Cryptography and Computer Security (CSS)

Lecture # 1

Dr. Anant V Nimkar PhD(CSE-IIT Kharagpur)

Associate Professor

Department of Computer Engineering
Sardar Patel Institute of Technology Mumbai

INTRODUCTION
TO
CSS COURSE
(CS401)

Introduction to CSS Course

- Credits, Teaching & Exam Scheme
- Academic Engagement
- Evaluation Scheme
- CSS Course Outcomes
- Text and Reference Books
- Syllabus

Teaching Scheme, Credits & Examination Scheme

✓CSS – Teaching Engagement and Credits

Weekly Engagement				
L	T	P	O	E
2	0	2	4	8

Total Credit			
L	T	P	Credits
2	0	1	3

✓ CSS Examination Scheme

Theory			
ISE	MSE	ESE	Total
50	50	100	200

Laboratory			
ISE	MSE	ESE	Total
50	--	50	100

Evaluation Scheme

✓CSS Theory – Evaluation Scheme

Sr. No.	Components	Breakup Tests	Marks	Total Weightage
1	ISE	ISE 1 (Understanding Test Series)	10	50
		ISE 2 (MCQ at CE/CSE Dept. Test)	10	
2	MSE	One Test of One Hour	30	50
3	ESE	One Test of Three Hour	100	100
Total				200

Evaluation Scheme

✓CSS Lab – Evaluation Scheme

Sr. No.	Components	Percentage (Weightage)	Marks
1	ISE (Laboratory Experiments)	50	100
2	ESE	50	20
Total		100	100

Weekly Theory and Lab Sessions

✓ Theory Session

Day	Time	Duration	Venue
Tue	01:30 PM – 3:30 PM	2 Hr	703

✓ Lab Sessions

Day	Time	Batch	Venue
Mon	3:30 PM - 05:30 PM	I & II	410-A & B
Tue	10:30 AM - 12:30 PM	VII	403-B
Wed	01:30 PM - 03:30 PM	VI	406-A
Thu	01:30 PM - 03:30 PM	VIII	410-A
Fri	3:30 PM - 05:30 PM	V	604

CSS Course Outcomes

✓Describe the different types of the cryptographic algorithms to secure information.

✓Apply different cryptographic techniques to solve security-related problems.

✓Create a message digest from data to authenticate authorized user.

✓Use system security practices.

Text Books

1) William Stallings, "Cryptography and Network Security: Principles and Practice", Pearson , 5th Edition, 2011
2) Bernard Menezes, "Network Security and Cryptography", Cengage Learning, 2nd Edition, 2011
3) Behrouz A Fourouzan, “Cryptography and Network Security”, TMH India, 1st Edition, 2007
4) Charles P. Pfleeger, “Security in Computing”, Pearson Education, 5th Edition, 2015

Reference Books

1) Behrouz A Fourouzan, Debdeep Mukhopadhyay, " Cryptography and Network", TMH India , 2nd Edition, 2010

2) Matt Bishop, "Computer Security Art and Science", Addison-Wesley, 1st Edition, 2002

CSS Theory Syllabus

- ✓ **Introduction to Security and Cryptography**
  - ✓ Security – Goals, Services, Mechanisms
  - ✓ Cryptography
    - ✓ Symmetric Cipher Model
    - ✓ Substitution & Transportation Techniques
    - ✓ Block and Stream Ciphers
- ✓ **Secret and Public Key Cryptography Techniques**
  - ✓ Secret Key Cryptography - DES
  - ✓ Public Key Cryptography - RSA, DH Key Exchange
- ✓ **Hashing Algorithms and Authentication Protocols**
  - ✓ Cryptographic Hash Functions – HMAC, Digital signatures, Digital Signature Schemes
  - ✓ Authentication Protocols - Key Management, Public Key Infrastructure, PGP, Kerberos

CSS Theory Syllabus

- ✓ System Security
  - ✓ Intrusion Detection System, Types of IDS, Firewalls Characteristics, Types of Firewalls
  - ✓ Internet Protocol Security (IPSec)
  - ✓ Secure Sockets Layer (SSL)
  - ✓ Transport Layer Security (TLS)
  - ✓ Non-cryptographic protocol Vulnerabilities - DoS, DDoS, Session Hijacking and Spoofing

CSS Lab Experiments

1) Implement different substitution techniques.
2) Implement different transportation techniques.
3) Implementation of RSA algorithm.
4) Implementation of Diffie-Hellman key exchange algorithm.
5) Generate and calculate Hashes and checksum files.
6) Implement Pretty Good Privacy (PGP) security method.
7) Implement SNORT Intrusion Detection System.
8) Configure Firewall rules using IP tables.
9) Implement Dos and DDoS
10) Implement Session Hijacking attack.