King Saud University
College of Science
Department of Mathematics

Course specification

Applications of Algebra, MATH442

(An elective course)

1432H/2011G

Institution: King Saud University
College/Department: College of Science/Department of Mathematics

A Course Identification and General Information

1. Course title and code: Applications of Algebra MATH442
2. Credit hours: 4 (3+1+0)
3. Program(s) in which the course is offered. Bachelor of Science in Mathematics
4. Name of faculty member responsible for the course: Dr. Fawzi Al-Thukair / for males Dr. Fairouz Tchier / for females
5. Level/year at which this course is offered: 8^{th} level/ fourth year
6. Pre-requisites for this course (if any): Rings and Fields, MATH441
7. Co-requisites for this course (if any): None
8. Location if not on main campus: At Diriya, Main campus: College of Science, Building No. 4 for males At Malaz for females.

B Objectives

1- Studying encryption systems as applications on number theory.
2- Studying public key systems and their algorithms.
3- Studying basics of coding theory and especially linear codes.

1. Summary of the main learning outcomes for students enrolled in the course.

After studying this course, the student is expected to be able to:

- Analyze classical encryption systems
- Design modern coding systems and their applications in electronic government
- Design codes that are suitable for detecting and correcting some errors which arise in transmission channel

2. Briefly describe any plans for developing and improving the course that are being implemented. (eg increased use of IT or web based reference material, changes in content as a result of new research in the field)

The plan is to increase the use of mathematics software to implement the algorithms studied during the course so that they use numbers close to the size used in the real world.

C. Course Description (Note: General description in the form to be used for the Bulletin or Handbook should be attached)

1 Topics to be Covered

List of Topics	No of Weeks	Contac thours
Classical cipher systems	2	10
Steam ciphers	2	10
Introduction to cryptanalysis	2	10
Exponential ciphers and public keys	2	10
Introduction to codes	2	10
Linear codes	2	10
Perfect codes	1	5
Cyclic codes	2	10

2 Course components (total contact hours per semester):				
Lecture: 45	Tutorial: 30	Laboratory	Practical/Field work/Internship	Other:

3. Additional private study/learning hours expected for students per week. (This should be an average :for the semester not a specific requirement in each week) 6 hours/week.

4. Development of Learning Outcomes in Domains of Learning For each of the domains of learning shown below indicate: • A brief summary of the knowledge or skill the course is intended to develop; • A description of the teaching strategies to be used in the course to develop that knowledge or skill; • The methods of student assessment to be used in the course to evaluate learning outcomes in the domain concerned.
a. Knowledge
(i) Description of the knowledge to be acquired The student acquires the principles of cryptography with examples of cipher systems. He also learns techniques of cryptanalysis. He gets introduced to coding theory and error correction. He learns about linear and cyclic codes.
(ii) Teaching strategies to be used to develop that knowledge Lectures, homework, and term projects.
(iii) Methods of assessment of knowledge acquired Two mid-term tests, quizzes, homework assessment, project assessment, final exam
b. Cognitive Skills
(i) Description of cognitive skills to be developed 1- How to design a cipher system. 2- How to analyse a cipher system. 3- How to design minimal codes to detect a predetermined number of errors and correct them.
(ii) Teaching strategies to be used to develop these cognitive skills Lectures, Homework, Computer programs

(iii) Methods of assessment of students cognitive skills Mid-term, quizzes, homework , final exam.
c. Interpersonal Skills and Responsibility
(i) Description of the interpersonal skills and capacity to carry responsibility to be developed 1- Cooperation on solving given problems. 2- Management of tasks to be performed in the assigned projects.
(ii) Teaching strategies to be used to develop these skills and abilities 1- Asking students to discuss solutions of the homework in class during the exercises session. 2- asking students to do projects in groups.
(iii) Methods of assessment of students interpersonal skills and capacity to carry responsibility term projects and discussed homework problems during the exercises session.
d. Communication, Information Technology and Numerical Skills
(i) Description of the skills to be developed in this domain. 1-Using computer programs to construct real world examples. 2- Finding out about the latest development of the field by searching journals on the internet.
(ii) Teaching strategies to be used to develop these skills 1- Assigning problems pertaining to the real world 2- Term projects that require the use of computer skills.
(iii) Methods of assessment of students numerical and communication skills Grading homework and term projects.
e. Psychomotor Skills (if applicable)
(i) Description of the psychomotor skills to be developed and the level of performance required
(ii) Teaching strategies to be used to develop these skills
(iii) Methods of assessment of students psychomotor skills

5. Schedule of Assessment Tasks for Students During the Semester

Assessment	Assessment task (eg. essay, test, group project, examination etc.)	Week due	Proportion of Final Assessment
1	1st mid-term test	6th	15

2	2nd mid-term test	12th week	15
3	Term project	14th	10
4	Homework	Every week	10
5	Final exam	Final week	50

D. Student Support

1. Arrangements for availability of faculty for individual student consultations and academic advice. (include amount of time faculty are available each week)

- 10 scheduled office hours per week
- 5 hours weekly for academic advice through the academic guidance unit in the department.

E Learning Resources

1. Required Text(s)
1- Introduction to Cryptography, by Maroof Samhan and Fawzi al-Thukair 2008 (in Arabic)
2- Cryptography: Theory and Practice., by Douglas R. Stinson. CRC Press 2000
3- Coding theory: The essentials, by D.G. Hoffman et al, Dekker Press 1992

2. Essential References
1- Cryptography with coding theory, by Wade Trappe and Lawrence Washington, Prentice Hall 2002.
2- Algebraic Aspects of Cryptography, Neal Koblitz, Springer 1991
3- Codes and Cryptography, by Dominic Welsh, Oxford Science Publications 1989.

3- Recommended Books and Reference Material (Journals, Reports, etc) (Attach List)

4-.Electronic Materials, Web Sites etc
1- cryptomath program.
2- Maple computer program

5- Other learning material such as computer-based programs/CD, professional standards/regulations

F. Facilities Required

Indicate requirements for the course including size of classrooms and laboratories (ie number of seats in classrooms and laboratories, extent of computer access etc.)

1. Accommodation (Lecture rooms, laboratories, etc.)

Class room with max capacity of 30

2. Computing resources Laptops for the students
3. Other resources (specify --eg. 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 Students evaluation forms at the end of the course.
2 Other Strategies for Evaluation of Teaching by the Instructor or by the Department Open discussions with the students during office hours.
3 Processes for Improvement of Teaching Listening to the students and benefiting from a feedback regarding homework or test problems.
4. Processes for Verifying Standards of Student Achievement (eg. check marking by an independentfaculty member of a sample of student work, periodic exchange and remarking of a sample of assignments with a faculty member in another institution) • Unified exams and common marking if there is more than one group. • Check the marking of a sample of student answer sheets in the final exam by an independent faculty member
5 Describe the planning arrangements for periodically reviewing course effectiveness and planning for improvement. Re-assessment of all the elements of the course every 5 years by an independent entity.

King Saud University
College of Science
Mathematics Department

COURSE SPECIFICATION

MATH442: Applications of Algebra

Kingdom of Saudi Arabia

The National Commission for Academic Accreditation & Assessment

COURSE SPECIFICATION

Applications of Algebra, Math 442

Revised March 2007

Applications of Algebra, MATH442

Institution King Saud University
College/Department College of Science/Department of Mathematics

A Course Identification and General Information

1. Course title and code: **Applications of Algebra MATH442**
2. Credit hours 4 (3+1+0)
3. Program(s) in which the course is offered. (If general elective available in many programs indicate this rather than list programs) BSc. In Mathematics
4. Name of faculty member responsible for the course Dr. Fawzi Al-Thukair
5. Level/year at which this course is offered: fourth year
6. Pre-requisites for this course (if any) MATH441 (rings and fields)
7. Co-requisites for this course (if any)
8. Location if not on main campus:

B Objectives

1. Summary of the main learning outcomes for students enrolled in the course. The student applies what he or she studied in courses of Number Theory and algebra in the fields of Cryptography and Coding theory.
2. Briefly describe any plans for developing and improving the course that are being implemented. (eg increased use of IT or web based reference material, changes in content as a result of new research in the field) The plan is to increase the use of mathematics software to implement the algorithms studied during the course so that they use numbers close to the size used in the real world.

C. Course Description (Note: General description in the form to be used for the Bulletin or Handbook should be attached)

1 Topics to be Covered		
List of Topics	No of Weeks	Contact hours
Classical cipher systems	2	10
Steam ciphers	2	10
Introduction to cryptanalysis	2	10
Exponential ciphers and public keys	2	10
Introduction to codes	2	10
Linear codes	2	10
Perfect codes	1	5
Cyclic codes	2	10

2 Course components (total contact hours per semester):				
Lecture: 45	Tutorial: 30	Laboratory	Practical/Field work/Internship	Other:

3. Additional private study/learning hours expected for students per week. (This should be an average :for the semester not a specific requirement in each week) 6 hours/week.

4. Development of Learning Outcomes in Domains of Learning
For each of the domains of learning shown below indicate:

- A brief summary of the knowledge or skill the course is intended to develop;
- A description of the teaching strategies to be used in the course to develop that knowledge or skill;
- The methods of student assessment to be used in the course to evaluate learning outcomes in the domain concerned.

a. Knowledge
(i) Description of the knowledge to be acquired The student acquires the principles of cryptography with examples of cipher systems. He also learns techniques of cryptanalysis. He gets introduced to coding theory and error correction. He learns about linear and cyclic codes.
(ii) Teaching strategies to be used to develop that knowledge Lectures, homework, and term projects.
(iii) Methods of assessment of knowledge acquired Two mid-term tests, quizzes, homework assessment, project assessment, final exam
b. Cognitive Skills
(i) Description of cognitive skills to be developed 1- How to design a cipher system. 2- How to analyse a cipher system. 3- How to design minimal codes to detect a predetermined number of errors and correct them.
(ii) Teaching strategies to be used to develop these cognitive skills Lectures, Homework, Computer programs
(iii) Methods of assessment of students cognitive skills Mid-term, quizzes, homework , final exam.
c. Interpersonal Skills and Responsibility
(i) Description of the interpersonal skills and capacity to carry responsibility to be developed 1- Cooperation on solving given problems. 2- Management of tasks to be performed in the assigned projects.
(ii) Teaching strategies to be used to develop these skills and abilities 1- Asking students to discuss solutions of the homework in class during the exercises session. 2- asking students to do projects in groups.
(iii) Methods of assessment of students interpersonal skills and capacity to carry responsibility term projects and discussed homework problems during the exercises session.
d. Communication, Information Technology and Numerical Skills
(i) Description of the skills to be developed in this domain. 1-Using computer programs to construct real world examples. 2- Finding out about the latest development of the field by searching journals on the internet.
(ii) Teaching strategies to be used to develop these skills 1- Assigning problems pertaining to the real world 2- Term projects that require the use of computer skills.
(iii) Methods of assessment of students numerical and communication skills Grading homework and term projects.

e. Psychomotor Skills (if applicable)
(i) Description of the psychomotor skills to be developed and the level of performance required
(ii) Teaching strategies to be used to develop these skills
(iii) Methods of assessment of students psychomotor skills

5. Schedule of Assessment Tasks for Students During the Semester			
Assessment	Assessment task (eg. essay, test, group project, examination etc.)	Week due	Proportion of Final Assessment
1	1st mid-term test	6th	15
2	2nd mid-term test	12th week	15
3	Term project	14th	10
4	Homework	Every week	10
5	Final exam	Final week	50

D. Student Support

1. Arrangements for availability of faculty for individual student consultations and academic advice. (include amount of time faculty are available each week) I am available 10 hours a week in my office to help students with questions they might have on the material of the course.

E Learning Resources

1. Required Text(s) 1- Introduction to Cryptography, by Maroof Samhan and Fawzi al-Thukair 2008 (in Arabic) 2- Cryptography: Theory and Practice., by Douglas R. Stinson. CRC Press 2000 3- Coding theory: The essentials, by D.G. Hoffman et al, Dekker Press 1992
2. Essential References 1- Cryptography with coding theory, by Wade Trappe and Lawrence Washington, Prentice Hall 2002. 2- Algebraic Aspects of Cryptography, Neal Koblitz, Springer 1991 3- Codes and Cryptography, by Dominic Welsh, Oxford Science Publications 1989.
3- Recommended Books and Reference Material (Journals, Reports, etc) (Attach List)
4-.Electronic Materials, Web Sites etc 1- cryptomath program. 2- Maple computer program
5- Other learning material such as computer-based programs/CD, professional standards/regulations

F. Facilities Required

Indicate requirements for the course including size of classrooms and laboratories (ie number of seats in classrooms and laboratories, extent of computer access etc.)
1. Accommodation (Lecture rooms, laboratories, etc.) Class room with max capacity of 30
2. Computing resources Laptops for the students
3. Other resources (specify --eg. 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 Students evaluation forms at the end of the course.
2 Other Strategies for Evaluation of Teaching by the Instructor or by the Department Open discussions with the students during office hours.
3 Processes for Improvement of Teaching listening to the students and benefiting from a feedback regarding homework or test problems.
4. Processes for Verifying Standards of Student Achievement (eg. check marking by an independentfaculty member of a sample of student work, periodic exchange and remarking of a sample of assignments with a faculty member in another institution) I hope that we will have the policy of an independent evaluator of students knowledge; including tests and projects.
5 Describe the planning arrangements for periodically reviewing course effectiveness and planning for improvement. Re-assessment of all the elements of the course every 5 years by an independent entity.