Data Security

- **Course number and name:**
  CC 518 – Data Security

- **Credits and contact hours**
  Credits Hours: 3Hrs
  Contact Hours: In Lecture 2Hrs, and In Tutorial 2Hrs

- **Instructor's or course coordinator's name**
  Coordinator Name: Dr. Rowayda Sadek

- **Text book, title, author, and year**
  - W. Stalling, "Cryptography and Network Security, Principles and Practices ".3rd Ed, Prentice Hall 2003.
  - "Cryptography and Network Security, Principles and Practices".3rd Ed, Prentice Hall 2003.

- **Specific course information**
  - **a. Catalog description**
    Goals of data security – classical encryption techniques – encryption standards – Internet security issues: (e-mail – e-commerce – firewall) – Symmetric cryptography – Asymmetric cryptography.
  - **b. prerequisites or co-requisites**
    Prerequisites: CC319
  - **c. Types of Course (required, elective, or selected elective course) in the program**
    Elective Course

- **Specific goals for the course**
  - **a. Specific outcomes of instruction**
    After the completion of this course the students will be able to:

	Course Learning Outcomes	SO
1	Understand what computer security is? Why it is important? And the security concept and security levels which specified in the (orange book) standard for trusted systems.	J,F
2	Understand security history, and describes what these security standards are and how they are developed.	J,F
3	Understand the encryption techniques their mathematics to protect stored & transmitted data.	A

Topics to be covered

- Overview
- Goals of data & information security
- Threats & types of Attacks
- A Model For Network Security
- Classical Encryption Technique: Symmetric Cipher Model, Substitution Techniques, Ceaser Cipher, Monoalphabetic Cipher
- Playfair Cipher & Hill Cipher
- Polyalphabetic Cipher & Transposition techniques
- Steganography
- Block Cipher & DES
- Block cipher modes of operation: ECB, CBC, CFB, OFB and CTR
- Advanced encryption standard: Evaluation criteria for AES
- Electronic mail Security Threats , Threats enabled by e-mail , E-mail based attacks
- Message authenitication Techniques
- Pretty good privacy(PGP) message generation
- Firewalls