SOFT COMPUTING
(TOE064)

COURSE OUTCOMES (COs):	
CO 1:	Understand and apply fuzzy logic and its applications.
CO 2:	Understand artificial neural networks and its applications.
CO 3:	Apply and solving multi-objective optimization problems using evolutionary algorithms (MOEAs).
CO 4:	Applications of Soft computing to solve problems in varieties of application domains.
CO 5:	Solving single-objective optimization problems using GAs.
Unit	**Topic**
I	Introduction to Soft Computing: Concept of computing systems. "Soft" computing versus "Hard" computing Characteristics of Soft computing Some applications of Soft Computing Techniques
II	Fuzzy logic: Introduction to Fuzzy logic: Fuzzy sets and membership functions. Operations on Fuzzy sets. Fuzzy relations, rules, propositions, implications and inferences. Defuzzification techniques. Fuzzy logic controller design. Some applications of Fuzzy logic.
III	Genetic Algorithms: Concept of "Genetics" and "Evolution" and its application to proablistic search techniques, Basic GA framework and different GA architectures. GA operators: Encoding, Crossover, Selection, Mutation, etc. Solving single-objective optimization problems using GAs.
IV	Multi-objective Optimization Problem Solving: Concept of multi-objective optimization problems (MOOPs) and issues of solving them. Multi-Objective Evolutionary Algorithm (MOEA). Non-Pareto approaches to solve MOOPs Pareto-based approaches to solve MOOPs. Some applications with MOEAs.
V	Artificila Neural Networks: Biological neurons and its working. Simulation of biolgical neurons to problem solving. Different ANNs architectures. Training techniques for ANNs. Applications of ANNs to solve some real-life problems.

Text Book (s):

1. Fuzzy Logic: A Practical approach, F. Martin, Mcneill, and Ellen Thro, AP Professional, 2000.
2. Fuzzy Logic with Engineering Applications (3rd Edn.), Timothy J. Ross, Willey, 2010.
3. Foundations of Neural Networks, Fuzzy Systems, and Knowledge Engineering, Nikola K. Kasabov, MIT Press, 1998.
4. Fuzzy Logic for Embedded Systems Applications, Ahmed M. Ibrahim, Elsevier Press, 2004.
5. An Introduction to Genetic Algorithms, Melanie Mitchell, MIT Press, 2000.
6. Genetic Algorithms in Search, Optimization and Machine Learning, David E. Goldberg, Pearson Education, 2002.

NETWORK SECURITY
(TOE074)

COURSE OUTCOMES (COs):	
CO 1:	To learn the vulnerabilities of computer networks to attacks by adversaries and hackers.
CO 2:	To evaluate he methods and techniques to defend against these attacks and to minimize their damage.
CO 3:	To understand and explain the risks faced by computer systems and networks.
CO 4:	To explain how standard security mechanisms work.
CO 5:	To develop security mechanisms to protect computer systems and networks.
Unit	**Topic**
I	Conventional encryption, Security attacks, Security, Model for network security, classical encryption techniques, DES, Triple DES, AES, block cipher modes, stream ciphers, key distribution, random number generation.
II	Introduction to number theory, Public - Key cryptography, principles of public – key cryptosystems, RSA algorithm, key management, distribution of public keys, public key – distribution of secret keys, elliptic curve cryptography.
III	Message authentication and hash functions, hash and MAC algorithms, digital signatures, authentication protocols, Kerberos, x-509 directory.
IV	Email security –PGP, IP Security, Web security, System security- intrusion detection, malicious software, firewalls.
V	Intruders: Intrusion Detection, Password Management, Recommended Reading and Web Sites. Malicious Software: Viruses and Related Threats, Virus Countermeasures, Distributed Denial of Service Attacks. Firewalls: Firewall Design Principles, Trusted Systems, Common Criteria for Information Technology Security Evaluation.

Text Book (s):

1. Stallings, W. (2011). Cryptography and network security: Principles and practice (5th ed.). PHI.
2. Schneier, B. (2015). Applied cryptography: Protocols, algorithms (2nd ed.). Wiley.
3. Kaufman, C., Perlman, R., & Speciner, M. (2006). Network security: Private communication in a public world (2nd ed.). Prentice-Hall/Pearson.
4. Menezes, A. J., C., V. O., & Vanstone, S. A. (1997). Handbook of applied cryptography. CRC Press.
5. Anderson, R. (2001). Security engineering: A guide to building dependable distributed systems. Wiley.
6. Stinson, D. R. (2006). Cryptography: Theory and practice (3rd ed.). Chapman & Hall/CRC.