CERTIFICATE COURSE: CYBER SECURITY
PAPER-I

Course Objectives:
- Learn the various threats in networks and security concepts.
- Apply authentication applications in different networks.
- Understand security services for email.
- Awareness of firewall and IT laws and policies

Course Outcomes:
After Completion of the course Student will be able to:
1. Understand the various network threats.
2. Analyse the forensic tools for evidence collection.
3. Apply the firewalls for threat analysis.

UNIT-I (10 HRS)

Ethical hacking, Attack Vectors, Cyberspace and Criminal Behaviour, Clarification of Terms, Traditional Problems associated with Computer Crimes, Realms of Cyber world, brief history of the internet, contaminants and destruction of data, unauthorized access, computer intrusions, white collar crimes, viruses and malicious code, virus attacks, pornography, software piracy, mail bombs, exploitation, stalking and obscenity in internet, Cyber psychology, Social Engineering.

UNIT-II (8 hrs)

Investigation Tools, e-discovery, EDRM Models, digital evidence collection and preservation, email investigation, email tracking, IP tracking, email recovery, searc and seizure of computer systems, password cracking.

Suggested Readings

1. Charles P. Fleeger, "Security in Computing", Prentice Hall, New Delhi, 2009.
2. BehrouzA.Forouzan, "Cryptography & Network Security", Tata McGraw Hill, India, New Delhi, 2009.

3. William Stallings, "Cryptography and Network Security", Prentice Hall, New Delhi, 2006.

4. Chalie Kaufman, Radia Perlman, Mike Speciner, "Network Security: Private Communication in a Public Network", Pearson Education, New Delhi, 2004.

5. Neal Krawetz, "Introduction to Network Security", Thomson Learning, Boston, 2007.

6. Bruce Schneier, "Applied Cryptography", John Wiley & Sons, New York, 2004.

CERTIFICATE COURSE: CYBER SECURITY
PAPER-II

Course Objectives:
- Learn the various threats in networks and security concepts.
- Apply authentication applications in different networks.
- Understand security services for email.
- Awareness of firewall and IT laws and policies

Course Outcomes:

After Completion of the course Student will be able to:
1. Understand the various network threats.
2. Analyse the forensic tools for evidence collection.
3. Apply the firewalls for threat analysis.

UNIT-I (10 hrs)

Introduction to Digital forensics, Forensic software and handling, forensic hardware and handling, analysis and advanced tools, forensic technology and practices, Biometrics: face, iris and fingerprint recognition, Audio-video evidence collection, Preservation and Forensic Analysis.

UNIT-II (8 hrs)

Forensic Analysis of OS artifact, Internet Artifacts, File System Artifacts, Registry Artifacts, Application Artifacts, Report Writing, Mobile Forensic-identification, collection and preservation of mobile evidences, social media analysis, data retrieval, Email analysis from mobile phones.

UNIT-III (12 HRS)

Ethics, Policies and IT Act Basics of Law and Technology, Introduction to Indian Laws, Scope and Jurisprudence, Digital Signatures, E Commerce-an Introduction, possible crime scenarios, law coverage, data interchange, mobile communication development, smart card and expert systems Indian Laws, Information Technology Act 2000, Indian Evidence Act, India Technology Amendment Act 2008, Indian

Penal Code , Computer Security Act 1987, National Information Infrastructure Protection Act 1996, Fraud Act 1997, Children Online Protection Act 1998, Computer Fraud and Abuse Act 2001, Intellectual Property, IP Theft, Copyright, Trademark, Privacy and Censorship, Introduction to Cyber Ethics, rights over intellectual property, Corporate IT Policy Formulations, Compliance Auditing.

Suggested Readings

1. Charles P. Fleeger, "Security in Computing", Prentice Hall, New Delhi, 2009.
2. BehrouzA.Forouzan, "Cryptography & Network Security", Tata McGraw Hill, India, New Delhi, 2009.
3. William Stallings, "Cryptography and Network Security", Prentice Hall, New Delhi, 2006.
4. Chalie Kaufman, Radia Perlman, Mike Speciner, "Network Security: Private Communication in a Public Network", Pearson Education, New Delhi, 2004.
5. Neal Krawetz, "Introduction to Network Security", Thomson Learning, Boston, 2007.
6. Bruce Schneier, "Applied Cryptography", John Wiley & Sons, New York, 2004.