



KAMALDNP

kamaldnp.com • IT Training, Varanasi

PDF created by Raj Kamal using AI

Cyber Security — Complete Syllabus (Elective — Pathway, Option 3)

BTEUP Diploma in Electronics Engineering • 6th Semester • Session 2026-27

Subject 6.2.3 — Elective (Pathway), Option 3 (Theory) • Total 100 Marks • 3 Credits • L 3
- P 0 • Choose this OR Managerial Economics OR Finance Fundamentals OR Data Science

Examination Scheme

Code	Paper	Type	L - P	Credits	Internal	External	Total
6.2.3	Elective (Pathway): Cyber Security	Theory	3 - 0	3	Theory 40	Theory 60 (3 hrs)	100
Cyber Security Total				3	40	60	100

What This Subject Aims To Do

To introduce the fundamentals of cyber security, threats and ethical practices; explain cryptography and data encryption; describe network vulnerabilities and protection methods; give knowledge of web application vulnerabilities and security techniques; and develop understanding of security policies, audits and ethical hacking.

Unit-Wise Complete Topic List

Unit	Topic	Periods	Marks Share
1	Introduction to Cyber Security	7	16%
2	Cryptography and Encryption	10	24%

3	Network Security	7	16%
4	Web and Application Security	9	22%
5	Cyber Security Management and Ethical Hacking	9	22%

Unit 1 — Introduction to Cyber Security (7 Periods, 16%)

Topics: Definition and Importance of Cyber Security, Cyber Threats and Attacks: Malware, Phishing, Ransomware, Social Engineering, Denial of Service (DoS) , Cyber Security Principles: Confidentiality, Integrity, Availability, Authentication, Non-repudiation. Cyber Security in Electronics and IoT: Security concerns in embedded systems, smart devices, and industrial control systems. Cyber Laws and Ethics: Overview of IT Act (2000), Data Protection Laws, Ethical Hacking

In simple words: The threats — malware, phishing, ransomware, social engineering, denial of service — the core principles (confidentiality, integrity, availability), security in electronics and IoT, and cyber law and ethics.

Unit 2 — Cryptography and Encryption (10 Periods, 24%)

Topics: Introduction to Cryptography: Basics of encryption and decryption, Types of Cryptographic Algorithms: Symmetric (AES, DES), Asymmetric (RSA, ECC), Hash functions (MD5, SHA), Public Key Infrastructure (PKI): Digital signatures, Certificates, Trust models, Applications of Cryptography: SSL/TLS, Secure Email, VPNs, Blockchain. Cryptography in IoT and Embedded Systems: Key exchange protocols, securing communication between IoT devices

In simple words: Encryption: symmetric and asymmetric algorithms (AES, DES, RSA, ECC), hashes, digital signatures and PKI, and real uses like SSL/TLS, VPNs and blockchain.

Unit 3 — Network Security (7 Periods, 16%)

Topics: Introduction to Network Security: Concepts of firewalls, intrusion detection and prevention systems (IDS/IPS), Network Security Protocols: IPsec, SSL/TLS, HTTPS, SSH. VPNs and Proxies: Understanding Virtual Private Networks and Proxy Servers for secure communication. Securing Wireless Networks: Wireless security standards (WPA, WPA2, WPA3), threats to wireless networks

In simple words: Protecting networks: firewalls, intrusion detection and prevention, security protocols, VPNs and proxies, and wireless security (WPA2/WPA3).

Unit 4 — Web and Application Security (9 Periods, 22%)

Topics: Web Application Vulnerabilities: XSS (Cross-Site Scripting), SQL Injection, CSRF (Cross-Site Request Forgery). Web Security Measures: Web Application Firewalls (WAFs), Secure Coding Practices, Input validation. Secure HTTP (HTTPS): SSL/TLS in securing web traffic. Mobile and IoT Application Security: Securing mobile applications, secure communication in IoT

In simple words: Web attacks — cross-site scripting, SQL injection, cross-site request forgery — and the defences: web application firewalls, secure coding and input validation.

Unit 5 — Cyber Security Management and Ethical Hacking (9 Periods, 22%)

Topics: Cyber Security Policies and Risk Management: Establishing security policies, risk assessment, and mitigation strategies. Security Audits: Understanding how to conduct a security audit, common audit frameworks. Ethical and Legal Issues: Legal aspects of hacking, cybersecurity compliance, and international regulations

In simple words: Managing security: policies, risk assessment and mitigation, security audits, and the legal and ethical side of hacking.

Reference Books (as listed in the syllabus)

- Cyber Security Essentials by Charles J. Brooks
- Principles of Information Security by Michael E. Whitman and Herbert J. Mattord
- Network Security Essentials by William Stallings
- Introduction to Modern Cryptography by Jonathan Katz and Yehuda Lindell
- Ethical Hacking and Penetration Testing Guide by Rafay Baloch
- Cyber Security and Cyber Laws by S. B. S. K. Sharma (Indian Author)
- Cyber Security: Understanding Cyber Crimes, Computer Forensics, and Legal Perspectives by Nishith Chhapparia (Indian Author)

KAMALDNP • kamaldnp.com • support@kamaldnp.com • +91 8318013442 • Varanasi, UP

Source: BTEUP 3rd Year curriculum (folder2627), approved in C.D.C. meeting held on 16.07.2026. Topic lists follow the official syllabus; short explanations are the author's own plain-English summaries, not syllabus text.

Please confirm with your own polytechnic for any local changes.