Course Name: Information and Computers Networks Security
Course Code: IT423

I. Basic Course Information

Major or minor element of program: Major
Department offering the course: Information Technology Department

Academic level: 300 Level
Semester in which course is offered: Second (Spring) Semester
Course pre-requisite(s): Computers Networks 1 (IT222)

Credit Hours: 3
Contact Hours Through:

Lecture	Tutorial*	Practical*	Total
2.5	0.0	1.5	4.0

* 1.5 hours for **either** Tutorial or Practical

Approval date of course specification: January 2015

II. Overall Aims of Course

The overall aims of this course are describing the principles and fundamentals of information and network security with emphasis on: Basic concepts of information and computer network security; classical encryption techniques; modern symmetric encryption techniques; public-key encryption; system and network security tools and network security practice.

III. Program ILOs covered by course

Program Intended Learning Outcomes (By Code)			
Knowledge & Understanding	Intellectual Skills	Professional Skills	General Skills
K9,K10,K11,K17	I17,I18,I19	P7,P9,P14	G2,G5,G6

IV. Intended Learning Outcomes of Course (ILOs)

a. Knowledge and Understanding

On completing the course, students should be able to:

- K.1 Define the three aspects of information security: services, mechanisms and attacks.
- K.2 Describe block cipher principles and mode of operations.
- K.3 Define and check the Finite Fields and Modular Arithmetic used in some modern ciphers.
- K.4 Describe the principles of Public-Key Cryptosystem.
- K.5 Explain the current underlying technologies of computer architecture and organization, operating systems, computer networks, watermarking, and digital signature as well.
- K.6 Illustarte the current underlying technologies used in network security such as Biometric technology.

b. Intellectual/Cognitive Skills

On completing the course, students should be able to:

- I.1 Evaluate classical techniques their extent to meet the criteria defined for its current use as secure systems.
- I.2 Asses Data Encryption Standard (DES) cipher and develop arguments on its development to Triple DES.
- I.3 Evaluate RSA& El-Gammal algorithms.
- I.4 Distinguish the difference between symmetric and asymmetric encryption.

c. Practical/Professional Skills

On completing the course, students should be able to:

- P.1 Implement classical techniques and measure their different security degrees.
- P.2 Implement Data Encryption Standard (DES) cipher.
- P.3 Implement RSA & El-Gammal algorithm and demonstrate the effect of large prime numbers in security.

d. General and Transferable Skills

On completing the course, students should be able to:

- G.1 Improve team working skills.
- G.2 Improve the report writing skills and the oral presentation skills.
- G.3 Improve the ability to describe and analyse problems.

V. Course MatrixContents

	Main Topics / Chapters	Duration (Weeks)	Course ILOs Covered by Topic (By ILO Code)			
			K & U	I.S.	P.S.	G.S.
1-	Introduction to Information Security	1	K1,K5	I1		
2-	Classical Encryption Techniques	1	K1	I1	P1	
3-	Finite Fields	2	K3			G3
4-	Symmetric Block Cipher (DES)	2	K2	I2	P2	All
5-	Introduction to Number Theory	1	K3			G3
6-	Public Key Cryptography (RSA& ElGammal)	2	K4	I3,I4	P2	G1,G3
7-	Digital Signature Schemes	1	K4,K5	I3,I4	P3	G1,G3
8-	Biometric technology	2	K6		P2,P3	
9-	Watermarking	1	K5		P2,P3	
	Net Teaching Weeks	**13**				

VI. Course Weekly Detailed Topics / hours / ILOs

Week No.	Sub-Topics	Total Hours	Contact Hours	
			Theoretical Hours	Practical Hours*
1	Introduction to Information Security	2.5	2.5	
2	Classical Encryption Techniques	4	2.5	1.5
3	Finite Fields	4	2.5	1.5
4	Secure Hill Cipher	4	2.5	1.5
5	Introduction to Symmetric Block Cipher	4	2.5	1.5
6	Data Encryption Standard (DES) algorithm	4	2.5	1.5
7	**Midterm Exam**			
8	Introduction to Number Theory	4	2.5	1.5
9	Public Key Cryptography and RSA	4	2.5	1.5
10	Asymmetric Encryption El-Gammal algorithm	4	2.5	1.5
11	Digital signature Schemes	4	2.5	1.5
12	Current and Future Direction of Biometric Technology	4	2.5	1.5
13	Age verification in real time	4	2.5	1.5
14	Water Marking of Vector Geospatial Data	4	2.5	1.5
15	**Final Exam**			
Total Teaching Hours		**51**	**33**	**18**

* **No Practical/Tutorial during the first week of the semester**

VII. Teaching and Learning Methods

Teaching/Learning Method	Selected Method	Course ILOs Covered by Method (By ILO Code)			
		K & U	Intellectual Skills	Professional Skills	General Skills
Lectures & Seminars	X	All	All	All	All
Tutorials					
Computer lab Sessions	X	All	All	All	G1,G3
Practical lab Work	X			All	G1,G3
Reading Materials	X	All	All		
Web-site Searches	X	All	All		
Research & Reporting	X	All	All		G2
Problem Solving / Problem-based Learning	X				G3
Projects	X		All	P2,P3	G1
Independent Work					
Group Work	X		All	All	G1
Case Studies	X	All	All	All	
Presentations	X				G2
Simulation Analysis					
Others (Specify):					

VIII. Assessment Methods, Schedule and Grade Distribution

Assessment Method	Selected Method	Course ILOs Covered by Method (By ILO Code)				Assessment Weight / Percentage	Week No.
		K & U	I.S.	P.S.	G.S.		
Midterm Exam	X	K1,K2,K3,K4	All			10%	7
Final Exam	X	All	All			60%	15
Quizzes	X	K4,K5	I1			10%	5
Course Work							
Report Writing							
Case Study Analysis							
Oral Presentations							
Practical	X			All	All	10%	10
Group Project	X			All	All	10%	12
Individual Project							
Others (Specify):							

IX. List of References

Essential Text Books	• Stallings, William. "Cryptography and network security: principles and practices", Fourth edition, Prentice-Hall, Inc, 2005
Course notes	• PowerPoint presentations for the course.
Recommended books	• Rick Lehtinen. "Computer Security Basics", second edition • Stallings, William. "Network Security Essentials: Applications and Standards", third edition • Arthur E. Hutt, Douglas B. Hoyt, Seymour Bosworth. "Computer Security Handbook", third edition
Periodicals, Web sites, etc.…	• http://pleiad.cairo-avicenna.edu.eg/ • http://www.ieee-security.org/index.html • http://scrc.nist.gov • http://www.securityfocus.com

X. Facilities required for teaching and learning

List the facilities required

- Computer lab connected through a network.
- Software: Microsoft .Net, Java compiler, firewall

Course coordinator: Prof.Aboul ElAlla Hassanien

Head of Department: Prof. Hesham El Mahdy

Date: January 2015