Andlus UNIVERSITY

FACULTY INFORMATION TECHNOLOGY

Quality Assurance Unit (QUA)

DEPARTMENT OF Information Technology

PROGRAM INFORMATION TECHNOLOGY

Course Specification of   Information Security

Semester 1 last year

2014

University of Andlus

Faculty of Information Technology

Department: Information Technology

Title of the Program: PIT in Information Technology

Template for Course Specification

I. Course Identification and General Information:

<table>
<tr><td>1</td><td>**Course Title:**</td><td colspan="5">**Advance Information Security**</td></tr>
<tr><td>2</td><td>**Course Code &Number:**</td><td colspan="5"></td></tr>
<tr><td rowspan="3">3</td><td rowspan="3">**Credit hours: 3**</td><td colspan="4">C.H</td><td rowspan="2">TOTAL</td></tr>
<tr><td>Th.</td><td>Seminar</td><td>Pr</td><td>Tr.</td></tr>
<tr><td>*2*</td><td></td><td>*2*</td><td></td><td>*4*</td></tr>
<tr><td>4</td><td>**Study level/semester at which this course is offered:**</td><td colspan="5">*First year semester 2*</td></tr>
<tr><td>5</td><td>**Pre –requisite (if any):**</td><td colspan="5">**Information Security**</td></tr>
<tr><td>6</td><td>**Co –requisite (if any):**</td><td colspan="5"></td></tr>
<tr><td>7</td><td>**Program (s) in which the course is offered:**</td><td colspan="5">Information **Technology**</td></tr>
<tr><td>8</td><td>**Language of teaching the course:**</td><td colspan="5">**English and Arabic**</td></tr>
<tr><td>9</td><td>**Location of teaching the course:**</td><td colspan="5">**Class**</td></tr>
<tr><td>10</td><td>**Prepared By:**</td><td colspan="5">**D/ Saleh Alasali**</td></tr>
<tr><td>11</td><td>**Date of Approval**</td><td colspan="5"></td></tr>
</table>

II. Course Description:

This course introduce to the students the science and study of methods of data protection computer and communication systems from unauthorized disclosure and modification, to show how to develop techniques for verification, identification, key safeguarding schemes and key distribution protocols and to introduce students to different methods of encrypting data for security purposes.

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

This course aims to student acquire the:

1. Understand the basic rules of protection to computer and information. A1
2. Understand the science theory of information protection. A2
3. Use the basics rules of protection to protect computer and information. B1
4. Use the science theories to protect information. B2
5. Use the science theory along with the suitable computer languages to build some encryption/decryption programs. C1
6. Analysis different techniques of information protection. C2
7. Select suitable security system for an organization. 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- Understand the basic rules of protection to computer and information	Lectures	**Exams**
A2- Understand the science theory of information protection	Lectures	**Exams**

(B) Alignment Course Intended Learning Outcomes of Intellectual Skills to Teaching Strategies and Assessment Strategies:

Course Intended Learning Outcomes	Teaching strategies	Assessment Strategies
B1- Use basics rules of protection to protect computer and information	Lectures	**Exams**
B2- Use the science theories to protect information.	Lectures	**Exams**

(C) 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- Use the science theories along with the suitable computer languages to build some encryption/decryption programs.	Lectures and simulation	Project and Exams
C2- Analysis different techniques of information protection	Project	**Seminars**

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

Course Intended Learning Outcomes	Teaching strategies	Assessment Strategies
D1- Select the suitable security system for an organization	Project	**Seminars**

IV. Course Content:

A – Theoretical Aspect:

Order	Units/Topics List	Learning Outcomes	Sub Topics List	Number of Weeks	contact hours
1	Life and Information	A .B	The concept of Information , the main resources of Information , the aspects , factors of security	2	6
2	The concept of integrity	A,B,C	The concept of integrity using CRC and Hamming methods	2	6
3	The concept of cyphers , the old cyphers	A,B,C	The concept of cyphers, Caesar, Veginner, Playfare and transposition cyphers. linear, nonlinear functions, random numbers and random numbers generator algorithms	3	9
4	The new cyphers	A ,B,C	Block cyphering SDES and DES algorithms	3	9
4	Infrastructure of public key, RAS, algorithms	A ,B,C	Modular arithmetic operations, GCD of two numbers and algorithm to generate GCD of two numbers, RAS, algorithms	2	9
5	Authentication using Hash function and Digital signature	A ,B,C.D	Hash functions and Digital signature.	2	3
Number of Weeks /and Units Per Semester				**14**	**42**

V. Teaching strategies of the course:

Lectures and simulations

VI. Assignments:

No	Assignments	Aligned CILOs(symbols)	Week Due	Mark
1	Program to generate CRC of an electronic document.	A,B,C	3	5
2	Program to generate Caesar, Veginner, Playfare and transposition cyphers.	A,B,C	5	5

3	Program to construct substitutions boxes in DES algorithm	A,B,C,D	7	5
4	Programs to construct session and Public keys	A,B,C,D	13	5

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	Program to generate CRC of an electronic document.	3	5	5%	A,B,C
2	Program to generate Caesar, Veginner, Playfare and transposition cyphers.	5	5	5%	A,B,C
3	Program to construct substitutions boxes in DES algorithm	7	5	5%	A,B,C,D
4	Programs to construct session and Public keys	13	5	5%	A,B,C,D

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− William Stallings (2003) “Cryptography and Network Security: Principles and Practice” 3rd Edn. India Reprint. Agrawal-M IETE-Technical-Review.

2− Bruce Schneier (2006) “Applied Cryptography” 4nd Edition John Wiley & Sons. (ASIA) Pvt. Ltd., Clementi Loop # 02-01, Singapore 129809.

2- Essential References.

1. David M. Burton (2005) “Elementary Number Theory” 2nd Edition Universal Book Stall New Delhi India.

2. Douglasr. Stinson (2010) “Cryptography: Theory and Practice” Department of Combinatory and Optimization University of Waterloo, Waterloo, Ontario Canada. 2nd Edition, Chapman & Hall/CRC.

3. Bruce Schneier (2006) “Applied Cryptography” 4nd Edition John Wiley & Sons. (ASIA) Pvt. Ltd., Clementi Loop # 02-01, Singapore 129809.

4. Deborah Russell and G. T. Gangemi Sr (2001) “ Computer Security Basics” O’Reilly & Associates, Inc., New York

IX. Course Policies:

1	**Class Attendance:** -
2	**Tardy:** -
3	**Exam Attendance/Punctuality:** -
4	**Assignments & Projects:** -
5	**Cheating:** -
6	**Plagiarism:**
7	**Other policies:** -

Template for Course Plan (Syllabus)

I. - Information about Faculty Member Responsible for the Course:

		Office Hours					
Name of Faculty Member							
Location&Telephone No.		SAT	SUN	MON	TUE	WED	THU
E-mail							

II. Course Identification and General Information:

1	Course Title:	Information Security				
2	Course Number & Code:					
3	Credit hours: 3	C.H				Total
		Th.	Seminar	Pr.	Tr.	
		2		2		4
4	Study level/year at which this course is offered:					
5	Pre –requisite (if any):	Data structure				
6	Co –requisite (if any):					
7	Program (s) in which the course is offered	information technology				
8	Language of teaching the course:	English and Arabic				
9	System of Study:	Attendance				
10	Mode of delivery:					
11	Location of teaching the course:	Class				

III. Course Description:

- Brief description of knowledge , skills and activities to be achieved (50-70 words)

- **This course** introduce to the students the science and study of methods of data protection computer and communication systems from unauthorized disclosure and modification, to show how to develop techniques for verification, identification, key safeguarding schemes and key distribution protocols and to introduce students to different methods of encrypting data for security purposes.

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

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

This course aims to student acquire the:

1. Understand the basic rules of protection to computer and information. A1
2. Understand the science theory of information protection. A2
3. Use the basics rules of protection to protect computer and information. B1
4. Use the science theories to protect information. B2
5. Use the science theory along with the suitable computer languages to build some encryption/decryption programs. C1
6. Analysis different techniques of information protection. C2
7. Select suitable security system for an organization. D1

V. Course Content:

- Distributionof Semester Weekly Plan of Course Topics/Items and Activities.

A – Theoretical Aspect:

Order	Topics List	Week Due	Contact Hours
1	The concept of Information , the main resources of Information , the aspects , factors of security	1-2	12
2	The concept of integrity using CRC and Hamming methods	3-4	6
3	The concept of cyphers, Caesar, Veginner, Playfare and transposition cyphers. linear, nonlinear functions, random numbers and random numbers generator algorithms	5-7	9
4	Mad term exam	8	2
5	Block cyphering SDES and DES algorithms	9-11	6
6	Modular arithmetic operations, GCD of two numbers and algorithm to generate GCD of two numbers, RAS, algorithms	12- 13	6
7	Hash functions and Digital signature.	14-15	6
8	Final exam	16	2
Number of Weeks /and Units Per Semester		**16**	**46**

VI. Teaching strategies of the course:

Lectures and simulation

VII.Assignments:

No	Assignments	Aligned CILOs(symbols)	Week Due	Mark
1	Program to generate CRC of an electronic document.	A,B,C	3	5
2	Program to generate Caesar, Veginner, Playfare and transposition cyphers.	A,B,C	5	5
3	Program to construct substitutions boxes in DES algorithm	A,B,C,D	7	5
	Programs to construct session and Public keys	A,B,C,D	13	5

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

Assessment	Type of Assessment Tasks	Week Due	Mark	Proportion of Final Assessment
1	Program to generate CRC of an electronic document.	3	5	5%
2	Program to generate Caesar, Veginner, Playfare and transposition cyphers.	5	5	5%
3	Program to construct substitutions boxes in DES algorithm	7	5	5%
4	Programs to construct session and Public keys	13	5	5%

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 (2003) “Cryptography and Network Security: Principles and Practice” 3rd Edn. India Reprint. Agrawal-M IETE-Technical-Review.

2. Bruce Schneier (2006) “Applied Cryptography” 4nd Edition John Wiley & Sons. (ASIA) Pvt. Ltd., Clementi Loop # 02-01, Singapore 129809.

2- Essential References.

1. David M. Burton (2005) “Elementary Number Theory” 2nd Edition Universal Book Stall New Delhi India.

2. Douglasr. Stinson (2010) “Cryptography: Theory and Practice” Department of Combinatory and Optimization University of Waterloo, Waterloo, Ontario Canada. 2nd Edition, Chapman & Hall/CRC.

3. Bruce Schneier (2006) “Applied Cryptography” 4^{nd} Edition John Wiley & Sons. (ASIA) Pvt. Ltd., Clementi Loop # 02-01, Singapore 129809.

4. Deborah Russell and G. T. Gangemi Sr (2001) “ Computer Security Basics” O’Reilly & Associates, Inc., New York

3- Recommended Books and Reference Materials.

1.
2.
3.
4.

4- Electronic Materials and Web Sites *etc*.

1.
2.
3.

5- Other Learning Material (such as computer-based programs/CD, professional standards/ regulations).

1.
2.
3.

X. Course Policies:

Unless otherwise stated, the normal course administration policies and rules of the Faculty of ----- apply.
For the policy, see: -----------------------------------

The University Regulations on academic misconduct will be strictly enforced. Please refer to -----------

1	**Class Attendance:**
2	**Tardy:**
3	**Exam Attendance/Punctuality:** -
4	**Assignments & Projects:** -
5	**Cheating**: -
6	**Plagiarism**:
7	**Other policies:**