(BHCS17A) Discipline Specific Elective Course 3 (DSE-3) - Information Security

Guidelines

References	Chapter	Topic
		Unit 1: Introduction
[3]	**1.1, 1.2, 1.3, 1.4, 1.5 (pg no. 21-33)**	Security Concepts, Security Challenges, Security architecture, Security attacks, Security services , Security mechanisms
		Unit 2: Error Detecting/Correction
[2]	**3.1, 3.2, 3.3, 3.4 (pg no. 66-90)**	Block Codes, Generator Matrix, Parity Check Matrix, Minimum distance of a Code, Error detection and correction, Standard Array and syndrome decoding
	4.1 (pg no. 100-102)	Hamming Codes
		Unit 3: Cryptography
[3]	**3.1, 3.2, 3.3 (pg no. 86-108)**	Encryption, Decryption, Symmetric encryption, cryptanalysis, Substitution Techniques – Caesar, Monoalphabetic cipher, Playfair and Hill, Polyalphabetic cipher, Vigenere and One-Time Pad. Transposition Techniques – Rail fence Cipher
[1]	**3.5 (pg no. 110-111)** **11.1 (pg no. 710)**	Steganography Watermarking
[3]	**4.1, 4.2, 4.3 (pg no. 119-133)**	Stream and Block ciphers, confusion and diffusion, DES (Data Encryption Standard)
	9.1, 9.2 (pg no. 285- 297)	Asymmetric encryption, Public-key cryptography
	10.1 (pg no. 314-318)	Diffie-Hellman key exchange, man-in-the-middle attack
	13.1 (pg no. 420-424)	Digital signature
		Unit 4: Malicious software's
[1]	**3.1 (pg no. 134-152, 160)**	Memory Exploits Buffer Overflow, Integer Overflow
	3.2 (pg no. 166-196)	Types of malwares (viruses, worms, Trojan horse, root kits, bots)
		Unit 5: Security in Internet-of-Things
[1]	**13.1 (pg no. 814-820)**	Security implications, Mobile device security - threats and strategies

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.

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.