Lab Performance	0.2	75% of students will minimum score 70% marks	20

CSC604.2: Analyze and evaluate the authentication and hashing algorithms. **(Analysis**)

Direct Methods(80%): Test 2+ Quiz2 + UniExamTh+ UniExamsOral+ Labs

CO2dm = 0.2T2 + 0.2Q+ 0.2UTh + 0.2UOr+ 0.2Lab

InDirect Methods(20%): Course exit survey

CO2idm

CSC302.2 = 0.8*CO2dm + 0.2* CO2idm

Direct Method	Weightage	Target	Marks
Test 2	0.2	65% of students will minimum score 60% marks	Test – 10
Quiz 6,7,8,9(NPTEL Course on Cryptography and Network Security)	0.2	65% of students will minimum score 70% marks	20
University Exam	0.2	60% of students will minimum score	80

		50% marks	
Oral Exam	0.2	60% of students will minimum score 70% marks	25
Lab Performance	0.2	75% of students will minimum score 70% marks	20

CSC604.3: Identify different attacks on networks and analyze the performance of security protocols. **(B3-Apply)**

Direct Methods(80%): Test2 +Q+ UniExamTh + UniExamOral+ Labs

CO3dm = 0.2T2 + 0.2Q+0.2UTh +0.2UOr+ 0.2Lab

InDirect Methods(20%): Course exit survey

CO3idm

CSC302.3 = 0.8*CO3dm + 0.2* CO3idm

Direct Method	Weightage	Target	Marks
Test2	0.2	65% of students will minimum score 60% marks	10
Quiz3	0.2	65% of students will minimum score 70% marks	20
University Exam	0.2	60% of students will minimum score 50% marks	80
Oral Exam	0.2	60% of students will minimum score 70% marks	25
Lab Performance	0.2	75% of students will minimum score 70% marks	20

Course Outcomes Target:

Upon completion of this course students will be able to:

CSC604.1: Illustrate different cryptosystems from an application viewpoint.

Target Level : 2.5

CSC604.2: Analyze and evaluate the authentication and hashing algorithms

Target Level : 2.7

CSC604.3: Identify different attacks on networks and analyze the performance of security protocols

Target Level : 2.7

Content Beyond Syllabus:

Sr.No	Topic	Relevance with Pos	Relevance with PSOs	Methods
2	Improved encryption technique	PO1,PO2,PO3,PO4	PSO1,PSO2	Classroom discussion, Lab experiment
3	Familiarizing students on quantum cryptography	PO1	PSO1	Classroom discussion, PPT

Curriculum Gap:

Sr. No	Description	Proposed Actions	Relevance with Pos	Relevance with PEOs
1	Elliptic Curve Cryptography- (TO MEET INDUSTRY/PROFESSION REQUIREMENTS)	NPTEL	PO1,PO2	PSO1
2	Current trends in system & Information security.	Research paper analysis & presentation	PO1,PO2,PO3,PO9,PO11	PSO1

Rubrics for the Assigments:

Sr. No.		**Exceed Expectation (EE)**	**Meet Expectation (ME)**	**Below Expectation (BE)**
1.	On time submission Or completion (2)	Early or on time (2)	One session late (1)	More than one session late (0)
2.	Design/Solution(6)	Correct and detailed design/ solution(6)	Correct design/solution but some of the specifications or steps in design / solution missing(4)	Partially correct designs/solution with major mistakes(2)

3.	Organization(2)	Readable and structured (2)	Poor readability and somewhat structured (1)	Poor readability and not structured (0)

Rubrics for the Lab Experiments:

RUBRICS FOR EVALUATION

Sr. No.		**Exceed Expectation (EE)**	**Meet Expectation (ME)**	**Below Expectation (BE)**
1.	On time submission Or completion (2)	Early or on time (2)	One session late (1)	More than one session late (0)
2.	Preparedness(2)	Awareness about experiment to be performed, Knows the basic theory related to the experiment very well.(2)	Managed to explain the theory related to the experiment. (1)	Not aware of the theory to the point. (0)
3.	Skill (4)	Structured and optimum performance (4)	Few steps are not appropriate (2)	Just managed (1)
4.	Output (2)	Output is shown and exceptionally presentable and easy to follow. (2)	Output shown but not as expected (Partial output) (1)	Practical performed but failed to show output due to some error. (0)

LIST OF EXPERIMENTS

Expt. No.	Name of the Experiments	CO Mapping	Planned Date	Actual Date BATCH A	Marks
1.	Design and Implementation of a product cipher using Substitution and Transposition ciphers.	CO1	Week 1		10
2.	Implementation of Diffie- Hellman Key exchange algorithm and Simulation of Man In the Middle attack	CO1	Week 2		10
3.	Implementation and analysis of RSA cryptosystem and Digital signature scheme using RSA.	CO1,CO2	Week 3		10
4.	Implementation and analysis of ElGamal cryptosystem and Digital signature scheme using ElGamal	CO1,CO2	Week 4		10
5.	Performance Analysis of Hash Algorithms	CO2	Week 5		10
6.	Study of packet sniffer tools like Wireshark and its capture filters.	CO3	Week 6		10
7.	Port scanning and OS fingerprinting using NMAP	CO3	Week 7		10
8.	Design and Implement your own encryption/ decryption algorithm using any programming language.	CO1	Week 8		10
9.	Simulate DOS attack using Hping, hping3 tools.	CO3	Week 9		10
10.	To study and implement SQL Injection.	CO3	SUBMISSION 5/4		10
11.	Research Paper Analysis on current issues & direction of security	CO1, CO2, CO3			10

Rubrics for Research Paper Analysis and Presentation

Groups of Students will make presentations for the topic they selected and researched. After each presentation, we have Q&A and Discussion session in the class.

Standards	**10. Excellent**	6. **Satisfactory**	3. **Deficient**
Organization (2)	Has a clear opening statement that catches audience's interest; Stays focused throughout; summarizes main points	Has opening statement relevant to topic and gives outline of speech; is mostly organized; provides adequate road map for the listener	Has no opening statement or irrelevant statement; leaves listener wondering where the presentation is headed.
Writing (3)	Writing is clear and relevant, with no grammatical and/or spelling errors – polished and professional. Reference section properly formatted.	Most ideas are stated clearly and are related to the topic, with only minor grammatical and/or spelling errors. Reference section adequate.	Many ideas require clarification and/or are off-topic or have marginal relevance to the assignment. Many grammatical and/or spellings errors throughout the paper. The paper is very challenging to read due to poor writing flow. Improper reference section.
Quality of conclusion (3)	excellent summary of thesis argument with concluding ideas that impact reader. Introduces no new information	good summary of topic with clear concluding ideas. Introduces no new information.	Lack of summary of topic.
Team Work (5)	Students divide the work fairly and communicate about the challenges that they encounter. They work together to	Students divide the work fairly and communicate about the challenges that they encounter. They do not work together	No coordination

	answer difficult questions.	to answer difficult questions.	

Prsentation/discussion of a paper

The presentation should last about 8 minutes. After that, the students and myself will ask questions, and we will have a short discussion about the paper. You should read and understand the paper very well to be able to answer questions correctly. The other students are not expected to have read the paper. In the presentation, you should:

- Discuss the high level approach, idea or insight in the paper. Please don't go into details because the other students cannot remember details about all the different papers we are reading (but be able to answer questions that might require some detail). The point is for the class to understand the conceptual novelty, the main contribution of this paper.
- Explain the difference between this paper and the main reading for the lecture. For example, some papers might use different tools to achieve the same goal: some use programing language techniques for security, others use cryptography, etc.

We'll ask questions after each part to make sure everyone understands up to that point. In this case, you will be able to go in more detail about the paper. Describe at a high level the threat model, security guarantees, show an architecture diagram, overview of the protocol, and any evaluation highlights you deem useful

FR. Conceicao Rodrigues College Of Engineering

Father Agnel Ashram, Bandstand, Bandra-west, Mumbai-50

Department of Computer Engineering

T.E. (Computer) (semester VI)

(2019-2020)

Lesson Plan : CSS

Semester VI **Year: 2019-20**

Modes of Content Delivery:

I	Class Room Teaching	v	Self Learning On line Resources	Ix	Industry Visit
Ii	Tutorial	vi	Slides	X	Group Discussion
iii	Remedial Coaching	vii	Simulations/Demonstrations	xi	Seminar
Iv	Lab Experiment	viii	Expert Lecture	xii	Case Study

Lect. No.	Portion to be covered	Planned date	Actual date	Content Delivery Method/Learning Activities	Books referred
1.	Introduction to Information Security	7/1	Y	Class room teaching	T2
2	Security attacks, security goals, Methods of defense, security services	8/1	Y	Class room teaching	T2
3	The OSI security architecture, Network security model, Classical Encryption techniques, Symmetric cipher model, mono-alphabetic and poly-alphabetic substitution techniques:	9/1	Y	Class room teaching, Group discussion	T2
4	Vigenere cipher transposition techniques: keyed and keyless transposition ciphers,	10/1	Y		
5	playfair cipher	14/1	Y		

6	Hill cipher	15/1	Y	Class room teaching	T1
7	Steganography	16/1	Self study		T1
8	Modular Arithmetic and Number Theory:- Euclid‘s algorithm-– Prime numbers- Fermat‘s	17/1	Y	Class room teaching, Lab Experiment	T1
7	Euler‘s theorem- Testing for primality - The Chinese remainder theorem, Discrete logarithms.	20/1	Y	Class room teaching	T1
9	Block cipher principles, block cipher modes of operation, DES,	21/1	Y	Class room teaching, Lab Experiment	T1
10	Double DES, Triple DES	23/1	Y	Class room teaching, Lab Experiment	R2
11	Advanced Encryption Standard (AES),	24/1	Self Study Y	Class room teaching	T1
12	Stream Ciphers: RC5 algorithm.	27/1	Self Study	Class room teaching	R2
13	Public key cryptography: Principles of public key cryptosystems- The RSA algorithm	28/1	Y	Class room teaching	R2
14	RSA problems	30/1	Y	Class room teaching, Lab Experiment	R2
15	The knapsack algorithm	31/1		Class room teaching	R2
16	ElGamal Algorithm	3/2		Class room teaching, Lab Experiment	R2
17	Key management techniques: using symmetric and asymmetric algorithms and trusted third party. Diffie Hellman Key	4/2	Y	Class room teaching	R2

	exchange algorithm.				
18	Cryptographic hash functions, Properties of secure hash function, MD5	6/2		Class room teaching	R2
19	SHA-1	7/2		Class room teaching	R2
20	MAC, HMAC,	10/2		Class room teaching	R2
21	CMAC	11/2		Class room teaching	R2
22	Digital Certificate: X.509, PKI	13/2		Class room teaching	R2
23	PKI	14/2		Class room teaching	R2
24	User Authentication and Entity Authentication, One-way and mutual authentication schemes, Needham Schroeder Authentication protocol	24/2		Class room teaching	R2
25	Kerberos Authentication protocol	25/2		Class room teaching	R2
26	Digital Signature Schemes – RSA	2/3		Class room teaching, Lab Experiment	R2
27	EIGamal signature schemes	3/3		Class room teaching	R1
28	Schnorr signature schemes.		Self study	Class room teaching	R1
29	Network security basics: TCP/IP vulnerabilities (Layer wise),	5/3		Class room teaching	R1
30	Network security basics: TCP/IP vulnerabilities (Layer wise) Continue	6/3		Class room teaching	R1
31	Packet Sniffing, ARP spoofing	9/3		Class room teaching	R1
32	port scanning, IP spoofing	12/3		Class room teaching	R2

33	TCP syn flood, DNS Spoofing	13/3		Class room teaching	R2
34	Denial of Service: Classic DOS attacks	16/3		Class room teaching	R2
35	Source Address spoofing, ICMP flood	17/3		Class room teaching, Lab Experiment	R2
36	SYN flood, UDP flood, Distributed Denial of Service, Defenses against Denial of Service Attacks	19/3		Class room teaching	R2
37	Software Vulnerabilities: Buffer Overflow, Format string	23/3		Class room teaching	R1
38	cross-site scripting, SQL injection	24/3		Class room teaching	R1
39	Malware: Viruses, Worms, Trojans, Logic Bomb, Bots, Rootkits.	26/3		Class room teaching	R1
40	Internet Security Protocols: SSL	27/3		Class room teaching	R1
41	SSL Continue	30/3		Class room teaching	R1
42	IPSEC	31/3		Class room teaching, Lab Experiment	R1
43	IPSEC Continue	2/4		Class room teaching	R1
44	Secure Email: PGP	3/ 4		Class room teaching	R2
45	Secure Email: PGP Continue	13/4		Class room teaching	R1
46	Firewalls and types	16/4		Class room teaching	R1
47	IDS and types		Self Study	Class room teaching	R1
48	Honey pots		Self Study	Class room teaching	R1

Text Books/ Reference Books:

Te x t B o o k s :

1. Cryptography and Network Security by Behrouz A. Forouzan, TATA McGraw hill.

2. Security in Computing by Charles P. Pfleeger , Pearson Education

Reference Books:

1. Information security Principles and Practice by Mark Stamp, Wiley publication

2. Cryptography and Network Security by Atul Kahate – McGraw Hill

3. Cryptography and Network Security, William Stalling, Prentice hall

4. Applied Cryptography, Protocols Algorithms and Source Code in C, Bruce Schneier, Wiley

Web Resources:

1.http://nptel.iitm.ac.in/courses/106105031/
2.http://www.cs.purdue.edu/homes/ninghui/courses/426_Fall10/lectures.html
3.http://www.cs.northwestern.edu/~ychen/classes/cs395-w05/lectures.html
4.http://www.cs.iit.edu/~cs549/cs549s07/lectures.htm
5.https://engineering.purdue.edu/kak/compsec/NewLectures
6.http://www.math.utk.edu/~finotti/papers/grad.pdf
7.http://www.maths.usyd.edu.au/u/afish/Math2068/index_lectures.html
8.https://www.youtube.com/channel/UC6gtk6qGqk1fOOwPjxeNw8g
9.Few web resources are uploaded on moodle.