FLORIDA ATLANTIC UNIVERSITY™

Graduate Programs—PROGRAM CHANGE REQUEST

UGPC APPROVAL _____
UFS APPROVAL _____
CATALOG _____

DEPARTMENT: COMPUTER/ELECTRICAL ENGINEERING AND COMPUTER SCIENCE	COLLEGE: ENGINEERING AND COMPUTER SCIENCE

PROGRAM NAME:	EFFECTIVE DATE (PROVIDE TERM/YEAR)
CYBER SECURITY CERTIFICATE	FALL 2017

PLEASE EXPLAIN THE REQUESTED CHANGE(S) AND OFFER RATIONALE BELOW AND/OR ATTACHED:

ADD THE COURSE "CIS 5371 PRACTICAL ASPECTS OF MODERN CRYPTOGRAPHY" TO THE GROUP OF CS CYBER SECURITY COURSES.

Faculty contact, email and complete phone number:	Consult and list departments that might be affected by the change and attach comments.
Frederick Bloetscher, Ph.D., P.E. **239-250-2423**	**College of Science / Mathematical Sciences**

	Date:
Department Chair: Maryam Ensaf	November 2, 2016 11-17-16
College Curriculum Chair:	
College Dean:	11/17/2016
UGPC Chair:	
Graduate College Dean:	
UFS President:	
Provost:	

Email this form and syllabus to *UGPC@fau.edu* **one week before** the University Graduate Programs Committee meeting so that materials may be viewed on the UGPC website prior to the meeting.

College of Science / Mathematical Sciences
College of Engineering and Computer Science/ Computer & Electrical engineering and Computer Science

==========

Cyber Security Graduate Certificate
Cybercrime-related issues especially impact the State of Florida because a significant part of the state's economic development comes from tourism, international banking and high-tech industries. The number of scientists, engineers and experts needed with special skills in cyber security exceeds the number available. The Cyber Security certificate provides opportunities for graduate students to expand their knowledge and skills to meet the needs of the cyber security field. Due to their extensive expertise and facilities, the departments of Computer and Electrical Engineering and Computer Science and Mathematical Sciences have jointly designed the Cyber Security certificate. This 12-credit certificate program has two tracks: Computer Science (CS) and Mathematics (Math).

Tracks
CS Track: The Cyber Security certificate with a track in Computer Science will be granted to a student who completes four 3-credit courses as follows: three 3-credit courses from the CS Cyber Security course list and one 3-credit course from either the CS or the Math Cyber Security course list.

Math Track: The Cyber Security certificate with a track in Mathematics will be granted to a student who completes four 3-credit courses as follows: three 3-credit courses from the Math Cyber Security course list and one 3-credit course from either the Math or the CS Cyber Security course list.

Admission
CS Track: Open to students who have a B.S. degree in Computer Science or in a related field of Science or Engineering and a GPA of at least 3.0. Students must satisfy the prerequisites for each course in the program. All four courses must be completed with a GPA of 3.0 or better. All course materials are in English; all international students must demonstrate proficiency in English to enter the program.

Math Track: Open to students who have a bachelor's degree in Mathematics or in a related field and a GPA of at least 3.0. Students must satisfy the prerequisites for each course in the program. All four courses must be completed with a GPA of 3.0 or better. All course materials are in English; all international students must demonstrate proficiency in English to enter the program.

Cyber Security Courses by Track

CS Cyber Security Courses *(Select three from this list and one more from this list or the list of Math courses.)*		
Computer Data Security	CIS 6370	3
Distributed Systems Security	CIS 6375	3
Secret Sharing Protocols	COT 6427	3
Cyber Security: Measurement and Data Analysis	CTS 6319	3
Practical Aspects of Modern Cryptography	CIS 5371	3
Math Cyber Security Courses *(Select three from this list and one more from this list or the list of CS courses.)*		
Introduction to Cryptology and Information Security	MAD 5474	3
Cryptanalysis	MAD 6478	3
Coding Theory	MAD 6607	3
Number Theory and Cryptography	MAS 6217	3

Email approval from Mathematical Sciences Department

From: Rainer Steinwandt [srainer@math.fau.edu]
Sent: Wednesday, November 02, 2016 8:00 AM
To: Mihaela Cardei
Cc: Nurgun Erdol; Yuan Wang
Subject: Re: Request for approval -- new course + addition to the Cyber Security Certificate

Sure, no problem.

Best,
Rainer

From: "Mihaela Cardei" <mcardei@fau.edu>
To: "Rainer Steinwandt" <srainer@math.fau.edu>
Cc: "Nurgun Erdol" <erdol@fau.edu>, "Yuan Wang" <YWANG@fau.edu>
Sent: Wednesday, November 2, 2016 7:44:46 AM
Subject: RE: Request for approval -- new course + addition to the Cyber Security Certificate

Hello Rainer,

The department Graduate Programs Committee recommended Mehrdad to come up with a better title for his course if possible.

So he would like to use the title "Practical Aspects of Modern Cryptography" for his course. The syllabus stays unchanged.

Please let me know if this is acceptable for the Math department.

Thank you,
Mihaela

From: Rainer Steinwandt [srainer@math.fau.edu]
Sent: Tuesday, November 01, 2016 10:13 AM
To: Mihaela Cardei
Cc: Nurgun Erdol; Yuan Wang
Subject: Re: Request for approval -- new course + addition to the Cyber Security Certificate

Hi Mihaela,

This revised syllabus looks good, thanks for sharing. There are no problems from our side with this.

Thanks,
Rainer

From: "Mihaela Cardei" <mcardei@fau.edu>
To: "Rainer Steinwandt" <srainer@math.fau.edu>
Cc: "Nurgun Erdol" <erdol@fau.edu>, "Yuan Wang" <YWANG@fau.edu>
Sent: Tuesday, November 1, 2016 8:20:32 AM
Subject: RE: Request for approval -- new course + addition to the Cyber Security Certificate

Dear Rainer,

Mehrdad has provided 2 alternative titles for his course ("Software Aspects of Cryptography" or "Cryptographic Implementations") and modified his syllabus according to Koray's comments (with Red and Green colors) , such that to eliminate any overlap. He covers what Koray does *NOT* cover, i.e., software implementations, working with large integers, security proofs and applications of common topics (e.g., DES, AES, RSA and ELGamal).

Could you please check the attached syllabus, and let us know if the course in this form is acceptable for the Math Department?

Thank you,
Mihaela

From: Rainer Steinwandt [srainer@math.fau.edu]
Sent: Friday, October 28, 2016 2:40 PM
To: Mihaela Cardei
Cc: Nurgun Erdol; Yuan Wang
Subject: Re: Request for approval -- new course + addition to the Cyber Security Certificate

Dear Mihaela,

Thank you for your email. I have reached out to Nurgun and hope there'll be a chance to chat with her about this proposal.

Below are comments from Koray, and I share his concerns on the proposed course. It is easy to resolve the issue with a bit of tweaking. Especially in regard to the CAE certification across multiple Colleges (Koray is working with Ed and Elias on this at the moment) the proposed course is right now almost counterproductive: in view of the overlap with MAD 5474 taking both the proposed course and MAD 5474 isn't attractive for a student, but then some students miss out on material that is needed for the CAE certification. So it would be much more helpful to have an implementation (or/and protocol) focused course on top of MAD 5474 -- just as we have a math-heavier course on top of the widely accessible MAD 5474. Then everything would align nicely for the certification and we'd have complementing, almost overlap-free, courses for students who want to specialize and go beyond the basics.

Best,
Rainer

--

Hi Rainer,

I have looked at Mehrdad's comments on the comparison of CIS 5371 and MAD5474. In summary, the overlap seems non-trivial to me. I do see the need for a crypto course particularly designed for CS/ENG students with heavy implementation aspects. This is similar to our need for a crypto course particularly designed for MATH grads (MAD 6478, Cryptanalysis). I may be missing something but my suggestion is to keep MAD5474 as the introductory level course across MATH/CEECS/BUS/CCJ and offer 6-thousand level advanced courses in such as MAD 6478, CIS 6***, etc. This would also help us a lot with our CAE designation efforts and for its productivity.

For more detail, please find below my reasoning where I quote some text from Mehrdad's e-mail in italics:

*2.4: **partial** overlap DES; I don't cover security analysis, math proof, etc. I only cover algorithmic accepts for implementation.*

KK: Algorithmic aspects of DES (i.e. initial permutation, key scheduling, Feistel ladder structure, etc.) are covered in MAD5474. I should though note that students are not required to implement the full DES in MAD 5474. This applies to other (symmetric/asymmetric) algorithms as well.

*2.5 **partial** overlap AES; I don't cover security analysis, math proof, etc. I only cover algorithmic accepts for implementation.*

KK: My comment above also applies to this one: algorithmic aspects are covered in MAD5474. I should note that students are not required to implement the full AES. On the other hand, they go through analysis/input-output structures of Feistel-based ciphers with small number of rounds, (full) RC4 key-scheduling and keystream generation, etc.

*2.6 **partial** overlap ECB and CBC as I cover 4 other modes of operations.*

KK: The remaining modes of operations are covered in the Assignment 2.6. So, we cover all modes of operations in the course.

*5.2 **partial** overlaps RSA; I don't cover formal/math description, security analysis, math proof, etc. I only cover algorithmic accepts of RSA for implementation.*
KK: Algorithmic aspects of RSA are covered and in particular, students go through some toy examples of RSA encryption/decryption in the course and in the assignments.

*5.5 **partial** overlaps; ElGamal; I don't cover formal/math description, security analysis, math proof, ElGamal DS, etc. I only cover algorithmic accepts of ElGamal for implementation.*

KK: My comments on "5.2 RSA" apply here as well.

In addition, I should note that the audience of MAD 5474 used to be math majors/grads but this is not the case anymore. MAD 5474 has been redesigned for SCIENCE/CEECS/BUS/CCJ students. For this purpose, MAD 5474 will not have any prerequisite anymore. For more detail, I will make some notes on Mehrdad's comments below:

Math Aspect: *Math Departments mainly focus on* ***mathematical*** *aspects of RSA, how the mechanic works, formal (math) security definition, math security analysis though integer factoring and proofs, attack models and scenarios, etc, etc, etc.*
KK: We do not cover in-detail analysis of factoring algorithms anymore. More generally, MAD 5474 is not a typical MATH-course anymore.

CS Aspect: *CS Departments (like what I cover) mainly focus on algorithmic aspects of RSA: algorithms for generating random numbers, algorithms for primality test (Miller-Rabin algorithm), efficient algorithms for modular exp like Square-and-Multiply algorithm, algorithms for finding inverse (like EE algorithm); the computational complexity of these algorithms and Big-O notations, the implementation of these algorithms when dealing with large integer numbers, say 256 bits. How to prevent overflow in C/C++/Java for these large integers as compilers don't support those large integers, etc, etc, etc. All these sub-topics will be covered when I teach RSA.*
KK: In MAD 5474, we do cover algorithmic aspects and efficient algorithms such as square-and-multiply , finding inverses, and talk about complexity. We do not discuss overflows, large-integer arithmetic.

Engineering Aspect: *Engineering Departments (like what Reza is developing now) mainly focus on* ***hardware*** *implementation of RSA, how to find fast implementation solutions (hybrid implementation: software and hardware), etc etc etc the entire mechanic is going to be different when you work on engineering aspects of RSA and when you are dealing with a hardware platform. Reza can explain this better than me.*
KK: We do not cover any hardware implementation of algorithms in MAD 5474.

[4] In fact, Math course, my applied crypto *course and the one that* ***Reza is developing*** *are COMPLEMENT of each other as students learn crypto from 3 different aspects. Furthermore, some Math students may not have any interest in algorithmic aspects or implementation with C++/Java, or some CS students may not have interests in mathematical proofs, or some Eng students may only have interests in engineering aspects of crypto....that way we can accommodate everyone on FAU campus.*
KK: I would say from my experience in teaching MAD 5474 that most of our crypto-oriented grad students would be very much interested in and benefit from the hardcore implementation of crypto algorithms in C++/Java. As I commented earlier, MAD 5474 does not have any prerequisite and, in particular, we do not cover any "proofs" anymore.

Best,
Koray,
--

Best,
Rainer

From: "Mihaela Cardei" <mcardei@fau.edu>
To: "Rainer Steinwandt" <srainer@math.fau.edu>
Cc: "Nurgun Erdol" <erdol@fau.edu>, "Mehrdad Nojoumian" <mnojoumian@fau.edu>, "Yuan Wang" <YWANG@fau.edu>
Sent: Wednesday, October 26, 2016 12:24:27 PM
Subject: FW: Request for approval -- new course + addition to the Cyber Security Certificate

Hello Rainer,

I asked Dr. Mehrdad Nojoumian, who is proposing the course "CIS 5371 Applied Cryptography", to look at the overlap with MAD 5474, and he has prepared an explanation, please see below.

Based on this, do you approve this new course proposal and adding it to the CS Cyber Security courses?

Thank you,
Mihaela

From: Mehrdad Nojoumian [mnojoumian@fau.edu]
Sent: Wednesday, October 26, 2016 9:32 AM
To: Mihaela Cardei
Cc: Eduardo Fernandez; Nurgun Erdol; Reza Azarderakhsh
Subject: Re: FW: Request for approval -- new course + addition to the Cyber Security Certificate

Dear Mihaela,

I have already talked to Dr. Rainer and Koray but explain things again.

[1] I have attached the syllabus of MAD5474.

1.1 No overlaps
2.1 No overlaps
2.2 No overlaps
2.3 No overlaps

2.4: **partial** overlap DES; I don't cover security analysis, math proof, etc. I only cover algorithmic accepts for implementation.
2.5 **partial** overlap AES; I don't cover security analysis, math proof, etc. I only cover algorithmic accepts for implementation.
2.6 **partial** overlap ECB and CBC as I cover 4 other modes of operations.
3.1 I don't go through those attack on hash functions or their mathematical analysis; only algorithmic aspect of one or two hash functions for implementation.

3.2 no overlaps

4.1 no overlaps
4.1 general materials and don't see any significant overlaps

5.2 **partial** overlaps RSA; I don't cover formal/math description, security analysis, math proof, etc. I only cover algorithmic accepts of RSA for implementation.
5.3 no overlaps
5.4 no overlaps
5.5 **partial** overlaps; ElGamal; I don't cover formal/math description, security analysis, math proof, ElGamal DS, etc. I only cover algorithmic accepts of ElGamal for implementation.

In summary, DES, AES, RSA and ElGamal are common topics between my course and MAD5474, but you should first read [2, 3, 4] below to see that they are ***not*** even overlaps.

[2] For instance, lets focus on **RSA Topic:**

Math Aspect: Math Departments mainly focus on **mathematical** aspects of RSA, how the mechanic works, formal (math) security definition, math security analysis though integer factoring and proofs, attack models and scenarios, etc, etc, etc.

CS Aspect: CS Departments (like what I cover) mainly focus on **algorithmic** aspects of RSA: algorithms for generating random numbers, algorithms for primality test (Miller-Rabin algorithm), efficient algorithms for modular exp like Square-and-Multiply algorithm, algorithms for finding inverse (like EE algorithm); the computational complexity of these algorithms and Big-O notations, the implementation of these algorithms when dealing with large integer numbers, say 256 bits. How to prevent overflow in C/C++/Java for these large integers as compilers don't support those large integers, etc, etc, etc. All these sub-topics will be covered when I teach RSA.

Engineering Aspect: Engineering Departments (like what Reza is developing now) mainly focus on **hardware** implementation of RSA, how to find fast implementation solutions (hybrid implementation: software and hardware), etc etc etc the entire mechanic is going to be different when you work on engineering aspects of RSA and when you are dealing with a hardware platform. Reza can explain this better than me.

As you can see, the TOPIC IS COMMON (i.e., RSA) but DIFFERENT ASPECTS of it will be covered in each department.

[3] In all universities that offer crypto courses (without even a single exception; your can check MIT, Stanford, UWaterloo, UCSB, etc), these 3 courses (even more) are offered in different units. Even if there might be some overlaps (just the title of the TOPIC like RSA), the CONTENTS that are offered in each course regarding that topic are totally different.

[4] In fact, **Math course, my applied crypto** course and the one that **Reza is developing** are COMPLEMENT of each other as students learn crypto from 3 different aspects. Furthermore, some Math students may not have any interest in algorithmic aspects or implementation with

C++/Java, or some CS students may not have interests in mathematical proofs, or some Eng students may only have interests in engineering aspects of crypto....that way we can accommodate everyone on FAU campus.

Best Regards,
Mehrdad

Mehrdad Nojoumian
Assistant Professor
Florida Atlantic University
Department of CEECS
Office: EE 530 Tel: (561) 297-3411
http://faculty.eng.fau.edu/nojoumian/

On Tue, Oct 25, 2016 at 10:37 AM, Mihaela Cardei <mcardei@fau.edu> wrote:

Hello Mehrdad,

could you please compare your course with MAD 5474 and look at the overlap?
If the overlap is too large, you may need to adjust your course.

Could you please provide an answer for Dr. Steinwandt , chair of Math department?

thanks,
Mihaela

From: Rainer Steinwandt [rsteinwandt@math.fau.edu]
Sent: Tuesday, October 25, 2016 10:33 AM
To: Mihaela Cardei
Cc: Nurgun Erdol; Yuan Wang
Subject: Re: Request for approval -- new course + addition to the Cyber Security Certificate

Dear Mihaela,

Based on the course description, this course has substantial overlap with the existing MAD 5474 course. The latter is already part of the cyber security certificate -- and already fits what is needed in a CAE-compliant evolution of this certificate, on which our departments collaborate. So I do not think that in the current format the proposed Applied Cryptography course would be a good complement to what exists at FAU already or a good addition to the cyber security certificate.

Having said this, I liked the idea of "This course greatly relies on programming and implementation." For an implementation-focused course (maybe 6000-level?), there would

definitely be a need, but the course description does not reflect an implementation focus (e.g., topics like constant execution flow and timing attacks)

Best,
Rainer

From: "Mihaela Cardei" <mcardei@fau.edu>
To: "Rainer Steinwandt" <srainer@math.fau.edu>
Cc: "Mihaela Cardei" <mcardei@fau.edu>, "Nurgun Erdol" <erdol@fau.edu>
Sent: Tuesday, October 25, 2016 7:38:38 AM
Subject: Request for approval -- new course + addition to the Cyber Security Certificate

Dear Dr. Steinwandt,

The Department of Computer & Electrical Engineering and Computer Science (CEECS) is proposing a new courses:
CIS 5371 Applied Cryptography
and we want to add it to the Cyber Security Graduate Certificate, as part of the CS Cyber Security courses.

Attached are the course and the Cyber Security certificate related documents.

We need your approval that the Department of Mathematical Sciences has no objections to the new course proposal and to add it to the CS Cyber Security courses.
Could you please review the material and email me your approval decision?

Thank you,
Mihaela

Mihaela Cardei, PhD
Professor and Director Graduate Studies
Computer & Electrical Engineering and Computer Science Department
College of Engineering and Computer Science
Florida Atlantic University
http://www.cse.fau.edu/~mihaela