Syrian Arab Republic		الجمهورية العربية السورية
Ministry of Higher Education		وزارة التعليم العالـــــي
Syrian Virtual University		الجامعة الافتراضية السورية

Course Definition:Cryptography

1- Basic Information:

Course Name	Cryptography
Course ID	CR
Contact Hours (Registered Sessions)	18
Contact Hours (Synchronized Sessions)	18
Mid Term Exam	---
Exam	2
Registered Sessions Work Load	36
Synchronized Session Work Load	36
Credit Hours	3

2- Pre-Requisites:

Course	ID
Numerical Analysis	ISE – NA

3- Course General Objectives:

Cryptography is considered as one of the most important tools used for creating a secure environment for exchanging and protecting information. We present in this course the basics and concepts of information encryption, and we show how we can use these techniques to achieve the following three goals: confidentiality, integrity and authentication. This takes place by learning the classical symmetric encryption methods that were invented and used in the past, and then by learning the modern ones like DES and AES standards. The course also presents the asymmetric encryption methods with a focus on RSA algorithm. In addition, we study message integrity verification, user authentication, and key management.

4- Intended Learning Outcomes (ILO):

Code	Intended Learning Outcomes
ILO1	Understanding the general concepts of information security and the relation with cryptography
ILO2	Learning the classical encryption and its ancient algorithms
ILO3	Understanding the model and functionality of symmetric cryptosystems, and the details of DES and AES standards
ILO4	Understanding the model and functionality of asymmetric cryptosystems, and the details of RSA algorithm
ILO5	Understanding hash functions and message authentication methods
ILO6	Learning key management and exchange mechanisms
ILO7	Acquiring the skill to implement and test an encryption algorithm

5- Course Syllabus (18 hours of total synchronized sessions)

- **RS:** Recorded Sessions; **SS:** Synchronized Sessions;

ILO	Course Syllabus	RS	SS	Type	Additional Notes
ILO1	• Computer security objectives • Computer security requirements • Security architecture • Security services • Security mechanisms • Network security model	3	3	---	---
ILO2	• Symmetric cryptography model • Substitution techniques • Transposition techniques	1.5	1.5	assignments	Exercises

ILO3	• Stream cipher • Block cipher • Feistel cipher • DES: Data Encryption Standard • AES: Advanced Encryption Standard • Block cipher operation	4.5	4.5	assignments	Exercises
ILO4	• Public key cryptography concepts • Public key cryptography applications • Public key cryptography requirements • RSA algorithm • Diffie-Hellman exchange • ElGamal algorithm • Elliptic Curve Cryptography algorithm	1.5	4.5	assignments	Exercises
ILO5	• Hash functions • Message authentication • MAC: Message Authentication Codes • Digital Signature • HMAC algorithm	6	3	assignments	Exercises
ILO6	• Symmetric key distribution • Public key certificates • PKI: Public Key Infrastructure	1.5	1.5	assignments	Exercises
ILO7	• Course assignment	0	0	assignments	---

6- Assessment Criteria (Related to ILOs)

ISC	Interactive Synchronized Collaboration		Ex	Exams		Rpt	Reports
PF2F	Presentations and Face-to-Face Assessments		PW	Practice Work			

ILO Code	ILO	Intended Results	Assessment Type				
			ISC	PW	Ex	PF2F	Rpt
ILO1	Understanding the general concepts of information security and the relation with cryptography	Understanding the necessary basics to learn cryptography	✓		✓		
ILO2	Learning the classical encryption and its ancient algorithms	Learning about the history of cryptography	✓	✓	✓		
ILO3	Understanding the model and functionality of symmetric cryptosystems, and the details of DES and AES standards	Learning the capabilities of symmetric encryption standards	✓	✓	✓		
ILO4	Understanding the model and functionality of asymmetric cryptosystems, and the details of RSA algorithm	Learning the capabilities of asymmetric encryption	✓	✓	✓		
ILO5	Understanding hash functions and message authentication methods	Learning how to verify the integrity of a message and the identity of its source	✓	✓	✓		

ILO6	Learning key management and exchange mechanisms	Learning about the solutions of encryption key sharing	✓		✓		
ILO7	Acquiring the skill to implement and test an encryption algorithm	Practical application of encryption algorithm development		✓			✓

7- Practice Tools:

Tool Name	Description
.NET	An environment for developing encryption algorithms

8- Main References

Stallings, William. *Cryptography and network security: principles and practice*. Pearson, 2017.

9- Additional References

- Katz, Jonathan, et al. *Handbook of applied cryptography*. CRC press, 1996.
- Schneier, Bruce. *Schneier's Cryptography Classics Library: Applied Cryptography, Secrets and Lies, and Practical Cryptography*. Wiley Publishing, 2007.