Course Specification of: Applied Cryptography & Network Security

Course Code (CCE556)

IV. General Information About the Course:

	Course Title:	**Applied Cryptography & Network Security**			
	Course Code and Number:	**CCE556**			
	Credit Hours:	**Credit Hours**			**Total**
		Lecture	Practical	Seminar/Tutorial	
		3	--	--	**3**
	Study Level and Semester:	**2nd Semester**			
	Pre-requisites (if any):				
	Co-requisites (if any):				
	Program (s) in which the course is offered:	M. Sc. in Computer Engineering & Control			
	Language of teaching the course:	English			
	Study System:	Courses & Thesis			
	Prepared By:	Assoc. Prof. Dr. Farouk Al-Fahaidy			
	Reviewed by:	Prof. Dr. Khalil Al-Wagih			
	Date of Approval:				

V. Course Description:

This course provides a deep knowledge in advanced concepts, theories, algorithm and protocols applied in data and network security. Course covers, an overview on Applied Cryptography, Classical Ciphers, Symmetric Ciphering, Public key encryption, differential and linear cryptanalysis, hash functions, authentication protocols, key distribution protocols, key management, security protocol pitfalls, and Internet cryptography protocols

such as, IP sec., SSL/TLS and e-mail security. It also focuses on development the student's skills in applying and implementing variety of cryptographic techniques in practicing to solve the data security to different environments.

VI. Course Intended Learning Outcomes (CILOs):

Upon successful completion of **Applied Cryptography & Network Security Course**, the graduates will be able to:

Demonstrate deep understanding of advanced concepts, theories, algorithms and protocols related to applied cryptography & Networks security.

Explain advanced numbers theories, modern cryptographic algorithms, IT frameworks and authentication protocols such as, hash functions and their practicing to the data and networks security.

solve environmental problems related to data and networks security using appropriate encryption, authentication & integrity algorithms and computer programming to meet desired domain specifications and constraints.

Propose innovative computational methods for solving problems related to cryptography after assessing applicable methods and their limits.

Develop computer programs for implementing of different cryptographic algorithms and protocols.

Use an appropriate cryptographic algorithm and protocol to protect an individual and organization information security properties during storing, processing and transmission.

Present a high level of skills in writing, presenting and defending research/project activities throughout individual and team course works.

Function effectively either individually or within a team to complete course projects.

VII. Alignment of Course Intended Learning Outcomes (CILOs) to Program Intended Learning Outcomes (PILOs)

CILOs		PILOs
n.	**Knowledge and Understanding:** Upon successful completion of **the Applied Cryptography & Network Security Course**, the graduates will be able to:	**M. Knowledge and Understanding:** Upon successful completion of the **M. Sc. In Computer Engineering & Control Program**, the graduates will be able to:
	Demonstrate deep understanding of advanced concepts, theories, algorithms and protocols related to applied cryptography & Networks security.	Demonstrate deep understanding of computer engineering and control as well as knowledge of applied mathematics and engineering science to the field of computing and intelligent control.
	Explain advanced numbers theories, modern cryptographic algorithms, IT frameworks and authentication protocols such as, hash functions and their practicing to the data and networks security.	**A2.** Recognize and Explain the contemporary engineering technologies and issues in the specialization field of computing and control.
ı. Cognitive/ Intellectual Skills: Upon successful completion of the **Applied Cryptography & Network Security Course,** the graduates will be able to:		**N. Cognitive/ Intellectual Skills:** Upon successful completion of the **M. Sc. In Mechanical Engineering Program,** the graduates will be able to:
	solve environmental problems related to data and networks security using appropriate encryption, authentication & integrity algorithms and computer programming to meet desired domain specifications and constraints.	**1.** Evaluate, select and apply appropriate principles, methodologies, techniques, tools and packages to the analysis, specification, development and evaluation of computing and engineering systems.
	Propose innovative computational methods for solving problems related to cryptography after assessing applicable methods and their limits.	**3.** Propose computing system, component, or process to meet desired needs within realistic constraints.

. Professional and Practical Skills: Upon successful completion of the **Applied Cryptography & Network Security Course,** the graduates will be able to:		**). Professional and Practical Skills:** Upon successful completion of the **M. Sc. In Computer Engineering & Control Program,** the graduates will be able to:
	Develop computer programs for implementing of different cryptographic algorithms and protocols.	**1.** Develop, configure, upgrade, and/or write computer software/program to solve computing and control problems.
	Use an appropriate cryptographic algorithm and protocol to protect an individual and organization information security properties during storing, processing and transmission.	**2.** Use advanced methodology and skills to the formulation and practice of computer science, engineering and control systems.
. Transferable Skills: Upon successful completion of the **Applied Cryptography & Network Security Course,** the graduates will be able to:		**. Transferable Skills:** Upon successful completion of the **M. Sc. In Computer Engineering & Control Program,** the graduates will be able to:
	Demonstrate a high level of skills in writing, presenting and defending research/project activities throughout individual and team course works.	**1.** Prepare complete thesis and reports, present ideas clearly and defend them.
	Function effectively either individually or within a team to complete course projects works.	Conduct independently and communicate research that advances and extends computing knowledge and scholarship in relate.

/III. Alignment of CILOs to Teaching and Assessment Strategies

. Alignment of Knowledge and Understanding CILOs:

Knowledge and Understanding CILOs		Teaching Strategies	Assessment Strategies
a1.	**Demonstrate deep understanding of advanced concepts, theories, algorithms and protocols related to applied cryptography & Networks security.**	Lectures, Self-Learning Problems/Studies.	Oral & Writing Exams Written Exam, Assignments.

	Explain advanced numbers theories, modern cryptographic algorithms, IT frameworks and authentication protocols such as, hash functions and their practicing to the data and networks security.	Lectures, Seminars, Group/Individual Projects and Studies, Active learning.	Oral & Writing Exams Reports, Written Exam, Assignments

Alignment of Intellectual Skills CILOs:

Intellectual Skills CILOs		Teaching Strategies	Assessment Strategies
b1.	**solve environmental problems related to data and networks security using appropriate encryption, authentication & integrity algorithms and computer programming to meet desired domain specifications and constraints.**	Lectures, Project Supervision, Self-Learning, Case Study, Simulation Exercises, Independent Study, Analysis and Problem Solving, Presentations,	Oral & Writing Exams Reports, Survey, Written Exam, Assignments
b2.	**Propose innovative computational methods for solving problems related to cryptography after assessing applicable methods and their limits.**	Lectures, Project Supervision, Self-Learning, Case Study, Simulation Exercises, Independent Study, Analysis and Problem Solving, Presentations,	Oral & Writing Exams Reports, Survey, Written Exam, Assignments

Alignment of Professional and Practical Skills CILOs:

Professional and Practical Skills CILOs		Teaching Strategies	Assessment Strategies
	Develop computer programs for implementing of different cryptographic algorithms and protocols.	Lectures, Project Supervision, Self-Learning, Case Study, Simulation Exercises, Independent Study, Analysis and Problem Solving,	Oral & Writing Exams Seminar Report, Assignments, Written Research Proposal.

		Presentations,	
	Use an appropriate cryptographic algorithm and protocol to protect an individual and organization information security properties during storing, processing and transmission.	Lectures, Project Supervision, Self-Learning, Case Study, Simulation Exercises, Independent Study, Analysis and Problem Solving, Presentations,	Oral & Writing Exams Seminar Report, Assignments, Written Research Proposal.

Alignment of Transferable (General) Skills CILOs:

Transferable (General) Skills CILOs		Teaching Strategies	Assessment Strategies
	Demonstrate a high level of skills in writing, presenting and defending research/project activities throughout individual and team course works.	Dissertation Defenses and Presentation, Independent Study, Presentation, Brainstorming, Presenting Researches.	Written Research Proposal, Assignments, Presentation, Written Report.
	Function effectively either individually or within a team to complete course projects.	Dissertation Defenses and Presentation, Independent Study, Presentation, Brainstorming, Presenting Researches.	Written Research Proposal, Assignments, Presentation, Written Report.

IX. Course Content

. Theoretical Aspect

Order	Topic List / Units	Sub -Topics List	Number of Weeks	Contact Hours	Course ILOs

1	Introduction to Cryptography and Network Security	Cryptography and Network Security: history, classifications and applications, Computer & Network Security Concepts & Terminologies.	1	3	a1, a2
2	Classical Ciphering Algorithms	Symmetric/Private-Key Ciphering Model & Concepts, Classical Ciphers Techniques: such as Caesar, Playfair, transposition and Vegner Table, Attackers types and ciphering analysis.	1	3	a1, a2, b1
3	Symmetric Ciphers (DES)	Block Ciphers: Data Encryption Standard (DES), Block Cipher Design Principles and Key Generation, A DES Example, The Strength of DES.	1	3	a1, a2, b1, b2, c2
4	Basic Number Theory	Finite Fields: Groups, Rings and Fields, Finite Fields of the Form GF(p), Greatest Common Divisor (GCD), Euclidean Distance and Extended Euclidean Distance	1	3	a1, a2, b1

		Algorithms, ▪ Finite Field Arithmetic, Addition, Multiplication & Inverse, ▪ Polynomial Arithmetic and Finite Fields, GF(2^n).			
5	Advanced Encryption Standard (AES) and Modes of Operations	▪ AES Structure, ▪ AES Transformation Functions, ▪ AES Key Expansion, ▪ AES Example, ▪ AES Implementation, ▪ Block & Stream Ciphers Operations: Multiple Encryption and Triple DES, Electronic Code Block, Cipher Block Chaining Mode, Cipher Feedback Mode, Output Feedback Mode, Counter Mode, XTS-AES Mode for Block-oriented Storage Devices.	2	6	a1, a2, b1, b2, c2
6	Pseudorandom Number Generation and Stream Ciphers	▪ Principles of Pseudorandom Number Generation, ▪ Block Cipher Vs. Stream Cipher, ▪ Pseudorandom Generation using a Block Cipher, ▪ Stream Ciphers: Concepts	1	3	a1, a2, b1

		and Operations RC4 Algorithm.			
7	Midterm Exam	Midterm Exam include ALL Previous Topics	1	3	a1, a2, b1, b2, c2
8	Asymmetric/Public-Key Ciphering Algorithms	Prime Numbers and Euler's Theorem, Asymmetric/Public-Key Cryptography Model, Principles of Public-Key Cryptosystems, The RSA Algorithm. Diffie-Hellman Key Exchange, Elgamal Cryptographic System, Elliptic Curve Algorithm.	2	6	a1, a2, b1, b2, c2
9	Cryptographic Data Integrity Functions & Codes	Cryptographic Hash Functions and their Applications, Hash Functions based on Cipher Block Chaining, Secure Hash Algorithm (SHA) and SHA-3, Message Authentication: Requirements & Functions, Message Authentication Codes (MACs) Requirements & Security,	2	6	a2, b1, b2, c2

		MACs Based on Hash Functions (HMAC), MACs Based on Block Ciphers (DAA & CMAC), Digital Signatures Principles and Applied Digital Signature Schemes such as Elgmal, NIST, Elliptic-Curve and RSA-PSS.			
10	Mutual Trust: Key Management & Distribution	**Symmetric Key Distribution using Symmetric/Asymmetric Encryptions, Distribution of Public Keys, X.509 Certificates, Remote User-Authentication Principles, Federated Identity Managements and Personal Identity Verification.**	1	3	**a2, b1, b2, c2**
11	Network Security Protocols	**Network Security Concepts & Requirements, IPSec Protocol: Headers, Structures and Modes. SSL/STL Security Protocols, New Trends in Network and Cyber Securities.**	1	3	**b1, b2, c2**

12	Case Studies & Course Projects Presentation	Students Presents in an individual and in Groups their course Projects, Programming Implementation and Paper Presentations works.	1	3	a2, b1, b2, c1, c2, d1, d2
13	Final Exam	ALL Topics Except the Case Study & Course Project works.	1	3	a1, a2, b1, b2, c1, c2
Number of Weeks /and Contact Hours Per Semester			16	48	

. Practical Aspect

Order	Practical / Tutorials topics	Number of Weeks	Contact Hours	Course ILOs
1	NONE			
2				
Number of Weeks /and Contact Hours Per Semester				

. Tutorial Aspect:

No.	Tutorial	Number of Weeks	Contact Hours	Learning Outcomes (CILOs)
1	NONE			
2				
Number of Weeks /and Units Per Semester		15	30	

J. Teaching Strategies:

Lectures,

Seminars,

Project Supervision,

Self-Learning,

Case Study,

Simulation Exercises,

Dissertation Defenses and Presentation,

Independent Study,

Analysis and Problem Solving,

Brainstorming,

Presenting Researches,

Presentations,

Group/Individual Projects and Studies,

Active learning.

I. Assessment Methods of the Course:

Oral & Writing Exams

Reports,

Survey,

Written Exam,

I. Assessment Methods of the Course:

Assignments

Seminar Report,

Written Research Proposal.

I. Tasks and Assignments:

No	Assignments/ Tasks	Individual/ Group	Mark	Week Due	CILOs (symbols)
1	**Assignments:** **Assignment 1: Implementation of Classical Ciphering Techniques using Programming** **Assignment 2: Implementation of DES Algorithm using Programming** **Assignment 3: Implementation of DES Algorithm using Programming** **Assignment 4: Implementation of different Public-Key Ciphering Algorithm, Hash Functions & Authentication Techniques using Programming**	**Individual**	**10**	**4th, 7th, 10th & 13th**	**a1, a2, b1, b2, c1, c2, d1, d2**
2	**Mini/Major Project:** **Graduates works and submit their individual & group Projects by searching Webs, using modern Programming Language to solve different domain problems related to data and networks Security.**	**Individual/ Group**	**16**	**From the 4th to 14th**	**a1, a2, b1, b2, c1, c2, d1, d2**

3	Papers presentation & Case studies	Individual/ Group	8	Work from the 4th to 14th weeks	a2, b1, b2, c1, c2, d1, d2
	Total Score		34	==	===

II. Learning Assessment:

No.	Assessment Tasks	Week due	Mark	Proportion of Final Assessment	CILOs
1	Tasks and Assignments	4th to 14th	34	34%	a1, a2, b1, b2, c1, c2,
2	Quizzes	6th & 12th	6	6%	a1, a2, b1, b2
3	Midterm Exam	8th	20	20%	a1, a2, b1, b2, c2
4	Final Exam (Theoretical)	16th	40	40%	a1, a2, b1, b2, c2
	Total			100%	===

V. Learning Resources:

0.Required Textbook(s):

William Stallings, 2020, Cryptography and Network Security Principles and Practice, 8th Edition, USA, Pearson, ISBN 13: 9780135764039.

Behrouz A. Forouzan, 2015, "Cryptography & Network Security", McGraw-Hill Education, 3rd edition, India, ISBN-13 9789339220945.

1.Essential References:

Kenneth H. Rosen, Ph,D., 2006, Cryptography Theory and Practice, 3rd Edition, Taylor and

Francis Group, LLC, USA.

Atul Kahata, 2003, Cryptography and network security, 1st ed., tata megraw.

Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, 1996, Handbook of Applied Cryptography.

2. Electronic Materials and Web Sites *etc.*

Websites:

To access Text Book, the Cryptography and Network Security: Principles and Practice, Sixth Edition, Premium Web site for the first time, you will need to register online using a computer with an Internet connection and a web browser.

Go to http://www.pearsonhighered.com/stallings/

To access some papers with codes

http://www.githup.com

Sample Course on Data & Network Security:

http://www.just.edu.jo/~tawalbeh/

Journals:

Enquire the search engines by sub-topic mentioned in the course plan to get accurate and up-to-date information.

IEEE Publisher

https://www.ieee.org

Elsevier Publisher

https://www.elsevier.org

Science Direct Publisher

https://www.Sciencedirect.com

Course Policies الضوابط والسياسات المتبعة في المقرر	
بعد الرجوع للوائح الجامعة يتم كتابة السياسة العامة للمقرر فيما يتعلق بالآتي:	
Class Attendance: سياسة حضور الفعاليات التعليمية - يلتزم الطالب بحضور 75% من المحاضرات ويحرم في حال عدم الوفاء بذلك. - يقدم أستاذ المقرر تقريرا بحضور وغياب الطلاب للقسم ويحرم الطالب من دخول الامتحان في حال تجاوز الغياب 25% ويتم اقرار الحرمان من مجلس القسم.	1
Tardy: الحضور المتأخر - يسمح للطالب حضور المحاضرة إذا تأخر لمدة ربع ساعة لثلاث مرات في الفصل الدراسي، وإذا تأخر زيادة عن ثلاث مرات يحذر شفويا من أستاذ المقرر، وعند عدم الالتزام يمنع من دخول المحاضرة.	2
Exam Attendance/Punctuality: ضوابط الامتحان - لا يسمح للطالب دخول الامتحان النهائي إذا تأخر مقدار (20) دقيقة من بدء الامتحان - إذا تغيب الطالب عن الامتحان النهائي تطبق اللوائح الخاصة بنظام الامتحان في الكلية.	3
Assignments & Projects: التعيينات والمشاريع - يحدد أستاذ المقرر نوع التعيينات في بداية الفصل ويحدد مواعيد تسليمها وضوابط تنفيذ التكليفات وتسليمها. - إذا تأخر الطالب في تسليم التكليفات عن الموعد المحدد يحرم من درجة التكليف الذي تأخر في تسليمه.	4
Cheating: الغش - في حال ثبوت قيام الطالب بالغش في الامتحان النصفي أو النهائي تطبق عليه لائحة شؤون الطلاب. - في حال ثبوت قيام الطالب بالغش او النقل في التكليفات والمشاريع يحرم من الدرجة المخصصة للتكليف.	5
Plagiarism: الانتحال - في حالة وجود شخص ينتحل شخصية طالب لأداء الامتحان نيابة عنه تطبق اللائحة الخاصة بذلك	6
Other policies: سياسات أخرى - أي سياسات أخرى مثل استخدام الموبايل أو مواعيد تسليم التكليفات ..... الخ	7

Academic Year: 2021

Course Plan (Syllabus): Applied Cryptography & Network Security

Information about Faculty Member Responsible for the Course:

Name	Farouk Al-Fahaidy	Office Hours					
Location &Telephone No.	777909815	SAT	SUN	MON	TUE	WED	THU
E-mail	farouqakh@gmail.com						

General information about the course:

3.	Course Title	Applied Cryptography & Network Security			
).	Course Code and Number	CCE556			
).	Credit Hours	Credit Hours			Total
		ecture	Practical	eminar/Tutorial	
		3	--	--	3
.	Study Level and Semester	nd Semester			
.	Pre-requisites				
.	Co –requisite				
.	Program (s) in which the course is offered	M. S. in Computer Engineering & Control Program			
.	Language of teaching the course	nglish			
.	Location of teaching the course				

Course Description:

This course provides a deep knowledge in advanced concepts, theories, algorithm and protocols applied in data and network security. Course covers, an overview on Applied Cryptography, Classical Ciphers, Symmetric Ciphering, Public key encryption, differential

and linear cryptanalysis, hash functions, authentication protocols, key distribution protocols, key management, security protocol pitfalls, and Internet cryptography protocols such as, IP sec., SSL/TLS and e-mail security. It also focuses on development the students skills in applying and implementing variety of cryptographic techniques in practicing to solve the data security to different environments.

. Course Intended Learning Outcomes (CILOs):

Upon successful completion of the **Applied Cryptography & Network Security** course, graduate students will be able to:

Demonstrate deep understanding of advanced concepts, theories, algorithms and protocols related to applied cryptography & Networks security.

Explain advanced numbers theories, modern cryptographic algorithms, IT frameworks and authentication protocols such as, hash functions and their practicing to the data and networks security.

solve environmental problems related to data and networks security using appropriate encryption, authentication & integrity algorithms and computer programming to meet desired domain specifications and constraints.

Propose innovative computational methods for solving problems related to cryptography after assessing applicable methods and their limits.

Develop computer programs for implementing of different cryptographic algorithms and protocols.

Use an appropriate cryptographic algorithm and protocol to protect an individual and organization information security properties during storing, processing and transmission.

Present a high level of skills in writing, presenting and defending research/project activities throughout individual and team course works.

d2. Function effectively either individually or within a team to complete course projects.

Course Content

Theoretical Aspect

Order	Topic List / Units	Sub -Topics List	Number of Weeks	Contact Hours
1	Introduction to Cryptography and Network Security	Cryptography and Network Security: history, classifications and applications, Computer & Network Security Concepts & Terminologies.	1	3
2	Classical Ciphering Algorithms	Symmetric/Private-Key Ciphering Model & Concepts, Classical Ciphers Techniques: such as Caesar, Playfair, transposition and Vegner Table, Attackers types and ciphering analysis.	1	3
3	Symmetric Ciphers (DES)	Block Ciphers: Data Encryption Standard (DES)، Block Cipher Design Principles and Key Generation, A DES Example، The Strength of DES.	1	3

4	Basic Number Theory	▪ Finite Fields: Groups, Rings and Fields, ▪ Finite Fields of the Form GF(p), Greatest Common Divisor (GCD), Euclidean Distance and Extended Euclidean Distance Algorithms, ▪ Finite Field Arithmetic, Addition, Multiplication & Inverse, ▪ Polynomial Arithmetic and Finite Fields, GF(2^n).	1	3
5	Advanced Encryption Standard (AES) and Modes of Operations	▪ AES Structure, ▪ AES Transformation Functions, ▪ AES Key Expansion, ▪ AES Example, ▪ AES Implementation, ▪ Block & Stream Ciphers Operations: Multiple Encryption and Triple DES, Electronic Code Block, Cipher Block Chaining Mode, Cipher Feedback Mode, Output Feedback Mode, Counter Mode, XTS-AES Mode for Block-oriented Storage Devices.	2	6
6	Pseudorandom Number Generation and Stream Ciphers	▪ Principles of Pseudorandom Number Generation, ▪ Block Cipher Vs. Stream Cipher, ▪ Pseudorandom Generation using a Block Cipher, ▪ Stream Ciphers: Concepts and	1	3

		Operations RC4 Algorithm.		
7	Midterm Exam	Midterm Exam include ALL Previous Topics	1	3
8	Asymmetric/Public-Key Ciphering Algorithms	Prime Numbers and Euler's Theorem, Asymmetric/Public-Key Cryptography Model, Principles of Public-Key Cryptosystems, The RSA Algorithm. Diffie-Hellman Key Exchange, Elgamal Cryptographic System, Elliptic Curve Algorithm.	2	6
9	Cryptographic Data Integrity Functions & Codes	Cryptographic Hash Functions and their Applications, Hash Functions based on Cipher Block Chaining, Secure Hash Algorithm (SHA) and SHA-3, Message Authentication: Requirements & Functions, Message Authentication Codes (MACs) Requirements & Security, MACs Based on Hash Functions (HMAC), MACs Based on Block Ciphers (DAA & CMAC), Digital Signatures Principles and Applied Digital Signature Schemes such as Elgmal, NIST, Elliptic-	2	6

		Curve and RSA-PSS.		
10	Mutual Trust: Key Management & Distribution	**Symmetric Key Distribution using Symmetric/Asymmetric Encryptions, Distribution of Public Keys, X.509 Certificates, Remote User-Authentication Principles, Federated Identity Managements and Personal Identity Verification.**	1	3
11	Network Security Protocols	**Network Security Concepts & Requirements, IPSec Protocol: Headers, Structures and Modes. SSL/STL Security Protocols, New Trends in Network and Cyber Securities.**	1	3
12	Case Studies & Course Projects Presentation	**Students Presents in an individual and in Groups their course Projects, Programming Implementation and Paper Presentations works.**	1	3
13	Final Exam	**ALL Topics Except the Case Study & Course Project works.**	1	3
Number of Weeks /and Contact Hours Per Semester			**16**	**48**

Practical Aspect

Order	Practical / Tutorials topics	Number of Weeks	Contact Hours	Course ILOs
1	. NONE			
Number of Weeks /and Contact Hours Per Semester				

Training/ Tutorials/ Exercises Aspects:

Order	Tutorials/ Exercises	Week Due	Contact Hours
1	NONE		
2			
Number of Weeks /and Contact Hours Per Semester			

Teaching Strategies:

Lectures,

Seminars,

Project Supervision,

Self-Learning,

Case Study,

Simulation Exercises,

Dissertation Defenses and Presentation,

Independent Study,

Analysis and Problem Solving,

Brainstorming,

Presenting Researches,

Presentations,

Group/Individual Projects and Studies,

Active learning.

I. Assessment Methods of the Course:

Oral & Writing Exams

Reports,

Survey,

Written Exam,

Assignments

Seminar Report,

Written Research Proposal.

I. Tasks and Assignments:

No	Assignments	Individual /Groups	Mark	Week Due
1	**Assignments:** **Assignment 1: Implementation of Classical Ciphering Techniques using Programming** **Assignment 2: Implementation of DES Algorithm using Programming**	**Individual**	**10**	**4th, 7th, 10th & 13th**

	Assignment 3: Implementation of DES Algorithm using Programming **Assignment 4: Implementation of different Public-Key Ciphering Algorithm, Hash Functions & Authentication Techniques using Programming**			
2	**Mini/Major Project:** **Graduates works and submit their individual & group Projects by searching Webs, using modern Programming Language to solve different domain problems related to data and networks Security.**	**Individual/ Group**	**16**	**From the 4th to 14th**
3	**Papers presentation & Case studies**	**Individual/ Group**	**8**	**Work from the 4th to 14th weeks**
	Total Score		**34**	

Learning Assessment:

No	Assessment Method	Week Due	Mark	Proportion of Final Assessment %
1	Tasks and Assignments	4th to 14th	34	34%
2	Quizzes	6th & 12th	6	6%
3	Midterm Exam	8th	20	20%
4	Final Exam (Theoretical)	16th	40	40%
	Total		100	100 %

Learning Resources:

. Required Textbook(s):

William Stallings, 2020, Cryptography and Network Security Principles and Practice, 8th Edition, USA, Pearson, ISBN 13: 9780135764039.

Behrouz A. Forouzan, 2015, "Cryptography & Network Security", McGraw-Hill Education, 3rd

edition, India, ISBN-13 9789339220945.

. Essential References:

Kenneth H. Rosen, Ph,D., 2006, Cryptography Theory and Practice, 3rd Edition, Taylor and Francis Group, LLC, USA.

Atul Kahata, 2003, Cryptography and network security, 1st ed., tata megraw.

Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, 1996, Handbook of Applied Cryptography.

. Electronic Materials and Web Sites *etc.*

Websites:

To access Text Book, the Cryptography and Network Security: Principles and Practice, Sixth Edition, Premium Web site for the first time, you will need to register online using a computer with an Internet connection and a web browser.

Go to http://www.pearsonhighered.com/stallings/

To access some papers with codes

http://www.githup.com

Sample Course on Data & Network Security:

http://www.just.edu.jo/~tawalbeh/

Journals:

Enquire the search engines by sub-topic mentioned in the course plan to get accurate and up-to-date information.

IEEE Publisher

https://www.ieee.org

Elsevier Publisher

https://www.elsevier.org

Science Direct Publisher

https://www.Sciencedirect.com

Course Policies الضوابط والسياسات المتبعة في المقرر	
بعد الرجوع للوائح الجامعة يتم كتابة السياسة العامة للمقرر فيما يتعلق بالآتي:	
Class Attendance: سياسة حضور الفعاليات التعليمية - يلتزم الطالب بحضور 75% من المحاضرات ويحرم في حال عدم الوفاء بذلك. - يقدم أستاذ المقرر تقريرا بحضور وغياب الطلاب للقسم ويحرم الطالب من دخول الامتحان في حال تجاوز الغياب 25% ويتم اقرار الحرمان من مجلس القسم.	1
Tardy: الحضور المتأخر - يسمح للطالب حضور المحاضرة إذا تأخر لمدة ربع ساعة لثلاث مرات في الفصل الدراسي، وإذا تأخر زيادة عن ثلاث مرات يحذر شفويا من أستاذ المقرر، وعند عدم الالتزام يمنع من دخول المحاضرة.	2
Exam Attendance/Punctuality: ضوابط الامتحان - لا يسمح للطالب دخول الامتحان النهائي إذا تأخر مقدار (20) دقيقة من بدء الامتحان - إذا تغيب الطالب عن الامتحان النهائي تطبق اللوائح الخاصة بنظام الامتحان في الكلية.	3
Assignments & Projects: التعيينات والمشاريع - يحدد أستاذ المقرر نوع التعيينات في بداية الفصل ويحدد مواعيد تسليمها وضوابط تنفيذ التكليفات وتسليمها. - إذا تأخر الطالب في تسليم التكليفات عن الموعد المحدد يحرم من درجة التكليف الذي تأخر في تسليمه.	4
Cheating: الغش - في حال ثبوت قيام الطالب بالغش في الامتحان النصفي أو النهائي تطبق عليه لائحة شؤون الطلاب. - في حال ثبوت قيام الطالب بالغش او النقل في التكليفات والمشاريع يحرم من الدرجة المخصصة للتكليف.	5
Plagiarism: الانتحال - في حالة وجود شخص ينتحل شخصية طالب لأداء الامتحان نيابة عنه تطبق اللائحة الخاصة بذلك	6
Other policies: سياسات أخرى - أي سياسات أخرى مثل استخدام الموبايل أو مواعيد تسليم التكليفات ..... الخ	7