BCT 2306- Fundamentals of Computer Security

Course logistics and details

- Lectures – Monday 12.00 noon – 2.00 p.m. [PAU 1.1 C)
- Assignments and CATs : 10 %
  - 2 written assignments
  - All submissions will be made in hard copy through the class representatives and MUST be in PRINTED format
- Continuous Assessment Tests: 20%
  - 2 sit in CATs
- FINAL EXAM: 70%
  - End of semester
- You can reach me through hratemo@jkuat.ac.ke .

Course Outline

- Information security in computer and communication systems
- Threat analysis (under security attack)
- Security services
- Physical and logical security
- Access control
- Identification
- Authentication
- Authorization
- Programmed threats
- Internet connection policies and implementation
- Message confidentiality
- Message authentication
- Non repudiation
- Web security
- Classical and public key cryptosystems
- Application to information schemes and digital signatures
- Key distribution and key agreement
- Authentication and secret sharing
- Security policies

Course Outline

Week	Topic/Chapter	Sub-topics
1	Introduction	• Introduction to computer security • Fundamental security objectives • Their organizational impact levels

2	Introduction	• Challenges of computer security
		  • Security attack
		  • Security service
		  • Security mechanism
		• Model for network security

Course Outline

Week	Topic/Chapter	Sub-topics
3	Number Theory and Cryptography	• Introduction • Divisibility and Modular Arithmetic • Modular Exponentiation • Primes and Greatest Common Divisors • Primality • Euclidean Algorithm • Basic Notions of Finite Fields • GCD and Linear Combinations • Solving Inverses

Course Outline

Week	Topic/Chapter	Sub-topics
4	Symmetric Ciphers Part 1	• Classical encryption techniques • Symmetric cipher model • Substitution techniques • Transposition techniques
5	Symmetric Ciphers Part 2	• Block cipher principles • Data Encryption Standard (DES) • Triple DES • CAT 1 + Assignment 1

Course Outline

Week	Topic/Chapter	Sub-topics
6	Public key encryption/Asymmetric Ciphers	• Public key Cryptography • RSA key Management • Diffie-Hellman Key Exchange • ElGamal Encryption Scheme
7	Digital Signatures	▪ Introduction ▪ Components of a signature scheme ▪ Security of digital signatures ▪ Attacks on digital Signatures ▪ ElGamal Signature Scheme

Course Outline

Week	Topic/Chapter	Sub-topics
8	Key Agreement Schemes	▪ Introduction ▪ Key Agreement Schemes ▪ Diffie Hellman
9	Key Distribution Schemes	▪ Introduction ▪ Key Distribution Centers ▪ Techniques of distributing public keys

Course Outline

Week	Topic/Chapter	Sub-topics

10	Message Authentication	▪ Introduction
		▪ Message Authentication Requirements
		▪ Message Authentication Functions
		  ▪ Encryption
		  ▪ MAC
		▪ CAT 2 + Assignment 2

11	Web Security	