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.

CO3: To make students use the different tools required for the mobile phone forensics.

CO4: To make the students aware of the ways and means to acquire different data from mobile phones.

UNIT I

Mobile Phone Security : Confidentiality, Integrity, and Availability Threats in Mobile Phones, A Multinational Survey on Users' Practices, Perceptions, and Awareness Regarding Mobile Phone Security, Voice, SMS, and Identification Data Interception in GSM, Software and Hardware Mobile Phone Tricks, SMS Security Issues, Mobile Phone Forensics.

(12 hours)

UNIT II

Introduction to Mobile Forensics : The need for mobile forensics, Understanding mobile forensics, Challenges in mobile forensics, The mobile phone evidence extraction process, Practical mobile forensic approaches, Potential evidence stored on mobile phones, Examination and analysis, Rules of evidence, Good forensic practices, **Android Forensics** : Understanding Android, The evolution of Android, The Android architecture, Android security, The Android file hierarchy, The Android filesystem, Android Forensic Setup and Pre-Data Extraction Techniques, Setting up a forensic environment for Android, Connecting an Android device to a workstation, Screen lock bypassing techniques, Gaining root access

(12 hours)

UNIT III

Android Data Extraction Techniques : Understanding data extraction techniques, Manual data extraction, Logical data extraction, Physical data extraction, Android Data Analysis and Recovery, Analyzing and extracting data from Android image files using the Autopsy tool, Understanding techniques to recover deleted files from the SD card and the internal memory, Android App Analysis, Malware, and Reverse Engineering, Analyzing widely used Android apps to retrieve valuable data, Techniques to reverse engineer an Android application, Android malware.

(12 hours)

Text Books:

(1). "Mobile Phone Security and Forensics - A Practical Approach", Iosif I. Androulidakis, Springer International Publishing Switzerland, 2016

(2). "Practical Mobile Forensics - Forensically investigate and analyze iOS, Android, and