



School of Computing Science and Engineering

B.Tech Cyber Security and Digital Forensics

Programme Output (POs):

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 the 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 to 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 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 teamwork: 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 own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.
12. Life-long learning: Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.

Programme Specific Outcomes (PSOs):

PSO1: Gain knowledge with respect to ever growing threats including both hardware and software.

PSO2: Develop skills to anticipate future cyber threats and develop methods to counter them.

PSO3: Ability to use various tools, methods and techniques to secure information.

PSO4: Implement security solutions without compromising Cyber laws and individual's privacy.

Programme Educational Outcome (PEOs):

PEO1: Impart strong foundation in comprehensive security issues along with sound knowledge and capability on proactive Cyber Defense.

PEO2: Prepare graduates to be up to date with the rapidly changing security threats and laws by comprehending, understanding and analysing.

PEO3: Analyse and utilize existing methods to solve problems in the domain of security and digital forensics.

PEO4: Prepare graduates with the skills required to be aware and protect the Computer Systems. Understand and communicate the risks, threats and mitigation techniques to decision makers and develop defensive strategies.

PEO5: Enable graduates to apply the knowledge of various tools and techniques gained through program to identify, counter and recover from cyber threats.

PEO6: Conduction of digital evidence collection, evaluation and expedite recovery using forensic tools.