13-14	Interrupts : Purpose of interrupts, Interrupt instructions, interrupt vectors and interrupt descriptors, functioning of interrupt controller
15	Direct Memory Access (DMA): Basic DMA operation, functioning of DMA controller

Assessment Methods

Written tests, assignments, quizzes, presentations as announced by the instructor in the class.

Keywords

Microprocessor architecture, microprocessor programming, interfacing,

---

Information Security (BHCS17A) Discipline Specific Course - (DSE)

Credit: 06

Course Objective

The course offers a broad overview of the fundamentals of information security covering topics such as error correction/detection, cryptography, steganography, malwares, This course also touches on the implications of security in Internet of Things (IoT).

Course Learning Outcomes

On successful completion of this course, a student will be able to,

1. Identify the major types of threats to information security
2. Describe the role of cryptography in security
3. Select appropriate error-detection and error-correction methods for an application
4. Discuss the strengths and weaknesses of private and public key crypto systems
5. Describe malwares and memory exploits
6. Discuss the need for security in IoT

Detailed Syllabus

Unit 1

Introduction: Security Concepts, Challenges, Security architecture, Security attacks, security services, security mechanisms

Unit 2

Error detecting/correction: Block Codes, Generator Matrix, Parity Check Matrix, Minimum distance of a Code, Error detection and correction, Standard Array and syndrome decoding, Hamming Codes

Unit 3

Cryptography: Encryption, Decryption, Substitution and Transposition, Confusion and diffusion, Symmetric and Asymmetric encryption, Stream and Block ciphers, DES, cryptanalysis.

Public-key cryptography, Diffie-Hellman key exchange, man-in-the-middle attack

Digital signature, Steganography, Watermarking.

Unit 4

Malicious software's: Types of malwares (viruses, worms, trojan horse, rootkits, bots), Memory exploits - Buffer overflow, Integer overflow

Unit 5

Security in Internet-of-Things: Security implications, Mobile device security - threats and strategies

Practical

1. Implement the error correcting code.
2. Implement the error detecting code.
3. Implement caeser cipher substitution operation.
4. Implement monoalphabetic and polyalphabetic cipher substitution operation.
5. Implement playfair cipher substitution operation.
6. Implement hill cipher substitution operation.
7. Implement rail fence cipher transposition operation.
8. Implement row transposition cipher transposition operation.
9. Implement product cipher transposition operation.
10. Illustrate the Ciphertext only and Known plaintext attacks.
11. Implement a stream cipher technique

References

1. Pfleeger, C.P., Pfleeger,S.L., & Margulies, J. (2015). *Security in Computing.* 5th edition. Prentice Hall
2. Lin, S. & Costello, D. J. (2004). *Error Control Coding: Fundamentals and applications*. 2nd edition. Pearson Education
3. Stallings, W. (2018). *Cryptography and network security*. 7th edition. Pearson Education.

Additional Resources

1. Berlekamp, E. R. (1986). *Algebraic Coding Theory*. McGraw Hill Book Company
2. Stallings, W. (2018) *Network security, essentials.* 6th edition. Pearson Education.
3. Whitman M.E., & Mattord H.J. (2017). *Principle of Information Security*. 6th edition. Cengage Learning.

Course Teaching Learning Process

- Use of ICT tools in conjunction with traditional class room teaching methods
- Interactive sessions
- Class discussions

Tentative weekly teaching plan is as follows:

Week	Content
1-2	Security Concepts, Challenges, Security architecture, Security attacks, security services, security mechanisms
3-4	Error detecting/correction, Block Codes, Generator Matrix, Parity Check Matrix, Minimum distance of a Code, Error detection and correction, Standard Array and syndrome decoding, Hamming Codes
5-7	Cryptography: Encryption, Decryption, Substitution and Transposition, Confusion and diffusion, Symmetric and Asymmetric encryption, Stream and Block ciphers, DES, Modes of DES
8-9	Cryptanalysis, Types of cryptanalytic attacks, Public-key cryptography, Diffie-Hellman key exchange, man-in-the-middle attack

10-11	Digital signatures, Steganography and Digital Watermarking
12-13	Malicious Software: Types of malwares (viruses, worms, trojan horse, rootkits, bots), Memory exploits - Buffer overflow, Integer overflow
14-15	Security in Internet-of-Things, Security implications, Mobile device security - threats and strategies, Cyberlaws

Assessment Methods

Written tests, assignments, quizzes, presentations as announced by the instructor in the class.

Keywords

Security mechanisms, private and public key cryptography, malware detection, security in IoT.

Data Mining (BHCS17B) Discipline Specific Elective - (DSE)

Credit: 06

Course Objective

This course introduces data mining techniques and enables students to apply these techniques on real-life datasets. The course focuses on three main data mining techniques: Classification, Clustering and Association Rule Mining tasks.

Course Learning Outcomes

On successful completion of the course, students will be able to do following:

1. Pre-process the data, and perform cleaning and transformation.
2. Apply suitable classification algorithm to train the classifier and evaluate its performance.
3. Apply appropriate clustering algorithm to cluster data and evaluate clustering quality
4. Use association rule mining algorithms and generate frequent item-sets and association rules

Detailed Syllabus