4/1/4. Course Specification:

COURSE SPECIFICATIONS

Form

Course Title: Algebraic Cryptography

Course Code: 4046407-4

Course Specifications

Institution Umm Al-Qura University	Date November 2018
College/Department College of Applied Science / Department of Mathematical Sciences	

A. Course Identification and General Information

1. Course title and code: **Algebraic Cryptography** 4046407-4
2. Credit hours 4
3. Program(s) in which the course is offered. (If general elective available in many programs indicate this rather than list programs) Master in Mathematics
4. Name of faculty member responsible for the course Prof. Ahmed A Khammash
5. Level/year at which this course is offered Level3/Master
6. Pre-requisites for this course (if any) 4044406-3 + 4043404-4
7. Co-requisites for this course (if any)
8. Location if not on main campus Al-Abidiyah campus and Al-Zahir campus

9. Mode of Instruction (mark all that apply)

a. traditional classroom	√	What percentage?	85
b. blended (traditional and online)		What percentage?	
c. e-learning	√	What percentage?	15
d. correspondence		What percentage?	
f. other		What percentage?	

Comments:

B Objectives

1. What is the main purpose for this course? To introduce the student to the basic concepts and different techniques of algebraic cryptography.
2. Briefly describe any plans for developing and improving the course that are being implemented. (e.g. increased use of IT or web based reference material, changes in content as a result of new research in the field) (1) Updating references and other resources used in teaching process. (2) Using e-learning facilities. (3) Encouraging students to collect problems (and conjectures) from web based resources, ask them to present their collected data and discuss it in an interactive way in the class.

C. Course Description (Note: General description in the form used in Bulletin or handbook)

Course Description: This course is a 4 credit hours course comprising approximately 60 hours of lectures.

1. Topics to be Covered		
List of Topics	No. of Weeks	Contact hours
(1) ELEMENTARY NUMBER THEORY • Time estimates for arithmetic , Divisibility , Congruence (1) FINITE FIELDS AND QUADRATIC RESIDUES • Finite fields , Quadratic residue	5	20
(2) CRYPTOGRAPHY • Basic principles of Cryptosystems , Reliability , Enciphering matrices (3) PUBLIC KEY • The idea of public key cryptography , RSA , Authentication	5	20
(4) PRIMALITY AND FACTORING (5) COMPUTATIONAL COMPLEXITY	5	20

2. Course components (total contact hours and credits per semester):						
	Lecture	Tutorial	Laboratory or Studio	Practical	Other:	Total

Contact Hours	60	0				60
Credit	4	0				4

3. Additional private study/learning hours expected for students per week.
Four hours of homework, revision and presentations

4. Course Learning Outcomes in NQF Domains of Learning and Alignment with Assessment Methods and Teaching Strategy

On the table below are the five NQF Learning Domains, numbered in the left column.
First, insert the suitable and measurable course learning outcomes required in the appropriate learning domains (see suggestions below the table). **Second**, insert supporting teaching strategies that fit and align with the assessment methods and intended learning outcomes. **Third**, insert appropriate assessment methods that accurately measure and evaluate the learning outcome. Each course learning outcomes, assessment method, and teaching strategy ought to reasonably fit and flow together as an integrated learning and teaching process. (Courses are not required to include learning outcomes from each domain.)

Code #	NQF Learning Domains And Course Learning Outcomes	Course Teaching Strategies	Course Assessment Methods
1.0	**Knowledge**		
1.1	Develop the knowledge and understanding of the concept and the main idea of the algebraic cryptography and the basic principles of Cryptosystems (enciphering , deciphering and breaking codes)	Lectures , homeworks and discovery-based-learning discussions	Quizzes , periodicals and final exams as well as presentations.
1.2	Learn the concept of public key cryptography , RSA , Authentication	Lectures , homeworks and discovery-based-learning discussions	Quizzes , periodicals and final exams as well as presentations
2.0	**Cognitive Skills**		
2.1	Demonstrate the ability to representing data digitally as well as implementing different techniques transferring and retrieving data using ciphering and deciphering process.	Lectures , homeworks and discovery-based-learning discussions	Quizzes , periodicals and final exams as well as presentations
2.2	Demonstrate the ability of using public	Lectures , homeworks and	Quizzes ,

	key ciphers and applying such ciphers in transferring secret data as well as judging its reliability	discovery-based-learning discussions	periodicals and final exams as well as presentations
3.0	**Interpersonal Skills & Responsibility**		
3.1	Practicing how to work within small team as an outcome of the discovery-based-learning discussions implemented throughout the course. Presentations teaches the student how to cite and quote	Lectures , homework and discovery-based-learning discussions	Quizzes , periodicals and final exams as well as presentations
3.2			
4.0	**Communication, Information Technology, Numerical**		
4.1	Demonstrate communication and listening skills with the people in the class with positive attitudes and deportment. Show the ability of raising mathematical questions (problems) and how to solve them	Lectures , homework and discovery-based-learning discussions	Quizzes , periodicals and final exams as well as presentations
4.2			
5.0	**Psychomotor**		
5.1	NOT APPLICABLE	NOT APPLICABLE	NOT APPLICABLE

5. Schedule of Assessment Tasks for Students During the Semester			
	Assessment task (e.g. essay, test, group project, examination, speech, oral presentation, etc.)	Week Due	Proportion of Total Assessment
1	First periodic exam	6	20
2	Second periodic exam	10	20
3	Homework and tutorial activities	Over all weeks	20
4	Final exam	End	40

D. Student Academic Counseling and Support

1. Arrangements for availability of faculty and teaching staff for individual student consultations and academic advice. (include amount of time teaching staff are expected to be available each week) The instructor is available for six hours at least per week. S/he is also available on appointments.

E Learning Resources

1. List Required Textbooks

(1) Neal Koblitz, Algebraic Aspects of Cryptography, Springer 1998 (2) Neal Koblitz, A course in number theory and cryptography , Springer 1987 (3) Charles GOLDIE and RICHARD PINCH, Communication theory, Cambridge University Press 1991.
2. List Essential References Materials (Journals, Reports, etc.)
3. List Recommended Textbooks and Reference Material (Journals, Reports, etc)
4. List Electronic Materials, Web Sites, Facebook, Twitter, etc.
5. Other learning material such as computer-based programs/CD, professional standards or regulations and software.

F. Facilities Required

Indicate requirements for the course including size of classrooms and laboratories (i.e. number of seats in classrooms and laboratories, extent of computer access etc.)
1. Accommodation (Classrooms, laboratories, demonstration rooms/labs, etc.) A classroom with the capacity of 10-20 students
2. Computing resources (AV, data show, Smart Board, software, etc.)
3. Other resources (specify, e.g. if specific laboratory equipment is required, list requirements or attach list)

G Course Evaluation and Improvement Processes

1 Strategies for Obtaining Student Feedback on Effectiveness of Teaching A student survey questions is implemented by the end of the semester which usually provides valuable feedback for both the teacher and the institution
2 Other Strategies for Evaluation of Teaching by the Instructor or by the Department Peer consultations and coordination
3 Processes for Improvement of Teaching In the light of the outcome of the survey questions in (1) and (2), the instructor and the department take series steps towards improving the teaching process.
4. Processes for Verifying Standards of Student Achievement (e.g. check marking by an independent member teaching staff of a sample of student work, periodic exchange and remarking of tests or a sample of assignments with staff at another institution) Coordination with other colleagues in both teaching and marking
5 Describe the planning arrangements for periodically reviewing course effectiveness and planning for improvement. The department obliged by the regulations to review the whole program each certain period of time (5 years) in the light of the different outcomes.

Name of Instructor: **Prof. Ahmed Khammash**
Signature: *Ahmed Khammash* Date Report Completed: November 1,2018

Name of Field Experience Teaching Staff Algebra (Representation Theory)
Program Coordinator:_____
Signature: _____ Date Received:_____