University of Sana'a
Faculty of Engineering
Department: Electrical Engineering
Title of the Program: Communication Engineering and Networks

Course Specification of Information and Network Security

I. Course Identification and General Information:

1.	Course Title:	Information and Network Security				
2.	Course Code & Number:	CNE445				
3.	Credit hours:	C.H				Total
		Th.	Tu.	Pr	Tr.	
		2	1	1	-	3
4.	Study level/ semester at which this course is offered:	Fifth Year / First Semester				
5.	Pre –requisite (if any):	Programming Language 2 (C/C++) (CCE152)				
6.	Co –requisite (if any):	None.				
7.	Program (s) in which the course is offered:	(Communication Engineering and Networks) and (Computer & Control)				
8.	Language of teaching the course:	English				
9.	Location of teaching the course:	Classes of Electrical Engineering Department				
10.	Prepared By:	Assoc. Prof. Dr. Farouk AL-Fuhaidy				
11.	Date of Approval					

II. Course Description:

This is an introductory course to the information and network security, to make students familiar with the basic concepts of information and network systems security and mechanisms. The course aims to the security goals, security functions, and security mechanisms. The course will cover various topics related to computer & network security, introduction to information security, information and network security and risk management, access control, security architecture and design, data privacy, telecommunications and network protection against various attacks. The course is supported with variant examples introduced by tutorial and laboratory works.

Prepared by	Head of Department	Quality Assurance Unit	Dean of the Faculty	Academic Development Center & Quality Assurance
Assoc. Prof. Dr. Farouk AL-Fuhaidy	Asst. Prof. Dr. Adel Ahmed Al-Shakiri	Assoc. Prof. Dr. Mohammad Algorafi	Prof. Dr. Mohammed AL-Bukhaiti	Assoc. Prof. Dr. Huda Al-Emad

Rector of Sana'a University
Prof. Dr. Al-Qassim Mohammed Abbas

III. Course Intended learning outcomes (CILOs) of the course		Referenced PILOs
a1	Demonstrate an understanding of basic categories of threats and attacks, encryption/decryption algorithms, public/private keys, and authentication related to information and networks.	A1
a2	Explain the objectives of information security and discuss the importance and applications of confidentiality, integrity, and availability.	A2
b1	Formulate the application of some encryption/decryption protocols including AES, DES, SSL, RSA, and IPSec to solve information and network security systems.	B1
c1	Apply concepts of public keys, private keys, cryptosystem, authentication, and digital signatures to secure simple information systems.	C1
c2	Implement network security protocols such as SSL and MAC, Web security, WEP and computer viruses and Internet attacks, and apply them in real applications to secure internet traffic using information and programming skills.	C4
d1	function effectively within teams to accomplish a common goal.	D1

(A) Alignment Course Intended Learning Outcomes of Knowledge and Understanding to Teaching Strategies and Assessment Strategies:

Course Intended Learning Outcomes	Teaching strategies	Assessment Strategies
a1- Demonstrate an understanding of basic categories of threats and attacks, encryption/decryption algorithms, public/private keys, and authentication related to information and networks.	▪ Lectures, ▪ Tutorial, ▪ Laboratory work, ▪ Projects, ▪ Use of communication and information technology	▪ Examinations, ▪ Homework presentations, ▪ Individual and group project reports

Prepared by	Head of Department	Quality Assurance Unit	Dean of the Faculty	Academic Development Center & Quality Assurance
Assoc. Prof. Dr. Farouk AL-Fuhaidy	Asst. Prof. Dr. Adel Ahmed Al-Shakiri	Assoc. Prof. Dr. Mohammad Algorafi	Prof. Dr. Mohammed AL-Bukhaiti	Assoc. Prof. Dr. Huda Al-Emad

Rector of Sana'a University
Prof. Dr. Al-Qassim Mohammed Abbas

a2- Explain the objectives of information security and discuss the importance and applications of confidentiality, integrity, and availability.	▪ Lectures, ▪ Tutorial, ▪ Laboratory work, ▪ Projects, ▪ Use of communication and information technology	▪ Examinations, ▪ Homework presentations, ▪ Individual and group project reports

(B) Alignment Course Intended Learning Outcomes of Intellectual Skills to Teaching Strategies and Assessment Strategies:		
Course Intended Learning Outcomes	Teaching strategies	Assessment Strategies
b1- Formulate the application of some encryption/decryption protocols including AES, DES, SSL, RSA, and IPSec to solve information and network security systems.	▪ Lectures, ▪ Tutorial, ▪ Laboratory work, ▪ Seminars, ▪ Group work, ▪ Projects, ▪ Use of communication and information technology	▪ Examinations, ▪ Homework, ▪ Laboratory reports Presentations, ▪ Individual and group project reports, ▪ Assignments

© Alignment Course Intended Learning Outcomes of Professional and Practical Skills to Teaching Strategies and Assessment Strategies:		
Course Intended Learning Outcomes	Teaching strategies	Assessment Strategies
c1- Apply concepts of public keys, private keys, cryptosystem, authentication, and digital signatures to secure simple information systems.	▪ Lectures, ▪ Tutorial, ▪ Laboratory work, ▪ Seminars, ▪ Group work,	▪ Examinations, ▪ Homework, ▪ Laboratory reports Presentations,

Prepared by	Head of Department	Quality Assurance Unit	Dean of the Faculty	Academic Development Center & Quality Assurance
Assoc. Prof. Dr. Farouk AL-Fuhaidy	Asst. Prof. Dr. Adel Ahmed Al-Shakiri	Assoc. Prof. Dr. Mohammad Algorafi	Prof. Dr. Mohammed AL-Bukhaiti	Assoc. Prof. Dr. Huda Al-Emad

Rector of Sana'a University
Prof. Dr. Al-Qassim Mohammed Abbas

		▪ Projects, ▪ Use of communication and information technology	▪ Individual and group project reports, ▪ Assignments
c2-	Implement network security protocols such as SSL and MAC, Web security, WEP and computer viruses and Internet attacks, and apply them in real applications to secure internet traffic using information and programming skills.	▪ Lectures, ▪ Tutorial, ▪ Laboratory work, ▪ Seminars, ▪ Group work, ▪ Projects, ▪ Use of communication and information technology	▪ Examinations, ▪ Homework, ▪ Laboratory reports Presentations, ▪ Individual and group project reports, ▪ Assignments

(D) Alignment Course Intended Learning Outcomes of Transferable Skills to Teaching Strategies and Assessment Strategies:

Course Intended Learning Outcomes		Teaching strategies	Assessment Strategies
d1-	function effectively within teams to accomplish a common goal.	▪ Seminars, ▪ Laboratory, ▪ Assignments, ▪ Projects ▪ Use of communication and information technology.	▪ Presentations, ▪ Individual and Group ▪ Project Reports

Prepared by	Head of Department	Quality Assurance Unit	Dean of the Faculty	Academic Development Center & Quality Assurance
Assoc. Prof. Dr. Farouk AL-Fuhaidy	Asst. Prof. Dr. Adel Ahmed Al-Shakiri	Assoc. Prof. Dr. Mohammad Algorafi	Prof. Dr. Mohammed AL-Bukhaiti	Assoc. Prof. Dr. Huda Al-Emad

Rector of Sana'a University
Prof. Dr. Al-Qassim Mohammed Abbas

IV. Course Content:

A – Theoretical Aspect:

Order	Units/Topics List	Learning Outcomes	Sub Topics List	Number of Weeks	Contact hours
1.	Course Orientations & Introduction to Information and Networks Security	a1, a2, b1	- Course Orientations, Introduction to Information & Networks Security, History of information security, what is security? CNSS Security Model, Security systems development life cycles, security professionals and organization, the need, importance and applications, business needs first, - Security threats, attacks, - Security Goals, Confidentiality, Authentications, Reliability, Integrity, and Availability, - Security functions and mechanisms, - Introduction to Computer, Networks, and WEB systems Security	1	2

Prepared by	Head of Department	Quality Assurance Unit	Dean of the Faculty	Academic Development Center & Quality Assurance
Assoc. Prof. Dr. Farouk AL-Fuhaidy	Asst. Prof. Dr. Adel Ahmed Al-Shakiri	Assoc. Prof. Dr. Mohammad Algorafi	Prof. Dr. Mohammed AL-Bukhaiti	Assoc. Prof. Dr. Huda Al-Emad

Rector of Sana'a University
Prof. Dr. Al-Qassim Mohammed Abbas

2.	Classical Symmetric Encryption/Decryption Techniques	a1, a2, c1	- Passive and Active Attacks work behaviors, Potential Threats, Risks, and Breaches, Cryptography & Cryptanalysis Definition, Access Control - Classical Encryption/ Decryption Algorithms, Symmetric Cipher Model, Simple XOR Enc/Dec., Substitution & Transposition Techniques, Rotor machine, and Stenography.	2	4
3.	Data Symmetric Block Ciphers, the Data Encryption Standard (DES)	a1, a2, b1, c1	- Block Cipher Principles, - The DES Structure, the strength of DES, Differential & Linear Cryptanalysis, S-Box, Substitutions & Permutations - Block Cipher Design Principles using DES.	2	4
4.	Advanced Symmetric Encryption Standard (AES) and More on Symmetric Ciphers	a1, a2, b1, c1	- Evaluation Criteria for AES, - The AES Cipher, - Multiple Encryption and Triple DES, - Traffic Confidentiality, - Key Distribution and Random Number Generation	2	4

Prepared by	Head of Department	Quality Assurance Unit	Dean of the Faculty	Academic Development Center & Quality Assurance
Assoc. Prof. Dr. Farouk AL-Fuhaidy	Asst. Prof. Dr. Adel Ahmed Al-Shakiri	Assoc. Prof. Dr. Mohammad Algorafi	Prof. Dr. Mohammed AL-Bukhaiti	Assoc. Prof. Dr. Huda Al-Emad

Rector of Sana'a University
Prof. Dr. Al-Qassim Mohammed Abbas

			- Using of Stream Cipher, RC4 & A5/1		
5.	Mathematics of Cryptography and Public-Key Encryption & Hash Function	a1, a2, b1	- Finite Fields, Groups, Rings, and Fields. Modular Arithmetic, The Euclidean algorithm - The Finite Field of the form GF(p), Polynomial Arithmetic and GF(2n). - Prime Numbers, - Fermat's & Euler's Theorems - The Chinese Reminder Theorem and Discrete Logarithms.	1,5	3
6.	Asymmetric-Key Cryptography, Public-Key Encryption, RSA algorithm and Others	a1, a2, b1, c1	- Principles of Public-Key Cryptosystems, - The RSA Algorithm, - Key Management, - Diffie-Hellman Key Exchange	1,5	3
7.	Message Authentication and Hash Functions	a1, a2, b1, c1	- Authentication Requirements, - Authentication Functions - Security of Hash Functions & MAC - Digital Signatures Standards & Authentication	1	2
8.	Network, Transport, and Application, Layers Security	a1, a2, b1, c1, d1	- IPSec, Overview, Architecture, Header	1,5	3

Prepared by	Head of Department	Quality Assurance Unit	Dean of the Faculty	Academic Development Center & Quality Assurance
Assoc. Prof. Dr. Farouk AL-Fuhaidy	Asst. Prof. Dr. Adel Ahmed Al-Shakiri	Assoc. Prof. Dr. Mohammad Algorafi	Prof. Dr. Mohammed AL-Bukhaiti	Assoc. Prof. Dr. Huda Al-Emad

Rector of Sana'a University
Prof. Dr. Al-Qassim Mohammed Abbas

			Authentication and Encapsulation Security - SSL Architecture, Message Format, and Security - Introduction to E-mail Structure and Security		
9.	Web and System Security	a1, a2, b1, c1, d1	- Introduction to Web Security Considerations, Secure Socket and Transport Layer Sec. - Intruders and their detections, - Malicious Software, Virus and Threats, Distributed Denial of Service attacks - Introduction to Firewall Design Principles and Trusted Systems	1,5	3
Number of Weeks /and Units Per Semester				**14**	**28**

B - Tutorial Aspect:

Order	Tasks/ Experiments	Number of Weeks	contact hours	Learning Outcomes
1.	- Introduction: Security Concepts, Confidentiality, Integrity, Authentication, Availability, - Threats and attacks	1st	2	a1, a2
2.	Examples demonstrating Classical Encryption Algorithms like Logic XOR, CASER diagraph, Playfair, and other Stenography Techniques	3rd	2	a1, a2, c1

Prepared by	Head of Department	Quality Assurance Unit	Dean of the Faculty	Academic Development Center & Quality Assurance
Assoc. Prof. Dr. Farouk AL-Fuhaidy	Asst. Prof. Dr. Adel Ahmed Al-Shakiri	Assoc. Prof. Dr. Mohammad Algorafi	Prof. Dr. Mohammed AL-Bukhaiti	Assoc. Prof. Dr. Huda Al-Emad

Rector of Sana'a University
Prof. Dr. Al-Qassim Mohammed Abbas

3.	Examples on DES and AES Algorithms	5th and 7th	4	a1, a2, b1, c1
4.	Examples on Public Key, Hash and RSA Algorithms and SSL and IPSec Protocols	9th & 11th	4	a1, a2, b1, c1
5.	System & Web security protocols, WPA, WEP	13th	2	a1, a2, b1, c1
Number of Weeks /and Units Per Semester		**7**	**14**	

C - Practical Aspect:

Order	Tasks/ Experiments	Number of Weeks	contact hours	Learning Outcomes
1.	Review on Programming using Java or C#	2nd	2	c2, d1
2.	Implementing using Programming variant Traditional Encryption/Decryption Algorithms like, XOR logic operation, CASER, Row Shifting for letters, Matrix Permutation and other Techniques (students distributed in small groups of 2 or 3 students and each group implement such different technique)	4th & 6th	4	a1, a2, c1, c2, d1
3.	Students in groups working for implementation of different Network and Information Enc/Dec Algorithms Like DES, AES, Public Key, Hash and RSA Algorithms	8th, 10th, 12th	6	a1, a2, b1, c1, c2, d1
4.	Students in groups present and discuss their projects	14th	2	a1, a2, b1, c1, c2, d1
Number of Weeks /and Units Per Semester		**7**	**14**	

Prepared by	Head of Department	Quality Assurance Unit	Dean of the Faculty	Academic Development Center & Quality Assurance
Assoc. Prof. Dr. Farouk AL-Fuhaidy	Asst. Prof. Dr. Adel Ahmed Al-Shakiri	Assoc. Prof. Dr. Mohammad Algorafi	Prof. Dr. Mohammed AL-Bukhaiti	Assoc. Prof. Dr. Huda Al-Emad

Rector of Sana'a University
Prof. Dr. Al-Qassim Mohammed Abbas

V. Teaching strategies of the course:

- Active Lectures,
- Tutorial,
- Laboratory,
- Projects works,
- Use of Communication and Information Technology.
- Seminars,
- Small group
- Group work,

VI. Assignments:

No	Assignments	Aligned CILOs(symbols)	Week Due	Mark
1.	Classical Encryption Techniques	a1, a2, c1, c2	3rd	3
2.	Symmetric Data Ciphers, DES & AES	a1, a2, b1, c1, c2, d1	5th to 7th	4.5
3.	Asymmetric, Hash, RSA, and Public-Key Ciphers	a1, a2, b1, c1, c2, d1	9th to 12th	4.5
4.	SSL, IPSec and Web	a1, a2, b1, c1, c2, d1	14th	3
	Total			**15**

VII. Schedule of Assessment Tasks for Students During the Semester:

No.	Assessment Method	Week Due	Mark	Proportion of Final Assessment	Aligned Course Learning Outcomes
1.	Assignments	3rd to 13th	15	10%	a1, a2, b1, c1, c2, d1
2.	Laboratory Work & Reports	4th to 12th	15	10%	a1, a2, b1, c1, c2, d1

Prepared by	Head of Department	Quality Assurance Unit	Dean of the Faculty	Academic Development Center & Quality Assurance
Assoc. Prof. Dr. Farouk AL-Fuhaidy	Asst. Prof. Dr. Adel Ahmed Al-Shakiri	Assoc. Prof. Dr. Mohammad Algorafi	Prof. Dr. Mohammed AL-Bukhaiti	Assoc. Prof. Dr. Huda Al-Emad

Rector of Sana'a University
Prof. Dr. Al-Qassim Mohammed Abbas

3.	Project Presentation	14th	15	10%	a1, a2, b1, c1, c2, d1
4.	Mid-Term Exam (Theoretically)	8th	22.5	15%	a1, a2, b1, c1
5.	Participation	ALL	7.5	5%	a1, a2, b1, c1, d1
6.	Final Exam (Theoretically)	16th	75	50%	a1, a2, b1, c1
	Total		**150**	**100%**	

VIII. Learning Resources:

- *Written in the following order: (Author - Year of publication – Title – Edition – Place of publication – Publisher).*

1- Required Textbook(s) (maximum two).

1- W. Stallings- 2013 - Cryptography and Network Security: Principles and Practice, Six Edition Prentice Hall.
2- Behrouz A. Frouzan- 2008 - Cryptography and Network Security- Special Indian Edittion- McGraw-Hill Companies, Inc, NewYork.
3- Michael E. Whitman, Herbert J. Mattord- 2013- Principles of information security, Cengage Learning,.

2- Essential References.

1. Michael E. Whitman and Herbert J. Mattord- January 19, 2010- Management of Information Security Course Technology- 3rd edition, ISBN-10: 1435488849, ISBN-13: 978-1435488847
2. Charles P. Pfleeger and Shari Lawrence Pfleeger- 2006- Security in Computing- 4th Edition, ISBN 978-0132390774- Prentice Hall.

3- Electronic Materials and Web Sites *etc*.

1. www.iacr.org
2. www.iit.edu

Prepared by	Head of Department	Quality Assurance Unit	Dean of the Faculty	Academic Development Center & Quality Assurance
Assoc. Prof. Dr. Farouk AL-Fuhaidy	Asst. Prof. Dr. Adel Ahmed Al-Shakiri	Assoc. Prof. Dr. Mohammad Algorafi	Prof. Dr. Mohammed AL-Bukhaiti	Assoc. Prof. Dr. Huda Al-Emad

Rector of Sana'a University
Prof. Dr. Al-Qassim Mohammed Abbas

IX. Course Policies:	
1.	**Class Attendance:** A student should attend not less than 75 % of total hours of the subject; otherwise he will not be able to take the exam and will be considered as exam failure. If the student is absent due to illness, he/she should bring a proof statement from university Clinic
2.	**Tardy:** For late in attending the class, the student will be initially notified. If he repeated lateness in attending class he will be considered as absent.
3.	**Exam Attendance/Punctuality:** A student should attend the exam on time. He is Permitted to attend an exam half one hour from exam beginning, after that he/she will not be permitted to take the exam and he/she will be considered as absent in exam-
4.	**Assignments & Projects:** The assignment is given to the students after each chapter; the student has to submit all the assignments for checking on time-
5.	**Cheating:** For cheating in exam, a student will be considered as fail. In case the cheating is repeated three times during his/her study the student will be disengaged from the Faculty-
6.	**Plagiarism**: Plagiarism is the attending of a student the exam of a course instead of another student. If the examination committee proofed a plagiarism of a student, he will be disengaged from the Faculty. The final disengagement of the student from the Faculty should be confirmed from the Student Council Affair of the university.
7.	**Other policies:** - Mobile phones are not allowed to use during a class lecture. It must be closed, otherwise the student will be asked to leave the lecture room - Mobile phones are not allowed in class during the examination. Lecture notes and assignments my given directly to students using soft or hard copy

Prepared by	Head of Department	Quality Assurance Unit	Dean of the Faculty	Academic Development Center & Quality Assurance
Assoc. Prof. Dr. Farouk AL-Fuhaidy	Asst. Prof. Dr. Adel Ahmed Al-Shakiri	Assoc. Prof. Dr. Mohammad Algorafi	Prof. Dr. Mohammed AL-Bukhaiti	Assoc. Prof. Dr. Huda Al-Emad

Rector of Sana'a University
Prof. Dr. Al-Qassim Mohammed Abbas

University of Sana'a
Faculty of Engineering
Department: Electrical Engineering
Title of the Program: Communication Engineering and Networks

Reviewed By	**Vice Dean for Academic Affairs and Post Graduate Studies: Asst. Prof. Dr. Tarek A. Barakat** **President of Quality Assurance Unit: Assoc. Prof. Dr. Mohammed Algorafi** **Name of Reviewer from the Department: Asst. Prof. Dr. Nasser H. Almofari**
	Deputy Rector for Academic Affairs Asst. Prof. Dr. Ibrahim AlMutaa **Assoc. Prof. Dr. Ahmed Mujahed** **Asst. Prof. Dr. Munasar Alsubri**

Prepared by	Head of Department	Quality Assurance Unit	Dean of the Faculty	Academic Development Center & Quality Assurance
Assoc. Prof. Dr. Farouk AL-Fuhaidy	Asst. Prof. Dr. Adel Ahmed Al-Shakiri	Assoc. Prof. Dr. Mohammad Algorafi	Prof. Dr. Mohammed AL-Bukhaiti	Assoc. Prof. Dr. Huda Al-Emad

Rector of Sana'a University
Prof. Dr. Al-Qassim Mohammed Abbas

University of Sana'a
Faculty of Engineering
Department: Electrical Engineering
Title of the Program: Communication Engineering and Networks

Course Plan (Syllabus) of Information and Network Security

I. Information about Faculty Member Responsible for the Course:

Name of Faculty Member	Assoc. Prof. Dr. Farouk AL-Fuhaidy	**Office Hours**					
Location& Telephone No.	777909815	**SAT**	**SUN**	**MON**	**TUE**	**WED**	**THU**
E-mail	farouqakh@gmail.com						

II. Course Identification and General Information:

1-	Course Title:	Information and Network Security				
2-	Course Number & Code:	CNE445				
3-	Credit hours:	C.H				Total
		Th.	Tu.	Pr.	Tr.	
		2	-	1	1	3
4-	Study level/year at which this course is offered:	Fifth Level/ First Semester				
5-	Pre –requisite (if any):	Programming Language 2 (C/C++) (CCE152)				
6-	Co –requisite (if any):	None.				
7-	Program (s) in which the course is offered	(Communication Engineering and Networks) and (Computer & Control)				
8-	Language of teaching the course:	English				
9-	System of Study:	Semester				
10-	Mode of delivery:	Weekly Lectures, Tut. And Lab.				
11-	Location of teaching the course:	Electrical Eng. Dept.				

Prepared by	Head of Department	Quality Assurance Unit	Dean of the Faculty	Academic Development Center & Quality Assurance
Assoc. Prof. Dr. Farouk AL-Fuhaidy	Asst. Prof. Dr. Adel Ahmed Al-Shakiri	Assoc. Prof. Dr. Mohammad Algorafi	Prof. Dr. Mohammed AL-Bukhaiti	Assoc. Prof. Dr. Huda Al-Emad

Rector of Sana'a University
Prof. Dr. Al-Qassim Mohammed Abbas

III. Course Description:

This is an introductory course to the information and network security, to make students familiar with the basic concepts of information and network systems security and mechanisms. The course aims to the security goals, security functions, and security mechanisms. The course will cover various topics related to computer & network security, introduction to information security, information and network security and risk management, access control, security architecture and design, data privacy, telecommunications and network protection against various attacks. The course is supported with variant examples introduced by tutorial and laboratory works.

IV. Intended learning outcomes (ILOs) of the course:

- Brief summary of the knowledge or skill the course is intended to develop**:**

1- Demonstrate an understanding of basic categories of threats and attacks, encryption/decryption algorithms, public/private keys, and authentication related to information and networks.
2- Explain the objectives of information security and discuss the importance and applications of confidentiality, integrity, and availability.
3- Formulate the application of some encryption/decryption protocols including AES, DES, SSL, RSA, and IPSec to solve information and network security systems.
4- Apply concepts of public keys, private keys, cryptosystem, authentication, and digital signatures to secure simple information systems.
5- Implement network security protocols such as SSL and MAC, Web security, WEP and computer viruses and Internet attacks, and apply them in real applications to secure internet traffic using information and programming skills.
6- function effectively within teams to accomplish a common goal.

Prepared by	Head of Department	Quality Assurance Unit	Dean of the Faculty	Academic Development Center & Quality Assurance
Assoc. Prof. Dr. Farouk AL-Fuhaidy	Asst. Prof. Dr. Adel Ahmed Al-Shakiri	Assoc. Prof. Dr. Mohammad Algorafi	Prof. Dr. Mohammed AL-Bukhaiti	Assoc. Prof. Dr. Huda Al-Emad

Rector of Sana'a University
Prof. Dr. Al-Qassim Mohammed Abbas

V. Course Content:

A – Theoretical Aspect:

Order	Units/Topics List	Sub Topics List	Number of Weeks	Contact hours
1.	Course Orientations & Introduction to Information and Networks Security	- Course Orientations, Introduction to Information & Networks Security, History of information security, what is security? CNSS Security Model, Security systems development life cycles, security professionals and organization, the need, importance and applications, business needs first, - Security threats, attacks, - Security Goals, Confidentiality, Authentications, Reliability, Integrity, and Availability, - Security functions and mechanisms, - Introduction to Computer, Networks, and WEB systems Security	1st	2
2.	Classical Symmetric Encryption/Decryption Techniques	- Passive and Active Attacks work behaviors, Potential Threats, Risks, and Breaches, Cryptography & Cryptanalysis Definition, Access Control - Classical Encryption/ Decryption Algorithms, Symmetric Cipher Model, Simple XOR Enc/Dec., Substitution &	2nd ,3rd	4

Prepared by	Head of Department	Quality Assurance Unit	Dean of the Faculty	Academic Development Center & Quality Assurance
Assoc. Prof. Dr. Farouk AL-Fuhaidy	Asst. Prof. Dr. Adel Ahmed Al-Shakiri	Assoc. Prof. Dr. Mohammad Algorafi	Prof. Dr. Mohammed AL-Bukhaiti	Assoc. Prof. Dr. Huda Al-Emad

Rector of Sana'a University
Prof. Dr. Al-Qassim Mohammed Abbas

		Transposition Techniques, Rotor machine, and Stenography.		
3.	Data Symmetric Block Ciphers, the Data Encryption Standard (DES)	- Block Cipher Principles, - The DES Structure, the strength of DES, Differential & Linear Cryptanalysis, S-Box, Substitutions & Permutations - Block Cipher Design Principles using DES.	4^{th} ,5^{th}	4
4.	Advanced Symmetric Encryption Standard (AES) and More on Symmetric Ciphers	- Evaluation Criteria for AES, - The AES Cipher, - Multiple Encryption and Triple DES, - Traffic Confidentiality, - Key Distribution and Random Number Generation - Using of Stream Cipher, RC4 & A5/1	6^{th} ,7^{th}	4
5.	Mid-Term Exam	- All Prev. Topics	8^{th}	2
6.	Mathematics of Cryptography and Public-Key Encryption & Hash Function	- Finite Fields, Groups, Rings, and Fields. Modular Arithmetic, The Euclidean algorithm - The Finite Field of the form GF(p), Polynomial Arithmetic and GF(2n). - Prime Numbers, - Fermat's & Euler's Theorems - The Chinese Reminder Theorem and Discrete Logarithms.	9^{th} ,10^{th}	3
7.	Asymmetric-Key Cryptography, Public-	- Principles of Public-Key Cryptosystems, - The RSA Algorithm,	10^{th} ,11^{th}	3

Prepared by	Head of Department	Quality Assurance Unit	Dean of the Faculty	Academic Development Center & Quality Assurance
Assoc. Prof. Dr. Farouk AL-Fuhaidy	Asst. Prof. Dr. Adel Ahmed Al-Shakiri	Assoc. Prof. Dr. Mohammad Algorafi	Prof. Dr. Mohammed AL-Bukhaiti	Assoc. Prof. Dr. Huda Al-Emad

Rector of Sana'a University
Prof. Dr. Al-Qassim Mohammed Abbas

	Key Encryption, RSA algorithm and Others	- Key Management, - Diffie-Hellman Key Exchange		
8.	Message Authentication and Hash Functions	- Authentication Requirements, - Authentication Functions - Security of Hash Functions & MAC - Digital Signatures Standards & Authentication	12th	2
9.	Network, Transport, and Application, Layers Security	- IPSec, Overview, Architecture, Header Authentication and Encapsulation Security - SSL Architecture, Message Format, and Security - Introduction to E-mail Structure and Security	13th ,14th	3
10.	Web and System Security	- Introduction to Web Security Considerations, Secure Socket and Transport Layer Sec. - Intruders and their detections, - Malicious Software, Virus and Threats, Distributed Denial of Service attacks - Introduction to Firewall Design Principles and Trusted Systems	14th ,15th	3
11.	Final Exam	- All Topics	16th	2
Number of Weeks /and Units Per Semester			**16**	**32**

Prepared by	Head of Department	Quality Assurance Unit	Dean of the Faculty	Academic Development Center & Quality Assurance
Assoc. Prof. Dr. Farouk AL-Fuhaidy	Asst. Prof. Dr. Adel Ahmed Al-Shakiri	Assoc. Prof. Dr. Mohammad Algorafi	Prof. Dr. Mohammed AL-Bukhaiti	Assoc. Prof. Dr. Huda Al-Emad

Rector of Sana'a University
Prof. Dr. Al-Qassim Mohammed Abbas

B - Tutorial Aspect:				
Order	**Tasks/ Experiments**	**Number of Weeks**	**Contact hours**	**Learning Outcomes**
1.	Introduction: Security Concepts, Confidentiality, Integrity, Authentication, Availability, Threats and attacks	1st	2	a1, a2
2.	Examples demonstrating Classical Encryption Algorithms like Logic XOR, CASER diagraph, Playfair, and other Stenography Techniques	3rd	2	a1, a2, c1
3.	Examples on DES and AES Algorithms	5th and 7th	4	a1, a2, b1, c1
4.	Examples on Public Key, Hash and RSA Algorithms and SSL and IPSec Protocols	9th & 11th	4	a1, a2, b1, c1
5.	System & Web security protocols, WPA, WEP	13th	2	a1, a2, b1, c1
Number of Weeks /and Units Per Semester		**7**	**14**	

C - Practical Aspect:			
Order	**Tasks/ Experiments**	**Number of Weeks**	**Contact hours**
1.	Review on Programming using Java or C#	2nd	2
2.	Implementing using Programming variant Traditional Encryption/Decryption Algorithms like, XOR logic operation, CASER, Row Shifting for letters, Matrix Permutation and other Techniques (students distributed in small groups of 2 or 3 students and each group implement such different technique)	4th & 6th	4
3.	Students in groups working for implementation of different Network and Information Enc/Dec Algorithms Like DES, AES, Public Key, Hash and RSA Algorithms	8th, 10th, 12th	6

Prepared by	Head of Department	Quality Assurance Unit	Dean of the Faculty	Academic Development Center & Quality Assurance
Assoc. Prof. Dr. Farouk AL-Fuhaidy	Asst. Prof. Dr. Adel Ahmed Al-Shakiri	Assoc. Prof. Dr. Mohammad Algorafi	Prof. Dr. Mohammed AL-Bukhaiti	Assoc. Prof. Dr. Huda Al-Emad

Rector of Sana'a University
Prof. Dr. Al-Qassim Mohammed Abbas

4.	Students in groups present and discuss their projects	14th	2
Number of Weeks /and Units Per Semester		**7**	**14**

VI. Teaching strategies of the course:

- Active Lectures,
- Tutorial,
- Laboratory,
- Projects works,
- Use of Communication and Information Technology.
- Seminars
- Small group
- Group work

VII. Assignments:

No	Assignments	Week Due	Mark
1.	Classical Encryption Techniques	3rd	3
2.	Symmetric Data Ciphers, DES & AES	5th to 7th	4.5
3.	Asymmetric, Hash, RSA, and Public-Key Ciphers	9th to 12th	4.5
4.	SSL, IPSec and Web	14th	3
	Total		**15**

VIII. Schedule of Assessment Tasks for Students During the Semester:

No.	Assessment Method	Week Due	Mark	Proportion of Final Assessment
1.	Assignments	3rd to 13th	15	10%
2.	Laboratory Work & Reports	4th to 12th	15	10%
3.	Project Presentation	14th	15	10%

Prepared by	Head of Department	Quality Assurance Unit	Dean of the Faculty	Academic Development Center & Quality Assurance
Assoc. Prof. Dr. Farouk AL-Fuhaidy	Asst. Prof. Dr. Adel Ahmed Al-Shakiri	Assoc. Prof. Dr. Mohammad Algorafi	Prof. Dr. Mohammed AL-Bukhaiti	Assoc. Prof. Dr. Huda Al-Emad

Rector of Sana'a University
Prof. Dr. Al-Qassim Mohammed Abbas

4.	Mid-Term Exam (Theoretically)	8th	22.5	15%
5.	Attendance & Participation	ALL	7.5	5%
6.	Final Exam (Theoretically)	16th	75	50%
	Total		**150**	**100%**

IX. Learning Resources:

- *Written in the following order: (Author - Year of publication – Title – Edition – Place of publication – Publisher).*

1- Required Textbook(s) (maximum two).

1- William. Stallings- 2013 - Cryptography and Network Security: Principles and Practice, Six Edition Prentice Hall.
2- Behrouz A. Frouzan- 2008 - Cryptography and Network Security- Special Indian Edittion- McGraw-Hill Companies, Inc, NewYork.
3- Michael E. Whitman, Herbert J. Mattord- 2013- Principles of information security, Cengage Learning,.

2- Essential References.

1- Michael E. Whitman and Herbert J. Mattord- January 19, 2010- Management of Information Security Course Technology- 3rd edition, ISBN-10: 1435488849, ISBN-13: 978-1435488847
2- Charles P. Pfleeger and Shari Lawrence Pfleeger- 2006- Security in Computing- 4th Edition, ISBN 978-0132390774- Prentice Hall.

3- Electronic Materials and Web Sites *etc*.

1- www.iacr.org
2- www.iit.edu

X. Course Policies:

1.	**Class Attendance:** A student should attend not less than 75 % of total hours of the subject; otherwise he will not be able to take the exam and will be considered as exam failure. If the student is absent due to illness, he/she should bring a proof statement from university Clinic
2.	**Tardy:**

Prepared by	Head of Department	Quality Assurance Unit	Dean of the Faculty	Academic Development Center & Quality Assurance
Assoc. Prof. Dr. Farouk AL-Fuhaidy	Asst. Prof. Dr. Adel Ahmed Al-Shakiri	Assoc. Prof. Dr. Mohammad Algorafi	Prof. Dr. Mohammed AL-Bukhaiti	Assoc. Prof. Dr. Huda Al-Emad

Rector of Sana'a University
Prof. Dr. Al-Qassim Mohammed Abbas

	For late in attending the class, the student will be initially notified. If he repeated lateness in attending class he will be considered as absent.
3.	**Exam Attendance/Punctuality:** A student should attend the exam on time. He is Permitted to attend an exam half one hour from exam beginning, after that he/she will not be permitted to take the exam and he/she will be considered as absent in exam-
4.	**Assignments & Projects:** The assignment is given to the students after each chapter; the student has to submit all the assignments for checking on time-
5.	**Cheating:** For cheating in exam, a student will be considered as fail. In case the cheating is repeated three times during his/her study the student will be disengaged from the Faculty-
6.	**Plagiarism**: Plagiarism is the attending of a student the exam of a course instead of another student. If the examination committee proofed a plagiarism of a student, he will be disengaged from the Faculty. The final disengagement of the student from the Faculty should be confirmed from the Student Council Affair of the university.
7.	**Other policies:** - Mobile phones are not allowed to use during a class lecture. It must be closed, otherwise the student will be asked to leave the lecture room - Mobile phones are not allowed in class during the examination. Lecture notes and assignments my given directly to students using soft or hard copy

Prepared by	Head of Department	Quality Assurance Unit	Dean of the Faculty	Academic Development Center & Quality Assurance
Assoc. Prof. Dr. Farouk AL-Fuhaidy	Asst. Prof. Dr. Adel Ahmed Al-Shakiri	Assoc. Prof. Dr. Mohammad Algorafi	Prof. Dr. Mohammed AL-Bukhaiti	Assoc. Prof. Dr. Huda Al-Emad

Rector of Sana'a University
Prof. Dr. Al-Qassim Mohammed Abbas