Arab Academy for Science and Technology and Maritime Transport
Computer Science Curriculum
Course Syllabus

Course Code: CS421	**Course Title:** Computer System Security	**Classification:** R	**Coordinator:** **Lecturer:** Prof. Dr. Aliaa Youssif	**Credit Hours:** 3
Pre-requisites: • CS322 (Operating Systems) • CE231 (Introduction to Networks)	**Co-requisites:** None	**Schedule:** Lecture: 2 hours Tutorial-Lab: 2 hours		

Office Hours:

Course Description:
The course is an introduction to computer and network security. The course encompasses the study of security mechanisms for secrecy, integrity, and availability. Topics include basic cryptography and its applications, security in computer networks and distributed systems and control and prevention of viruses and other rogue programs. In addition, hands-on experience will be provided through a series of programming assignments.

Textbook:
W. Stallings, *Cryptography and Network Security, Principles and Practices*, Prentice Hall.

References:

- William Stallings, Network Security Essentials: Applications and Standards, Prentice Hall.
- Charles P. Pfleeger and Shari Lawrence Pfleeger, Security in Computing, Prentice Hall.

Course Objective/Course Learning Outcome:	**Contribution to Program Student Outcomes:**
1 Identify threats to computer system.	(SO1) Analyze a complex computing problem and to apply principles of computing and other relevant disciplines to identify solutions.
2 Outline security attacks methods.	(SO2) Design, implement, and evaluate a computing-based solution to meet a given set of computing requirements in the context of the program’s discipline
3 Master classical and modern cryptography techniques.	(SO3) Communicate effectively in a variety of professional contexts.
4 Experiment with symmetric and asymmetric key distribution protocols.	(SO4) Recognize professional responsibilities and make informed judgments in computing practice based on legal and ethical principles.

5 Experiment with authentication protocols.	(SO6) Apply computer science theory and software development fundamentals to produce computing-based solutions.
6 Experiment with authentication protocols.	
Course Outline: 1. Classical Encryption Techniques 2. Block Ciphers & DES. 3. Block cipher design principles/Block cipher modes of operation. 4. Advanced encryption standard (AES) 5. Introduction to Number Theory 6. Public key cryptography	7. Key Distribution for Symmetric Encryption 8. Key Distribution for Asymmetric Encryption 9. Message Authentication and Hash Functions 10. Hash and MAC Algorithms 11. Firewalls

Grade Distribution:

7th Week Assessment (30%)

12th Week Assessment (20%)

Year Work (10%)

Final Exam (40%)

Policies:

Attendance:
AASTMT Education and Study Regulations (available at aast.edu)

Academic Honesty:
AASTMT Education and Study Regulations (available at aast.edu)

Late Submission:
Late submissions are graded out of 75% (1 week late), 50% (2 weeks late), 25% (3 weeks late), 0% (more than 3 weeks late)