NIRMA UNIVERSITY
SCHOOL OF TECHNOLOGY, INSTITUTE OF TECHNOLOGY
M. Tech. in Electronics and Communication Engineering (Embedded System)
M.Tech. Semester - II
Department Elective II

L	T	Practical component				C
		LPW	PW	W	S	
3	-	-	-	-	-	3

Course Code	**6EC271ME22**
Course Title	**Hardware Security**

Course Learning Outcomes (CLOs):

At the end of the course, students will be able to -

1. Identify and analyze vulnerabilities in Digital Logic Design and its solution using Crypto Algorithms.
2. Analyze physical and side-channel attacks and provide solution for its countermeasures.
3. Analyze and design secured cryptographic Hardware using trusted Trojan detection mechanism, trusted IC and FPGA implementation of crypto hardware.

Syllabus: **Teaching Hours:45**

UNIT I: Introduction to Crypto Algorithms **10**

Cryptography basics, Cryptographic algorithms - Symmetric Key algorithms, Public Key algorithms and Hash Algorithms, Data Encryption Standards, Advanced Encryption Standards, RSA, BowFish .

UNIT II: Design Intellectual Property Protection **08**

Introduction to IP Protection, Watermarking Basics, Watermarking Examples, Good Watermarks, Fingerprinting, Hardware Metering.

UNIT III: Physical Attacks and Modular Exponentiation **06**

Physical Attacks (PA) Basics, Physical Attacks and Countermeasures, Building Secure Systems, Modular Exponentiation (ME) Basics, ME in Cryptography, ME Implementation and Vulnerability, Montgomery Reduction.

UNIT IV: Side Channel Attacks and Counter Measures **06**

Introduction to Side Channel Attacks, Memory Vulnerabilities and Cache Attacks, Power Analysis, More Attacks and Countermeasures, Modified Modular Exponentiation.

UNIT V: Hardware Trojan Detection and Trusted IC Design **05**

Hardware Trojan (HT) and Trusted IC, Hardware Trojan Taxonomy, Hardware Trojan Detection Overview, Hardware Trojan Detection Methods, Trusted IC Design with HT Prevention.

UNIT VI: Emerging Technologies **10**

FPGA Implementation of Crypto algorithms, Vulnerabilities and Countermeasures in FPGA Systems, Role of Hardware in Security and Trust, Physical Unclonable Functions (PUF) Basics, Reliability, Trust Platform Modules

Self-Study:

The self-study contents will be declared at the commencement of semester. Around 10% of the questions will be asked from self-study contents.

Suggested Readings:

1. Debdeep Mukhopadhyay and Rajat Subhra Chakraborty, Hardware Security: Design, Threats, and Safeguards, CRC Press.
2. Tehranipoor, Mohammad, Wang, Introduction to Hardware Security and Trust, Springer.
3. Ted Huffmire, Handbook of FPGA Design Security, Springer.
4. Stefan Mangard, Elisabeth Oswald, Thomas Popp, Power Analysis Attacks - Revealing the Secrets of Smart Cards, Springer.
5. Doug Stinson, Cryptography Theory and Practice, CRC Press.