


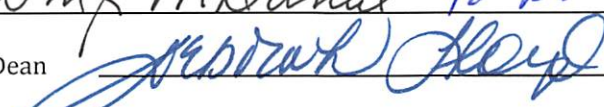
 FLORIDA ATLANTIC UNIVERSITY	COURSE CHANGE REQUEST Graduate Programs		UGPC Approval _____ UFS Approval _____ SCNS Submittal _____ Confirmed _____ Banner Posted _____ Catalog _____
	Department <u>MATHEMATICAL SCIENCES</u> College <u>CHARLES E. SCHMIDT COLLEGE OF SCIENCE</u>		
Current Course Prefix and Number MAD 5474		Current Course Title Introduction to Cryptology and Information Security	
<i>Syllabus must be attached for ANY changes to current course details. See Guidelines. Please consult and list departments that may be affected by the changes; attach documentation.</i>			
Change title to: N/A		Change description to: N/A	
Change prefix From: N/A To: N/A		Change prerequisites/minimum grades to: BACHELOR'S DEGREE EXISTING PREREQUISITES/MINIMUM GRADES: MINIMUM GRADE OF C IN MAS 2103 MATRIX THEORY MINIMUM GRADE OF C IN MAD 2502 INTRODUCTION TO COMPUTATIONAL MATHEMATICS MINIMUM GRADE OF C IN MAS 4301 MODERN ALGEBRA TWO MAJOR REVISIONS HAVE BEEN MADE: 1) THE COURSE IS NOW FULLY ONLINE 2) CONTENT HAS BEEN SLIGHTLY MODIFIED SO THAT PREREQUISITES ARE NOT REQUIRED ANYMORE. THE MAIN MOTIVATION FOR THE REVISION IS TO BE ABLE TO INCLUDE THIS COURSE IN OUR APPLICATION FOR THE NSA/DHS CAE-CDE PROGRAM (CENTERS FOR ACADEMIC EXCELLENCE IN CYBER DEFENSE EDUCATION). AS PART OF THE PROGRAM REQUIREMENTS, THIS COURSE SHOULD IDEALLY BE AVAILABLE TO STUDENTS FROM 4 COLLEGES (SCIENCE, ENGINEERING AND COMPUTER SCIENCE, BUSINESS, AND DESIGN AND SOCIAL INQUIRY) AND HAVE NO PREREQUISITES.	
Change course number From: N/A To: N/A			
Change credits* From: N/A To: N/A			
Change grading From: N/A To: N/A		Change corequisites to: N/A	
*Review Provost Memorandum		Change registration controls to: N/A Please list existing and new pre/corequisites, specify AND or OR and include minimum passing grade.	
Effective Date (TERM & YEAR)		Terminate course List final active term	
Faculty Contact/Email/Phone Koray Karabina, kkarabina@fau.edu , 561 699-5656			
Approved by		Date	
Department Chair 		<u>10-24-16</u>	
College Curriculum Chair 		<u>10-27-16</u>	
College Dean <u>Dr. Charles Roberts</u>		<u>11/7/2016</u>	
UGPC Chair <u>Wm McDaniel</u> 		<u>11-9-2016</u>	
Graduate College Dean 		<u>11-14-16</u>	
Provost _____		_____	

Email this form and syllabus to UGPC@fau.edu one week before the UGPC meeting.

**Florida Atlantic University
Department of Mathematical Sciences**

**Introduction to Cryptology and Information Security
MAD 5474
Fall 2016
3 Credit Hours**

Instructor: Dr. Koray Karabina
Office Location: SE 266
Office Hours: WF 9am - 10am, or by appointment
Contact Phone Number: 561-297-0809
Email: kkarabina@fau.edu

Course Prerequisites: Bachelor's degree

Time Commitment per Credit Hour: This course has 3 credit hours. For traditionally delivered courses, not less than one (1) hour of classroom or direct faculty instruction each week for fifteen (15) weeks per Fall or Spring semester, and a minimum of two (2) hours of out-of-class student work for each credit hour. Equivalent time and effort is required for Summer Semesters, which may be offered over a shortened time frame. Fully Online courses, hybrid, shortened, intensive format courses, and other non-traditional modes of delivery will demonstrate equivalent time and effort.

Course Description/Introduction

Cryptographic applications; classical ciphers and their analysis; symmetric key cryptography; block ciphers; stream ciphers; modes of operations; cryptographic hash functions; message authentication codes; public key cryptography; encryption and digital signature schemes (RSA and ElGamal); key agreement protocols (Diffie-Hellman); real life deployments and standardization efforts.

Course Objectives

1. Define the security of fundamental cryptographic primitives and systems
2. Analyze security of symmetric and public key schemes, hash functions, message authentication codes and cryptographic protocols
3. Define and Apply generic cryptanalysis methods including brute force, frequency analysis, meet-in-the-middle attacks
4. Examine symmetric key and public key schemes: encryption functions, hash functions, message authentication codes, signature schemes. Key establishment protocols.
5. Identify applications, real-life deployment, and learn about the history standardization of cryptographic constructions
6. Develop skills for implementing cryptographic algorithms and for analyzing their security
7. Master basic number theoretical, algorithmic, probabilistic and statistical notions and apply this knowledge in cryptanalysis

Course Delivery Mode

This is a fully online course accessible only through FAU's learning management system—Blackboard. You must log into Blackboard with your FAU ID and Password to access the materials and assignments in this course. If you do not know your FAU ID or Password click the following link for help. [Link to Office of Information Technology Help.](#)

The course is organized into modules with dates provided for each module. Dates and durations for each module may vary so please pay close attention to start and due dates. The course begins with the START HERE page, which will familiarize you with the organization and navigation of the course. You will open a new learning unit to access the assigned reading materials, PowerPoints, and other relevant materials for each subsequent module.

Required Text and Materials

The course textbook is available online at <http://cacr.uwaterloo.ca/hac/>

Handbook of Applied Cryptology

Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone

ISBN-10: 0849385237

ISBN-13: 9780849385230

Copyright: 1997

Technology and Computer Requirements

Minimum Technology Requirements for This Course

In this course you will need the following technology and computer requirements:

Hardware

- Dependable computer
- Computer speakers
- Headset with microphone
- Webcam

Software

- Microsoft 365 Suite [Link to Download](#)
- Reliable web browser (recommended [Chrome](#) or [Firefox](#))
- Java – [Link to Download](#) and/or [Link to Verify Java](#) on your computer
- Adobe Flash Player: [Link to Download](#)
- Blackboard Mobile Learn (optional) is a free mobile app that provides full access to your course directly from your smartphone (Android, BlackBerry, iPhone, iPod Touch, and iPad). [Click here for more information.](#)

Internet Connection

- Recommended: Broadband (high-speed) Internet connection with a speed of 4 Mbps or higher
- To function properly, Blackboard requires a high-speed Internet connection (cable modem, DSL, satellite broadband, T1, etc.). The minimum Internet connection speed to access Blackboard is a consistent 1.5 Mbps (megabits per second) or higher.
- To check your internet speed [click here](#).

Minimum Technical Skills Requirements

The general and course-specific technical skills a student must have to succeed in the course include but are not limited to:

1. Accessing Internet.
2. Using Blackboard (including taking tests, attaching documents, etc.).
3. Using email with attachments.
4. Creating and submitting files in commonly used word processing program formats such as Microsoft Office Tools.
5. Copying and pasting functions.
6. Downloading and installing software.
7. Using presentation, graphics, and other programs.
8. Creating and posting to a discussion board, blog, or wiki.
9. Searching the FAU library and websites.

Computer Requirement

- Operating System
 - A computer that can run Mac OSX or Win XP or higher.
- Peripherals
 - A backup option should be available to minimize the loss of work. This can be an external hard drive, a USB drive, cloud storage, or your folder on the FAU servers.
 - You may also need headphones with a microphone for varied multimedia in the class.
- Software
 - [Once logged in to Blackboard](#), please visit the *Students* tab located at the top of each Blackboard page for LMS compatibility with your computer. Make sure your Internet browser is compatible and that you have all the recommended plug-ins installed.
 - Other software may be required for specific learning units and/or modules. If so, the necessary links to download and install will be provided within the applicable unit and/or module.

Technical Support

In the online environment, technical issues are always possible (e.g., lost connection, hardware or software failure). Many of these can be resolved relatively quickly, but if you wait until the last minute before due dates, the chances of these glitches affecting your success are greatly increased. Please plan appropriately. If a problem occurs, it is essential you take immediate action to document the issue so your instructor can verify and take appropriate action to resolve the problem. Please take the following steps when a problem occurs:

1. Contact the eLearning Success Advisor for assistance:
eLearning Success Advisor - 561-297-3590
2. If you can, make a Print Screen of the monitor when the problem occurs. Save the Print Screen as a .jpg file. If you are unfamiliar with creating a Print Screen file, visit [Link to Print Screen Instructions](#).
3. Complete a Help Desk ticket [Link to Help Desk](#). Make sure you complete the form entirely and give a full description of your problem so the Help Desk staff will have the pertinent information in order to assist you properly. This includes:
 - a. Select "Blackboard (Student)" for the Ticket Type.

- b. Input the Course ID.
 - c. In the Summary/Additional Details section, include your operating system, Internet browser, and Internet service provider (ISP).
 - d. Attach the Print Screen file, if available.
4. Send a message within Blackboard to your instructor to notify him/her of the problem. Include all pertinent information of the incident (2b-d above).
 5. If you do not have access to Blackboard, send an email to your instructor with all pertinent information of the incident (2b-d above).
 6. If you do not have access to a computer, call your instructor with all pertinent information of the incident. If he/she is not available, make sure you leave a detailed message.
 7. If you do not hear back from the Help Desk or your instructor within a timely manner (48 hours), it is your responsibility to follow up with the appropriate person until a resolution is obtained.

Course Assessments, Assignments, Grading Policy, and Course Policies

Introductions and Syllabus Quiz: Not Graded

You will post an introduction in the student introductions discussion board and take a syllabus quiz. The syllabus quiz can be taken as many times as necessary to achieve 100%.

Discussion Boards: Not Graded

1. Your instructor will post at least 3 discussion problems during the term. Your active participation in discussions will play a key role in your success. You should post an original submission to the discussion board for each discussion problem and reply to at least 2 other students' posts with a substantive response. A substantive response adds value to the discussion by bringing new ideas, research, evidence, etc. to the conversation. "I agree", "Ditto", and the like are not acceptable replies. Rules of Netiquette must be followed. Replies are not texts with your friends. Full sentences, proper spelling, proper source citations, etc., are expected.
2. You are encouraged to use the discussion board for collaborating with other students on the assignment problems.

Assignments: A Total of 210 points

There will be a total of 10 assignments throughout the term. Assignments are worth a total of 210 points. Assignments may not be weighted equally.

Each assignment's availability and due date is clearly stated in the course schedule. Print the PDF for each assignment and answer the questions. You are encouraged to type your solutions in LATEX but this is not mandatory. You may also type your solutions in WORD using proper math formula and equation formats. If you choose to hand-write and scan your answers, make sure you scan each page and they are dark enough to read. In the end, **you have to save your solutions as a PDF file and submit a single file.** Do not upload photo of your answers. You will have plenty of time to work on the assignment problems and so **no late submissions will be accepted and make-ups are not allowed.** Your instructor will mark all written assignments. You must show all of your work to receive full mark. Your solutions must be legible and well organized.

Quizzes: A total of 90 points

There will be a total of 3 quizzes throughout the term. Each quiz is worth 30 points with a total of 90 points.

Each quiz's availability and due date are clearly stated in the course schedule. Print the PDF for each quiz and answer the questions. You are encouraged to type your solutions in LATEX but this is not mandatory. You may also type your solutions in WORD using proper math formula and equation formats. If you choose to hand-write and scan your answers, make sure you scan each page and they are dark enough to read. In the end, **you have to save your solutions as a PDF file and submit a single file.** Do not upload photo of your answers. Each quiz will be due on the same day it is available and **no late submissions will be accepted.** Your instructor will mark all quizzes. You must show all of your work to receive full mark. Your solutions must be legible and well organized.

Grading and Scale

There are maximum 300 points to collect in this course. Total number of points collected by a student will be divided by 300, and the resulted percentage will be converted to a final letter grade according to the following catalogue:

Total Points	87-100	83-86	77-82	73-76	70-72	67-69	63-66	60-62	57-59	53-56	50-52	<50
Grade	A	A-	B+	B	B-	C+	C	C-	D+	D	D-	F

Late Assignments and Quizzes Policy

Late assignments and late quizzes will not be accepted except in very special circumstances.

Make-up Policy for Assignments and Quizzes:

You will have plenty of time to work on the assignment problems and so **no late submissions will be accepted and no make-up for assignments.**

Make-up quizzes will be given only under extraordinary circumstances such as such as illness, family emergencies, military obligation, court-imposed legal obligations, or participation in university-approved activities – See FAU website for a list of university-approved activities. If you miss a quiz, you must provide a written, verifiable excuse, if possible in advance of the scheduled exam. Doctor notes, letters, emails from immediate family members are not accepted as proof of absence from any quizzes. Approval for a make-up quiz must be obtained from your instructor.

Incomplete Grade Policy

The University policy states that a student who is passing a course, but has not completed all work due to exceptional circumstances, may, with consent of the instructor, temporarily receive a grade of incomplete ("I"). The assignment of the "I" grade is at the discretion of the instructor, but is allowed only if the student is passing the course.

Code of Academic Integrity Policy Statement

Students at Florida Atlantic University are expected to maintain the highest ethical standards. Academic dishonesty is considered a serious breach of these ethical standards, because it interferes with the University mission to provide a high quality education in which no student enjoys an unfair advantage over any other. Academic dishonesty is also destructive of the university community, which is grounded in a system of mutual trust and places high value on personal integrity and individual responsibility. Harsh penalties are associated with academic dishonesty. For more information, see [University Regulation 4.001](#).

[Plagiarism](#) is unacceptable in the University community. Academic work that is submitted by students is assumed to be the result of their own thought, research, or self-expression. When students borrow ideas, wording, or organization from another source, they are expected to acknowledge that fact in an appropriate manner. Plagiarism is the deliberate use and appropriation of another's work without identifying the source and trying to pass off such work as one's own. Any student who fails to give full credit for ideas or materials taken from another has plagiarized. This includes all discussion board posts, journal entries, wikis, and other written and oral presentation assignments. If in doubt, cite your source!

Online Attendance Policy

Since the course is delivered online, you are expected to access the course **at least three times per week** to ensure you do not miss pertinent postings, messages, or announcements. It is imperative that you meet course deadlines and stay active in discussion boards, group projects, etc. If you are experiencing major illness, absences due to University duties, or other large-scale issues, contact the instructor immediately to formulate a resolution.

Netiquette and Classroom Etiquette Policy

Netiquette

Due to the casual communication common in the online environment, students are sometimes tempted to relax their grammar, spelling, and/or professionalism. Please remember that you are adult students and professionals—your communication should be appropriate.

For more in-depth information, please see the FAU statement on Netiquette at:

[Link to Netiquette policy](#)

Classroom Etiquette/Disruptive Behavior Policy Statement

Disruptive behavior is defined in the FAU Student Code of Conduct as “... *activities which interfere with the educational mission within classroom.*” Students who behave in the face-to-face and/or virtual classroom such that the educational experiences of other students and/or the instructor’s course objectives are disrupted are subject to disciplinary action. Such behavior impedes students’ ability to learn or an instructor’s ability to teach. Disruptive behavior may include, but is not limited to: non-approved use of electronic devices (including cellular telephones); cursing or shouting at others in such a way as to be disruptive; or, other violations of an instructor’s expectations for classroom conduct.

For more information, please see the FAU Office of Student Conduct:

[Link to Student Conduct Policy](#)

Communication Policy

Expectations for Students

- Announcements
 - You are responsible for reading all announcements posted by the instructor. Check the course announcements each time you log in.
- Email
 - You are responsible for reading all of your course email and responding in a timely manner.
- Course-Related Questions
 - Post course-related questions to the FAQ discussion board. This allows other participants with the same question to benefit from the responses. Also, make sure you review this forum prior to posting a question; it may have already been asked and answered in previous posts.

Instructor's Plan for Classroom Response Time & Feedback

- Email Policy
 - Except for Saturdays, Sundays, and holidays, instructor typically, will respond to messages within 48 hours. Such messages should only be used to communicate personal or confidential matters; otherwise, please use the FAQ discussion board within the course.
- Assignment Feedback Policy
 - Feedback will be provided on submitted assignments within one week of the submission date. Some assignments may require a longer review period, which will be communicated to students by the instructor.
- Course-Related Questions
 - Except Saturdays, Sundays, and holidays, questions will, generally, be answered by instructors within 48 hours.

Support Services and Online Resources

Office of Information Technology Online Help Desk:	Link to FAU Help Desk
FAU Libraries:	Link to FAU Library
Center for Learning and Student Success:	Link to FAU Center for Learning
University Center for Excellence in Writing:	Link to FAU Excellence in Writing
Math Learning Center:	Link to FAU Math Center
Office of Undergraduate Research and Inquiry:	Link to FAU Undergraduate Research
Student Accessibility Services:	Link to FAU Student Accessibility Services
Office of International Programs and Study Abroad:	Link to FAU International Programs
Freshman Academic Advising Services:	Link to FAU Freshman Advising

Faculty Rights and Responsibilities

Florida Atlantic University respects the rights of instructors to teach and students to learn. Maintenance of these rights requires classroom conditions which do not impede their exercise. To ensure these rights, faculty members have the prerogative:

- To establish and implement academic standards.
- To establish and enforce reasonable behavior standards in each class.
- To refer disciplinary action to those students whose behavior may be judged to be disruptive under the *Student Code of Conduct*.

Instructor reserves the right to adjust this syllabus as necessary.

Selected University and College Policies

Accessibility Policy Statement

In compliance with the Americans with Disabilities Act (ADA), students who require special accommodations to properly execute coursework due to a disability, must register with Student Accessibility Services (SAS) located in the Boca Raton, Davie, and Jupiter campuses and follow all SAS procedures. For additional information, please see: [Link to Student Accessibility Services](#).

Questions relating to academic accommodations for students with disabilities are to be directed to Students Accessibility Services, Boca Raton campus, Room 133, (561) 297-3880, TDD (561) 297-0358.

Grade Appeal Process

A student may request a review of the final course grade when s/he believes that one of the following conditions apply:

- There was a computational or recording error in the grading.
- Non-academic criteria were applied in the grading process.
- There was a gross violation of the instructor's own grading system.
- Procedures for a grade appeal may be found in [Chapter 4 of the University Regulations](#).

Religious Accommodation Policy Statement

In accordance with rules of the Florida Board of Education and Florida law, students have the right to reasonable accommodations from the University in order to observe religious practices and beliefs with regard to admissions, registration, class attendance, and the scheduling of examinations and work assignments. For further information, please see [Academic Policies and Regulations](#).

University Approved Absence Policy Statement

In accordance with rules of the Florida Atlantic University, students have the right to reasonable accommodations to participate in University approved activities, including athletic or scholastics teams, musical and theatrical performances and debate activities. It is the student's responsibility to notify the instructor at least one week prior to missing any course assignment.

Drops/Withdrawals

Students are responsible for completing the process of dropping or withdrawing from a course. Please click on the following link for more information on dropping and/or withdrawing from a course. [Link to FAU Registrar Office](#)

Course Schedule

See the course webpage for the course schedule.

MAD 5474 INTRODUCTION TO CRYPTOLOGY AND INFORMATION SECURITY
FALL 2016 ONLINE COURSE SCHEDULE



MODULE	DATES	TOPIC	READ/LISTEN/VIEW	TO DO
START HERE	08.22	INTRODUCTION TO COURSE	<ul style="list-style-type: none"> • Syllabus • Course Schedule • Instructor Introduction 	<ul style="list-style-type: none"> • Post student introduction
1.0	08.22 - 08.23	INTRODUCTION TO CRYPTOGRAPHY		
1.1	08.22 - 08.23	OVERVIEW	<ul style="list-style-type: none"> • Lecture/Podcast(s) • PowerPoint(s) • Textbook Reading(s) 	<ul style="list-style-type: none"> • Assignment 1.1 Due 08.26
2.0	08.24 - 09.30	SYMMETRIC KEY CRYPTOGRAPHY		
2.1	08.24 - 08.26	OVERVIEW	<ul style="list-style-type: none"> • Lecture/Podcast(s) • PowerPoint(s) • Textbook Reading(s) 	<ul style="list-style-type: none"> • Assignment 2.1-2.2
2.2	08.29 - 09.02	CLASSICAL CIPHERS	<ul style="list-style-type: none"> • Lecture/Podcast(s) • PowerPoint(s) • Textbook Reading(s) 	<ul style="list-style-type: none"> • Assignment 2.1-2.2 Due 09.02
2.3	09.05 - 09.09	STREAM CIPHERS	<ul style="list-style-type: none"> • Lecture/Podcast(s) • PowerPoint(s) • Textbook Reading(s) 	<ul style="list-style-type: none"> • Assignment 2.3 Due 09.09
2.4	09.12 - 09.16	BLOCK CIPHERS	<ul style="list-style-type: none"> • Lecture/Podcast(s) • PowerPoint(s) • Textbook Reading(s) 	<ul style="list-style-type: none"> • Assignment 2.4 Due 09.16
2.5	09.19 - 09.20	STANDARDIZATION EFFORTS AND THE AES	<ul style="list-style-type: none"> • Lecture/Podcast(s) • PowerPoint(s) • Textbook Reading(s) 	<ul style="list-style-type: none"> • Assignment 2.5 Due 09.23
2.6	09.21 - 09.30	MULTIPLE ENCRYPTION AND THE MODES OF OPERATION	<ul style="list-style-type: none"> • Lecture/Podcast(s) • PowerPoint(s) • Textbook Reading(s) 	<ul style="list-style-type: none"> • Assignment 2.6 Due 09.30 • QUIZ 1: on 09.28

MAD 5474 INTRODUCTION TO CRYPTOLOGY AND INFORMATION SECURITY
FALL 2016 ONLINE COURSE SCHEDULE



UNITS	DATES	TOPIC	READ/LISTEN/VIEW	TO DO
3.0	10.01 - 10.14	HASH FUNCTIONS		
3.1	10.03 - 10.04	OVERVIEW	<ul style="list-style-type: none"> • Lecture/Podcast(s) • PowerPoint(s) • Textbook Reading(s) 	<ul style="list-style-type: none"> • Assignment 3.1-3.2
3.2	10.05 - 10.14	HASH CONSTRUCTION METHODS	<ul style="list-style-type: none"> • Lecture/Podcast(s) • PowerPoint(s) • Textbook Reading(s) 	<ul style="list-style-type: none"> • Assignment 3.1-3.2 Due 10.14
4.0	10.15 - 10.21	MESSAGE AUTHENTICATION CODE SCHEMES		
4.1	10.17 - 10.21	OVERVIEW, CONSTRUCTION METHODS, AND SECURITY	<ul style="list-style-type: none"> • Lecture/Podcast(s) • PowerPoint(s) • Textbook Reading(s) 	<ul style="list-style-type: none"> • Assignment 4.1 Due 10.21 • QUIZ 2: on 10.19
5.0	10.22 - 12.05	PUBLIC KEY CRYPTOGRAPHY		
5.1	10.24 - 10.26	OVERVIEW	<ul style="list-style-type: none"> • Lecture/Podcast(s) • PowerPoint(s) • Textbook Reading(s) 	<ul style="list-style-type: none"> • Assignment 5.1-5.2-5.3
5.2	10.27 - 11.02	THE RSA CRYPTOSYSTEM AND ITS SECURITY	<ul style="list-style-type: none"> • Lecture/Podcast(s) • PowerPoint(s) • Textbook Reading(s) 	<ul style="list-style-type: none"> • Assignment 5.1-5.2-5.3
5.3	11.03 - 11.11	THE RSA DIGITAL SIGNATURE SCHEME	<ul style="list-style-type: none"> • Lecture/Podcast(s) • PowerPoint(s) • Textbook Reading(s) 	<ul style="list-style-type: none"> • Assignment 5.1-5.2-5.3 Due 11.11
5.4	11.14 - 11.18	KEY ESTABLISHMENT AND THE DIFFIE-HELLMAN PROTOCOL	<ul style="list-style-type: none"> • Lecture/Podcast(s) • PowerPoint(s) • Textbook Reading(s) 	<ul style="list-style-type: none"> • Assignment 5.4-5.5
5.5	11.21 - 12.02	ELGAMAL ENCRYPTION AND DIGITAL SIGNATURE SCHEMES	<ul style="list-style-type: none"> • Lecture/Podcast(s) • PowerPoint(s) • Textbook Reading(s) 	<ul style="list-style-type: none"> • Assignment 5.4-5.5 Due 12.02 • QUIZ 3: on 12.05

Note: Instructor has the right to modify course schedule accordingly