RAJIV GANDHI PROUDHOGIKI VISHWAVIDYALAYA, BHOPAL

New Scheme Based On AICTE Flexible Curricula

CSE-Cyber Security /Cyber Security, VIII Semester

CY-801Hardware Security

Course Outcome:

- CO1: Understand and optimize the process of implementing cryptographic algorithms on hardware
- CO2: Learn the different kinds of attacks that can be mounted against cryptographic algorithms
- CO3: Learn the process of building Physical Unclonable Functions and make them resilient to attacks
- CO4: Understand the different kinds of Trojans, their impact and learn the effective countermeasures for defending against them
- CO5: Learn the different kinds of threats at the micro architectural level and their corresponding countermeasures.

UNIT: 1: Overview of Different Issues of Hardware Security , Algebra of Finite Fields, Basics of the Mathematical Theory of Public Key Cryptography, Basics of Digital Design on Field-programmable Gate Array (FPGA), Classification using Support Vector Machines (SVMs).

UNIT: 2:Useful Hardware Security Primitives: Cryptographic Hardware and their Implementation, Optimization of Cryptographic Hardware on FPGA, Physically Unclonable Functions (PUFs), PUF Implementations, PUF Quality Evaluation, Design Techniques to Increase PUF Response Quality.

UNIT: 3: Side-channel Attacks on Cryptographic Hardware: Basic Idea, Current-measurement based Side-channel Attacks (Case Study: Kochers Attack on DES), Design Techniques to Prevent Side-channel Attacks, Improved Side-channel Attack Algorithms (Template Attack, etc.), Cache Attacks

UNIT: 4 : Testability and Verification of Cryptographic Hardware: Fault-tolerance of Cryptographic Hardware, Fault Attacks, Verification of Finite-field Arithmetic Circuits, Modern IC Design and Manufacturing Practices and Their Implications.

UNIT: 5: Hardware Intellectual Property (IP) Piracy and IC Piracy, Design Techniques to Prevent IP and IC Piracy, Using PUFs to prevent Hardware Piracy,Model Building Attacks on PUFs (Case Study: SVM Modelling of Arbiter PUFs, Genetic Programming based Modelling of Ring Oscillator PUF).

Text Books:

1. Debdeep Mukhopadhyay and RajatSubhra Chakraborty, "Hardware Security: Design, Threats, and Safeguards", CRC Press.
2. Ahmad-Reza Sadeghi and David Naccache (eds.): Towards Hardware-intrinsic Security: Theory and Practice, Springer.
3. Ted Huffmire et al: Handbook of FPGA Design Security, Springer.
4. Stefan Mangard, Elisabeth Oswald, Thomas Popp: Power analysis attacks - revealing the secrets of smart cards. Springer 2007.
5. Doug Stinson, Cryptography Theory and Practice, CRC Press.

RAJIV GANDHI PROUDHOGIKI VISHWAVIDYALAYA, BHOPAL

New Scheme Based On AICTE Flexible Curricula

CSE-Cyber Security /Cyber Security, VIII Semester

CY-802(A)-Database Security

Pre-Requisite: Students should have an understanding of basic database concepts and mathematics.
Course Outcomes:
After completing the course student should be able to:

1. Identify security threats in database systems.
2. Ensure the data confidentiality anddata integrity.
3. Only authorized user has access to the data, avoid unauthorized data observation & modification.
4. Design and Implement secure database systems.
5. Solve Complex Problems in a Team of database works.

Course Contents:

Unit1: Introduction:-Databases and Information Systems, An example usage context, Database system concepts and architecture, Overview of Information Security, Database design using the relational model
Functional dependencies: Keys in a relational model, Concept of functional dependencies, Normal forms based on primary keys, BCNF Further Dependencies: Multi-values dependencies and fourth normal form, Join dependencies and fifth normal form, Inclusion dependencies, other dependencies and normal forms.

Unit2. Database security lifecycle, data risk assessment, Analyze data threats, risks and vulnerabilities, Understand the need for a database security architecture, database security architecture, Implement a feedback mechanisms, Understand how to adjust policies and practices based on feedback mechanisms using different securitymodels.

Unit3. Database Vulnerabilities, Threats and Physical Security: distinction between data and database security from network and perimeter security, external and internal database threats, flaws in perimeter security, risks of not securing an organization’s data, typical database security hierarchy, analysis general security landscape, evaluation of security fundamentals, Understand the importance for staying current with database releases, fixes and security patches , Managing USB ports and USB enabled devices, Understand the implications of the physical placement of databasefiles and their copies.

Unit4. Security Models - Bell and LaPadula's Model Biba's Model Dion's Model Sea View Model Jajodia and Sandhu's Model The Lattice Model for the Flow Control conclusion Security Mechanisms Introduction User Identification/Authentication Memory Protection Resource Protection Control Flow Mechanisms Isolation Security Functionalities in Some Operating Systems Trusted Computer System Evaluation

Unit5. Security Management, Data/ information, protecting Password file, Access Control Structure, Software Security, Element of Information Security, Steps for Better Security, Malicious Software, System Security Assurance Concepts, Importance of Information System.

Recommended Books with Full Specification:

1. Handbook of Database Security: Applications and Trends by Michael Gertz and SushilJajodia
2. Database Security and Auditing, Hassan A. Afyouni, India Edition, CENGAGE Learning, 2009.
3. Database Security, Castano, Second edition, Pearson Education
4. Database security by alfred basta, melissazgola, CENGAGE learning
5. H. F. KorthandA.Silberschatz.DatabaseConcept, TMH.
6. Godbole, “Information system security”, Wiley.
7. Cole.Krutz&Conley “Networksecurity”Wiley.

RAJIV GANDHI PROUDHOGIKI VISHWAVIDYALAYA, BHOPAL

New Scheme Based On AICTE Flexible Curricula

CSE-Cyber Security /Cyber Security, VIII Semester

CY-802(B) -Deep & Reinforcement Learning

Pre-Requisite: Machine Learning
Course Outcomes: After completing the course student should be able to:
1. Describe in-depth about theories, models and algorithms in machine learning.
2. Compare and contrast different learning algorithms with parameters.
3. Examine the nature of a problem at hand and find the appropriate learning algorithms and it's parameters that can solve it efficiently enough.
4. Design and implement of deep and reinforcement learning approaches for solving real-life problems.

Course Contents:

Unit 1: History of Deep Learning, McCulloch Pitts Neuron, Thresholding Logic, Activation functions,
Gradient Descent (GD), Momentum Based GD, Nesterov Accelerated GD, Stochastic GD, AdaGrad,
RMSProp, Adam, Eigenvalue Decomposition. Recurrent Neural Networks, Back propagation through
time (BPTT), Vanishing and Exploding Gradients, Truncated BPTT, GRU, LSTMs, Encoder Decoder
Models, Attention Mechanism, Attention over images.

Unit 2: Autoencoders and relation to PCA, Regularization in auto encoders, denoisingauto encoders,
Sparse auto encoders, Contractive auto encoders, Regularization: Bias Variance Tradeoff, L2 regularization, early stopping, Dataset augmentation, Parameter sharing and tying, Injecting noise at Input, Ensemble methods, Dropout, Batch Normalization, Instance Normalization, Group Normalization.

Unit 3: Greedy Layer wise Pre-training, Better activation functions, Better weight initialization methods,
Learning Vectorial Representations of Words, Convolutional Neural Networks, LeNet, AlexNet, ZF-Net,
VGGNet, GoogLeNet, ResNet, Visualizing Convolutional Neural Networks, Guided Back propagation,
Deep Dream, Deep Art, Recent Trends in Deep Learning Architectures.

Unit 4: Introduction to reinforcement learning (RL), Bandit algorithms – UCB, PAC, Median Elimination, Policy Gradient, Full RL & MDPs, Bellman Optimality, Dynamic Programming - Value iteration, Policy iteration, and Q-learning & Temporal Difference Methods, Temporal-Difference Learning, Eligibility Traces, Function Approximation, Least Squares Methods.

Unit 5: Fitted Q, Deep Q-Learning, Advanced Q-learning algorithms, Learning policies by imitating Optimal controllers , DQN & Policy Gradient, Policy Gradient Algorithms for Full RL, Hierarchical RL, POMDPs, Actor-Critic Method, Inverse reinforcement learning, Maximum Entropy Deep Inverse Reinforcement Learning, Generative Adversarial Imitation Learning, Recent Trends in RL Architectures.

Text Books:

1. Deep Learning, An MIT Press book, Ian Goodfellow and YoshuaBengio and Aaron Courville
2. Pattern Classification- Richard O. Duda, Peter E. Hart, David G. Stork, John Wiley & Sons Inc.
3. Reinforcement Learning: An Introduction, Sutton and Barto, 2nd Edition.
4. Reinforcement Learning: State-of-the-Art, Marco Wiering and Martijn van Otterlo, Eds.

RAJIV GANDHI PROUDHOGIKI VISHWAVIDYALAYA, BHOPAL

New Scheme Based On AICTE Flexible Curricula

CSE-Cyber Security /Cyber Security, VIII Semester

CY-802(C) -Lightweight Cryptography

Course Outcomes: After completing the course student should be able to:

1. To understand the design strategies of lightweight ciphers to secure resource constrained devices.
2. To compare various lightweightcryptographic algorithms.
3. To acquire the fundamental knowledge onthe applications of lightweight cryptography.

Course Contents:

Unit 1: Introduction, Overview of Lightweight Cryptography - Security Threats for resource constrained devices, Design strategies for lightweight cryptography - Constraints and Compromises of Lightweight Algorithms- Modes of Operation.

Unit 2: Lightweight Cryptographic Primitives, Lightweight Block Ciphers: DESL and DESXL-, PRESENT-CLEFIA - LED-SIMON and SPECK-TWINE-PRINCE-MIDORI- RECTANGLE GRANULE-CRAFT.

Unit 3: Lightweight Stream Ciphers, Lightweight HASH functions, Lightweight Message, Authentication Codes, Key management and Applications of Lightweight Cryptography.

Unit 4: Key management: Challenges in Designing IoTGroup Key Management Protocols-Lightweight Group Key Management Protocols-SymmetricKey Constructions- Asymmetric Key Constructions. Applications: IPsec, TLS, Cyber Physical Systems, IoT devices.

Text Books:

1. SrinivasanRamakrishnan, “Lightweight Cryptographic Techniques and Cyber security Approaches”, ISBN: 978-1-80355-733-5, 2022.
2. Eisenbarth , “Lightweight Cryptography for Security and Privacy”, Springer ,2015.

RAJIV GANDHI PROUDHOGIKI VISHWAVIDYALAYA, BHOPAL

New Scheme Based On AICTE Flexible Curricula

CSE-Cyber Security /Cyber Security, VIII Semester

CY-803(A)-Mobile and Wireless Security

Course Contents:

Unit1: Wireless Networking Trends, Key Wireless Physical Layer Concepts, Wireless Local Area Networks, Wireless Personal Area Networks, WiMAX (Physical layer, Media access control, Mobility and Networking)

Unit2. Mobile IPv4, Mobile IPv6, TCP over Wireless Networks, Ad Hoc Networks - Issues and Routing, Wireless Sensor Networks, Wireless Mesh and Multi-Hop Relay Networks.

Unit3. 3G and 4G Network, General Packet Radio Services (GPRS), Universal Mobile Telecommunication System (UMTS).Radio Frequency Identification (RFID).

Unit4, Introduction to LTE, Security Issues in Wireless Networks, Security Models: Military and civil security, vulnerability and threat models, End-end Security, link encryption, compartments Privacy. Authentication. Denial of service. Nonrepudiation. Issues in multi-level secure systems. Internet security models: IPv4/IPv6 encapsulation header.

Unit5. E-Commerce, M-Commerce, Electronic payment systems, electronic cards, Secure Electronic Transactions: Trust, Encryption, Authentication, confidentiality, integrity and non-repudiation.

Recommended Books:

1. Stalling W., “ Network Security Essentials”, Pearson
2. Practical Packet Analysis: Using Wireshark to Solve Real-Word Network problems by ChrisSanders
3. Jochen Schiller, “Mobile Communications”, PHI.
4. UweHansmann, LotharMerk, Martin S. Nicklons and Thomas Stober, Principles of MobileComputing, Springer, New York, 2003
5. Frank Adelstein, Sandeep KS Gupta, Golden Richard, Fundamentals of Mobile and PervasiveComputing,McGraw-Hill

RAJIV GANDHI PROUDHOGIKI VISHWAVIDYALAYA, BHOPAL

New Scheme Based On AICTE Flexible Curricula

CSE-Cyber Security /Cyber Security, VIII Semester

CY-803(B)-Financial crime, Motivations and Typologies

Course Outcome:

1. Understand Tracing Illicit financialTransactions.
2. Understand the various anti-moneylaundering laws.
3. Explain the various schemes of insurancefraud.
4. State and explain Bankruptcy schemes.
5. Explain the methods of proving corruptpayments.

Course Contents:

Unit1:Tracing Illicit Transactions: Identify the common areas of interviewquestions in tracing financial crime evidence-State and explain the main sources income andexpenditure of illicit financial crime- Distinguishbetween the direct and indirect methods oftracing illicit financial transactions- Describe theinvestigation procedures for tax fraud – Describethe indirect method of tracing financial crime-Describe the Net worth Method of investigatingfinancial crime- Prepare a profile of a financial fraudster-Determine the net worth of a financialcrime suspect.

Unit 2: Anti-Money Laundering Laws: Define Money Laundering and Identify theprocess of money laundering - Identify the MajorMoney Laundering Countries in the World-Explain Money Laundering and describe thepenalty for Money Laundering under the MoneyLaundering Act- Describe the Composition ofthe Financial Intelligence Centre- DefineAccountable Institutions - State and explain thecomposition of accountable institutions- Identifythe various International bodies that imposesMoney Laundering Sanctions- State and Explainthe various of types of Money LaunderingSanctions.

Unit 3: Insurance and Medical Fraud: Define insurance fraud- State and explain the types of insurance policies-State and explain the various schemes of insurance fraud- Identify the red flags associated with insurance fraud- State and explain the types of insurance fraud investigation tips- Define medical fraud- State and explain the types of medical fraud schemes.

Unit 4: Bankruptcy: Define Bankruptcy- Identify the red flagsassociated with bankruptcy-State and explainBankruptcy schemes- Define Planned Bustoutand state its characteristics- State and Explainthe objectives of the world bank principles oneffective insolvency- State and Explain the legalframework for creditor rights and Insolvency.

Unit 5: Bribery and Corruption: Define bribery and corruption-State and explainkickback schemes-State and explain the methodsof making illegal payments- State and explainthe types of procurement fraud schemes-Identify the red flags associated with bribery.

Recommended Books:

8. Expert Fraud Investigation; a step-by-stepguide by Tracy L. Coenen.
9. A Practitioner’s Guide to the Law andRegulation of Financial Crime by ArunSrivastava and Andrew Keltie, 2010.
10. Anti-Money Laundering ActForensic Criminology by Wayne A.Petherick, Brent E. Turvey, Claire E.Ferguson, 2009.
11. Insurance Fraud Casebook, Paying apremium for crime by Joseph T. Wells andLaura Hymes

RAJIV GANDHI PROUDHOGIKI VISHWAVIDYALAYA, BHOPAL

New Scheme Based On AICTE Flexible Curricula

CSE-Cyber Security /Cyber Security, VIII Semester

CY-803(C)-Human Computer Interaction

Course Objectives:
To provide the basic knowledge on the levels of interaction, design models, techniques and validations focusing on the different aspects of human-computer interface and interactions.

Course Outcomes:
After the completion of this course, the students will be able to:
1. Enumerate the basic concepts of human, computer interactions
2. Create the processes of human computer interaction life cycle
3. Analyze and design the various interaction design models
4. Apply the interface design standards/guidelines for evaluating the developed interactions
5. Apply product usability evaluations and testing methods

Course Contents:
Unit I HCI Foundations: Input–output channels, Human memory, Thinking: reasoning and problem solving, Emotion,Individual differences, Psychology and the design of interactive systems, Text entry devices,Positioning, pointing and drawing, Display devices, Devices for virtual reality and 3D interaction,Physical controls, sensors and special devices, Paper: printing and scanning.

Unit II Designing Interaction: Overview of Interaction Design Models, Discovery - Framework, Collection - Observation,Elicitation, Interpretation - Task Analysis, Storyboarding, Use Cases, Primary StakeholderProfiles, Project Management Document.

Unit III Interaction Design Models: Model Human Processor - Working Memory, Long-Term Memory, Processor Timing, KeyboardLevel Model - Operators, Encoding Methods, Heuristics for M Operator Placement, What theKeyboard Level Model Does Not Model, Application of the Keyboard Level Model, GOMS -CMN-GOMS Analysis, Modeling Structure, State Transition Networks - Three-State Model,Glimpse Model, Physical Models, Fitts' Law.

Unit IV Guidelines in HCI: Shneideman's eight golden rules, Norman's Sever principles, Norman's model of interaction,Nielsen's ten heuristics, Heuristic evaluation, contextual evaluation, Cognitive walk-throughCollaboration and Communication:Face-to-face Communication, Conversation, Text-based Communication, Group working, Dialogdesign notations, Diagrammatic notations, Textual dialog notations, Dialog semantics, Dialoganalysis and design.

Unit V Human Factors and Security: Groupware, Meeting and decision support systems, Shared applications and artifacts, Frameworksfor groupware Implementing synchronous groupware, Mixed, Augmented and Virtual RealityValidation: Validations - Usability testing, Interface Testing, Use Acceptance Testing.

References:

- A Dix, Janet Finlay, G D Abowd, R Beale., Human-Computer Interaction, 3rd Edition,Pearson Publishers,2008.
- Shneiderman, Plaisant, Cohen and Jacobs, Designing the User Interface: Strategies forEffective Human Computer Interaction, 5th Edition, Pearson Publishers, 2010.
- Hans-JorgBullinger," Human-Computer Interaction", Lawrence Erlbaum Associates,Publishers.
- Jakob Nielsen," Advances in Human-computer Interaction",Ablex Publishing Corporation
- Thomas S. Huang," Real-Time Vision for Human-Computer Interaction", Springer
- Preece et al, Human-Computer Interaction, Addison-Wesley, 19.