MC5004 SECURITY IN COMPUTING

DETAILED SYLLABUS

UNIT I ELEMENTARY CRYPTOGRAPHY

Terminology and Background – Substitution Ciphers – Transpositions – Making Good Encryption Algorithms- Data Encryption Standard- AES Encryption Algorithm – Public Key Encryption – Cryptographic Hash Functions – Key Exchange – Digital Signatures.

UNIT II PROGRAM SECURITY

Secure programs – Non-malicious Program Errors – Viruses – Targeted Malicious code – Controls Against Program Threat – Control of Access to General Objects – User Authentication – Good Coding Practices – Open Web Application Security Project Flaws.

UNIT III SECURITY IN NETWORKS

Threats in networks – Virtual Private Networks – PKI – SSL – IPSec – Content Integrity – Access Controls – Honeypots – Traffic Flow Security – Firewalls – Intrusion Detection Systems – Secure e-mail.

UNIT IV SECURITY IN DATABASES

Security requirements of database systems – Reliability and Integrity in databases – Redundancy – Recovery – Concurrency/ Consistency – Monitors – Sensitive Data – Types of disclosures –Inference-finding and confirming sql injection.

UNIT V SECURITY MODELS AND STANDARDS

Secure SDLC – Security architecture models – Bell-La Padula Confidentiality Model – Biba Integrity Model – Graham-Denning Access Control Model – Harrison-Ruzzo-Ulman Model – Secure Frameworks – COSO – CobiT – Security Standards - ISO 27000 family of standards – NIST.

REFERENCES

1. Education Charles P. Pfleeger, Shari Lawrence Pfleeger, “Security in Computing”, Fourth Edition, Pearson, 2007
2. Michael Whitman, Herbert J. Mattord, “Management of Information Security”,Third Edition, Course Technology, 2010.
3. Michael Howard, David LeBlanc, John Viega, “24 Deadly Sins of Software Security: Programming Flaws and How to Fix Them”, First Edition, Mc GrawHill Osborne Media, 2009.