(2). “Blockchain A Practical Guide to Developing Business, Law, and Technology Solutions”, Joseph J. Bambara Paul R. Allen, McGraw-Hill Education, 2018

(3). “Blockchain Enabled Applications”, Vikram Dhillon, David Metcalf, Max Hooper, Apress, 2017

(4). “Blockchain Blueprint for a New Economy”, Melanie Swan, O’Reilly Media, 2015

(5). “Blockchain Basics: A Non-Technical Introduction in 25 Steps”, Daniel Drescher, Apress, 2017

CSCS 504 : Cryptanalysis of Hardware Security

CO1 : To perform the cryptanalysis at the hardware level, which requires special kind skills, tools and methods which are different from software level cryptanalysis.

CO2: To understand the different means of breaking the hardware security like side channel attack.

CO3: To understand the different means of breaking hardware security like power analysis attack.

CO4: To understand the different means of breaking hardware security like timing attack.

UNIT I

Side Channel Analysis : Difference of Side Channel Analysis and Conventional Cryptanalysis, Types of Side Channel Attacks, Kocher’s Seminal Works, Power Attacks, Fault Attacks, Cache Attacks, Scan Chain Based Attacks, **Differential Fault Analysis of Ciphers :** General Principle of DFA of Block Ciphers, DFA and Associated Fault Models, Principle of Differential Fault Attacks on AES. **(12 hours)**

UNIT II

State-of-the-art DFAs on AES, Multiple-Byte DFA of AES-128, Extension of the DFA to Other Variants of AES, DFA of AES Targeting the Key Schedule, DFA countermeasures **Cache Attacks on Ciphers :** Memory Hierarchy and Cache Memory, Timing Attacks Due to CPU Architecture, Trace-Driven Cache Attacks, Access-Driven Cache Attacks, Time-Driven Cache

Attacks, Countermeasures for Timing Attacks. **(12 hours)**

UNIT III

Power Analysis of Cipher Implementations, Testability of Cryptographic Hardware, Hardware Intellectual Property Protection through Obfuscation, Hardware Trojans, Logic Testing based Hardware Trojan Detection, Side-channel Analysis Techniques for Hardware Trojans Detection, Design Techniques for Hardware Trojan Threat Mitigation, Physically Unclonable Functions: a Root-of-Trust for Hardware Security, Genetic Programming-based Model-building Attack on PUFs. **(12 hours)**

TextBooks:

(1). “Hardware Security Design, Threats, and Safeguards”, Debdeep Mukhopadhyay Rajat Subhra Chakraborty, CRC Press, 2015

(2). “ Hardware IP Security and Trust “ , Prabhat Mishra, Swarup Bhunia, Mark Tehranipoor, Springer, 2017

(3). “Fault Tolerant Architectures for Cryptography and Hardware Security”, Sikhar Patranabis Debdeep Mukhopadhyay, Springer, 2018

(4). “Security of Block Ciphers - From Algorithm Design to Hardware Implementation”, Kazuo Sakiyama, Yu Sasaki, Yang Li, Wiley, 2015

(5). “Physically Unclonable Functions From Basic Design Principles to Advanced Hardware Security Applications”, Basel Halak, Springer, 2018

(6). “Hardware-Based Computer Security Techniques to Defeat Hackers From Biometrics to Quantum Cryptography”, Roger Dube, Wiley, 2008

CSCS 505 : Mobile Phone Security and Forensics

CO1 : To make the students aware of the forensics of mobile phones, which would aid the police investigation of a cybercrime.

CO2: To sensitize the students about the process of the mobile phone forensics and the legal aspects of the same.