Republic of Iraq
The Ministry of Higher Education & Scientific Research

University : **Kufa**
College : **Education for Girls**
Department : **Computers**
Stage : **4th**
Instructor Name : **Abdallah A. Lafta**
Academic Status : **A.I.**
Qualification :**Computer Msc.**
Place of work : **Najaf**

Course Syllabus
2014 / 2015

Course Instructor	Abdallah A. Laftah				
E-mail	abdullaa.lafta@uokufa.edu.iq				
Title	Network Security and Cryptography				
Course Description	We cover in this course principles and practice of cryptography and network security: classical systems, symmetric block ciphers (DES, AES, other contemporary symmetric ciphers), cryptanalysis, public-key cryptography (RSA, discrete logarithms), cryptographic protocols, hash functions, authentication, key management, key exchange, signature schemes, email and web security, viruses, firewalls, and other topics.				
Course Objective	• Provides an in-depth coverage of Information Security and Cryptography from both a conceptual and application-oriented viewpoint.				
Textbook	• Stallings, W., Cryptography and Network Security: Principles and Practice, 6th edition, Prentice Hall, 2014.				
References	• Computer Security: Principles and Practice, 2015				
Course Assessment	Course Student Assessment			Final Exam	
	Tests	Practice	Assignments	Practice	Theoretical
	30%	10%	10%	10%	40%
General Notes	• Microsoft Visual Studio 2013 Ultimate Edition used for practice the examples.				

Republic of Iraq
The Ministry of Higher Education
& Scientific Research

University : **Kufa**
College : **Education for Girls**
Department : **Computers**
Stage : **4th**
Instructor Name : **Abdallah A. Lafta**
Academic Status : **A.I.**
Qualification :**Computer Msc.**
Place of work : **Najaf**

Course weekly Outline
2014 / 2015

Week	Date	Topics Covered	Lab.	Assignments
1		Information Security: An Overview		
2		Threats, and Security Measures		
3		Defining security policies		HW1
4		Cryptography		
5		Substitution cipher		
6		Mono-alphabetic cipher		HW2
7		Poly-alphabetic cipher		
8		Polygram cipher		
9		Homophonic cipher		
10		Transposition cipher		
11		Message reversal cipher		HW3
12		Columnar cipher		
13		Rail-fence cipher		
14		Route cipher		
15		Combination substitution/ transposition cipher		
16		Symmetric Key Ciphers		HW4
17		One time pad		
18		Block Ciphers (DES)		
19				
20		Encode each 64 bit block of data		
21		DES mode operation		
22		The decryption process		HW5
23		Weakness of DES		
24		Stream cipher		
25		Synchronous stream cipher		
26		Linear feed back		HW6
27		RSA		
28		Knapsack algorithm		
29				

As the instructor for this course, I reserve the right to adjust this schedule in any way that serves the educational needs of the students enrolled in this course.

Instructor Signature: Dean Signature: