DATA SECURITY COURSE SPECIFICATION

HIGHER EDUCATION PERFORMANCE REVIEW: PROGRAMME REVIEW

COURSE SPECIFICATION

This Course Specification provides a concise summary of the main features of the course and the learning outcomes that a typical student might reasonably be expected to achieve and demonstrate if he/she takes full advantage of the learning opportunities that are provided. It should be cross-referenced with the programme specification.

1. Teaching Institution	University of Baghdad/ college of Science for Women
2. University Department/Centre	Computer Science department
3. Course title/code	Data Security/ CDY 408
4. Program(s) to which it contributes	
5. Modes of Attendance offered	Class and Lab attendance is required
6. Semester/Year	4th year/ 2nd Semester

7. Number of hours tuition (total)	60 hour (30 theoretical + 30 practical)
8. Date of production/revision of this specification	3/4/2016
9. Aims of the Course	
Identify the principles of encryption and decryption and study different encryption methods, the fundamental ones like Substitution and Transposition methods and the new ones, which are used globally, like DES, AES and RSA.	

10· Learning Outcomes, Teaching ,Learning and Assessment Method

H- Knowledge and Understanding

A1. Identifying the fundamental encryption principles.

A2. Identifying the skills that are used for the decryption

A3. Identifying the new encryption methods, which are used globally.

B. Subject-specific skills

B1. The ability to design encryption algorithms depends substitution methods.

B2. The ability to design encryption algorithms depends Transposition methods.

B3. The ability to deal with RSA, AES and DES methods.

B4. Building software for encryption and decryption using deferent methods.

C. Thinking Skills

C1. Depending the discussion in presenting a subject and listen to different opinions to solve the problems.

C2. Making the student acting in building the programs in the laboratory without confining this a specific template

Teaching and Learning Methods

- Providing a printed chapters from a number of books (in English) for all the students before the start of the semester.
- Explain the subject in Arabic and answer students' questions.
- Each student in the laboratory creates an integrated database system that addresses a problem that was studied and analyzed according to what has been studied.

Assessment methods

- Written exams
- Practical exams (Laboratory)
- Prepare a computer software (Project)

D. General and Transferable Skills (other skills relevant to employability and personal development)

D1.Foucsing on building the mentality that depends on the analysis and conclusion in solving problems.

11. Course Structure

Week	Hours	ILOs	Unit/Module or Topic Title	Teaching Method	Assessment Method
1	4	Learning the basics of cryptography	Terminology and background of Cryptography	As mentioned in 10	As mentioned in 10
2-3	8	Learning substitution ciphers methods	Substitution ciphers		
4-5	8	Learning transposition ciphers methods	Transposition ciphers		
6	4	Learning characteristics of good cipher	Characteristics of good cipher		
7	4	Learning symmetric and asymmetric encryption systems	Symmetric and asymmetric encryption systems		
8-9	8	Learning cryptanalysis methods	Cryptanalysis		
10-11	8	Learning data encryption	Data encryption		

		standard (DES) method	standard (DES)		
12	8	Learning AES encryption method	AES encryption		
13	4	Learning public key encryption	Public key encryption		
14	4	Learning the encryption using RSA encryption	RSA encryption		
15	4	Learning the properties of digital signatures	Digital signatures		

13. Admissions

Pre-requisites	Visual Basic.net + Computer Security + Enough knowledge of mathematics.
Minimum number of students	10 students
Maximum number of students	30 students
12. Infrastructure	
Required reading: · CORE TEXTS · COURSE MATERIALS · OTHER	**BOOK: Security in Computing, by Charles P. Pfleegers ,Fourth Edition, Prentic Hall,2006** **APPLICATION:** Using Visual Basic.Net to prepare the software that encipher and decipher the methods that have been studied.
Special requirements (include for example workshops, periodicals, IT software, websites)	
Community-based facilities (include for example, guest Lectures , internship , field studies)	