UNIVERSITY OF MARY WASHINGTON -- NEW COURSE PROPOSAL

Electronically submit this completed form with attachments in one file to the Chair of the College Curriculum Committee.

COLLEGE (check one):	**Arts and Sciences**	X	**Business**		**Education**	
Proposal Submitted By: Randall D. Helmstutler			Date Prepared: 9/26/2019			
Course Title:	Mathematical Cryptography					
Department/discipline and course number*:	MATH 453					
Prerequisites:	MATH 431					

**This course number must be approved by the Office of the Registrar before the proposal is submitted.*

Number of credits:	3	Will this course meet for at least 700 contact minutes for each credit hour proposed? ***If no, provide a credit hour justification.***	**YES**	X	**NO**	
Will this be a ***new***, *repeatable* "special topics" course? (Do you want students to be able to take this new course more than once if the topic changes?)			**NO**	X	**YES**	

Date of first offering of this ***new*** course: **FALL SEMESTER, year**	Spring 2021				
Proposed frequency of offering of the course:	Alternating years				
Proposed enrollment limit for the course:	15				
List the faculty who will likely teach the course:	Helmstutler, Lehman				
Are ANY new resources required?	**NO**	X	**YES**		*Document in attached impact statement*

**The earliest the course may be offered is the fall semester of the academic year FOLLOWING the year in which the course proposal is approved.

This new course will be (check all that apply):					
Required in the major		Required in the minor		General Elective	X
Elective in the major	X	Elective in the minor	X	General Education**	

***AFTER the new course is approved, a separate proposal must be sent to the General Education Committee.*

Catalog Description (suggested length – less than 50 words):

A rigorous development of modern encryption techniques from the group theory perspective, including private- and public-key systems, key exchange protocols, and digital signature schemes. Includes cryptanalysis by both classical message attacks and collisions. Credit for only one of MATH 253 or MATH 453 may count toward degree requirements.

COURSE HISTORY:	Was this course taught previously as a topics or experimental course?	**YES**	X	**NO**	
Course Number and Title of Previous Course		**Semester Offered**		**Enrollment**	
MATH 461Q: Cryptology		Fall 2016		17	
MATH 416Q: Cryptology		Spring 2019		18	

X **CHECK HERE** if the proposed course is to be ***equated*** with the earlier topics or experimental offerings. If equated, students who took the earlier "topics" course will only be able to take the new course as a repeat (C- grade or lower).

NOTE: If the proposed course has not been previously offered as a topics or experimental course, **explain in the attached rationale statement** why the course should be adopted even though it has not been tried out.

REQUIRED ATTACHMENTS:

1. **Rationale Statement** – Why is this course needed? What purposes will it serve?
2. **Credit Hour Justification** (if required) – explain how this course will comply with the UMW Credit Hours Policy (D.5.3)
3. **Impact Statement** – Provide details about the Library, space, staffing, budget, and technology impacts created by adding this new course. Include supporting statements from the Library, IT Department, etc. ***Any change that impacts another Department must have a written statement (such as an email) from the Chair(s) agreeing to the change.***
4. **Sample Syllabus**

Department Chair Approval*: Randall D. Helmstutler **Date:** 9/26/2019

CCC Chair Approval: **Date:** 10/7/19

***COB and COE proposals approved by the Associate Dean. *BEFORE* consideration by the UCC, the proposal must be approved the two levels noted above. Approval by the UCC and UFC are noted on the proposal "status history" at the UCC web site.**

Rationale

Cryptography is a relatively new area of mathematics, one that has become more prominent and visible due to the rise of e-commerce and related issues in data and identity security and cryptocurrency. We have offered this course twice as a special topics course (MATH 461Q), counting as an elective in the mathematics major. In both instances it over-enrolled, and it remains the most common course request I receive from our majors' annual survey. Past students in this course have gone on to complete research projects and external summer programs in cryptography, several of them presenting at regional and national mathematics conferences. Exposure to cryptography through this course has also helped place our students in intelligence careers. Given the impact of this course, we would like to make it a permanent addition to our curriculum, acting as an additional 400-level elective choice in the mathematics major and minor.

Impact Statement

This course has been offered twice with no impact on Library or IT resources. There are no issues with space or staffing. This will not change going forward. This course has no effect on any other programs.

Sample Syllabus

See the following pages.

Math 453: Mathematical Cryptography
Dr. Randall Helmstutler
Spring 2021

Meeting Times: 10:00–10:50 MWF
Location: Trinkle 119
Textbook: *An Introduction to Mathematical Cryptography* (2nd ed.) by Hoffstein, Pipher, & Silverman, © 2015 Springer-Verlag
Course Materials: `http://canvas.umw.edu`

Office: Trinkle 122
Phone: 654–1329
Email: `rhelmstu<at>umw<dot>edu`
Personal Webpage: `http://doctorh.umwblogs.org`
Office Hours: These may vary due to fluctuations in my own schedule. Up-to-date office hours may always be found on my personal webpage. Appointments are more than welcome. Currently, my office hours are:

MWF	1:30–2:30
T	10:00–12:00
Th	by appt only

Course Objectives: Cryptography is the art of hiding secret information inside of (hopefully very) hard mathematics problems. Done successfully, only authorized users possess the extra information needed to solve these hard problems and read our secrets; an intruder or eavesdropper finds these problems too hard to solve in their lifetime, thereby leaving our secrets safe. Nowadays, an "authorized user" is more likely to be a machine than a human being, as when you submit your credit card number to Amazon without thinking twice about it being intercepted: you trust that Amazon's website will encrypt your credit card number safely in such a way that a hacker watching your transmission cannot recover it.

Naturally, the sort of mathematics involved must either be inherently hard or computationally intense (or both!), making the mathematics of cryptology deeply interesting. In this class we will start at the beginning, studying the so-called *classical ciphers*, eventually working toward a complete understanding of modern *public key cryptography*, the class of protocols used today for web transactions, digital identity verification, and Bitcoin. Upon completion of this course, students will:

- understand the aspects of group theory and field theory central to modern cryptography;
- learn the mathematical formulations of various symmetric and public key encryption systems;
- understand the central problems in mathematics that currently provide security for encryption;
- be able to analyze standard message attacks and collision attacks on encryption systems;
- understand security issues and limitations of cryptographic protocols.

Required Software: First and foremost, you'll need a working LaTeX system for your personal computer. If this is ever a problem, each computer in the department lab in Trinkle B9 has a fully functional LaTeX system. You should take it as your first assignment to go to my personal webpage and follow the instructions in my LaTeX tutorial for acquiring a (free, or close to it) LaTeX environment. This will require four components, as outlined in my handout. Follow my instructions closely and installation should be easy. (In the past my students have been able to teach themselves LaTeX simply by following the exercises on my tutorial site.)

Secondly, you need to save the ECrypt.jar executable file somewhere on your PC where you won't easily lose it. I've put this file on our Canvas page, under the "Files" tab conveniently enough. We will need this only for the first few weeks of class, but it will be indispensable during this time. Since this is just a Java executable, you should update your computer's Java run-time environment while you're at it.

Lastly, you need a decent modular calculator for the entire semester. You will need this for class just as often as you will for homework. My personal favorite option is the $0.99 iPhone app called Modular, but I'm sure there are tons of good options out there. (For instance, ECrypt has a built-in modular calculator which works just fine, but I find it a little clunky.) If you have any questions about what to use here, please ask.

Grades: Your course grade will be computed from the following components according to the given weights:

Homework & quizzes	45%
Midterm exam	15%
Writing project	20%
Final exam	20%

Your end-of-semester letter grade will be assigned to your overall course average according to the following thresholds:

A	93	B–	80	D+	67
A–	90	C+	77	D	60
B+	87	C	73	F	< 60
B	83	C–	70		

Grades on exams and other assignments are not curved at any time. Experience has shown that I rarely need to adjust the grading scale at the end of the term, so do not rely on a curve to pad your grade.

Homework & Quizzes: We will have homework assignments on a regular basis, along with the occasional quiz to check your understanding of the basics. All such assignments are weighted equally and account for 45% of your final course grade. *Moreover, beginning with the second assignment, all graded homework sets must be formally typeset in LaTeX.* For a crash course in getting started with LaTeX, visit my personal webpage and follow my LaTeX tutorial.

Writing Project: In lieu of a second midterm exam, each student will write a mathematical paper on a topic of their choice in cryptology. These papers should not simply present a solution to a problem (that's what homework is for), but should be more self-contained and expository in nature. A list of suggested topics will be provided, and students are free to choose their own with the instructor's approval. As expected, papers must be compiled using LaTeX. More details and helpful advice on the writing project will be provided in class.

Final Exam: Our comprehensive final exam is scheduled for 8:30–11:00 a.m. on Monday, April 29th. I reserve the right to make the final exam either take-home or in-class (or a hybrid of both), with two weeks notice.

Midterm Grades: A midterm deficiency will be entered for any student with an F on any two assignments at the time midterm grades are due to the Registrar.

Make-up/Extension Policy: All dates and deadlines are firm. Any adjustment must be requested beforehand, with one week's notice whenever possible. An extension or make-up will be granted only for a legitimate reason. Otherwise, late work is never accepted. (It should be noted that placing something in my mailbox after class counts as being late.)

Attendance Policy: I do not take attendance formally, hence you will not be directly penalized for absences (unless, of course, you miss an in-class assignment due to your absence). In the event of an absence it is the student's responsibility, not the instructor's, to see that steps are taken to rectify any deficiencies that occur from missing class.

Etiquette: Class begins promptly at 10:00 and students are expected to be punctual. Use of electronic devices (especially phones) in class should be limited to actual class activities.

The Honor System: It goes without saying that the Honor System is deeply respected at this university and is strictly observed in this class. I will be very explicit about the groundrules for each assignment, but please talk to me if you have any questions about what is (or is not) allowed for any particular assignment.

Web/Email Updates: Important dates and other announcements will be addressed in class and posted on our Canvas page. You are expected to check your UMW email account and the class Canvas page regularly for the most up-to-date information.

Special Accommodations: If you have a documented disability that requires special accommodations in the classroom or testing environment, please let me know by Monday, January 28th. The Office of Disability Resources is located in Lee Hall.

Problems? Feel free to talk to me when you have concerns about the course, whether it is homework, concepts in general, or other course-related issues. If you have a conflict with my office hours, see me to schedule a private appointment.

Important Dates

January 18	Last day to add
January 21	No class (MLK Day)
February 1	Last day to drop
February 22	Midterm exam
March 4–8	No class (spring break)
March 22	Withdrawal deadline
April 29	Final exam

Course Content

Sections	Topics
1.1	Simple substitutions
1.7	Crypto, abstractly
1.3	Modular arithmetic
1.2	Euclidean algorithm
1.3	Invertibility in $\mathbb{Z}_n$
1.7.4	Affine ciphers
—	Euler's φ-function
5.2	Vigenère cipher
1.7	One-time pads
1.5	Primitive elements in $\mathbb{Z}_p$
2.3	Diffie-Hellman key exchange
2.2	Discrete log problem
1.3.2	Fast powering
3.3	MIM attack on DHKE
2.1	Public key crypto
3.1	Euler's theorem
3.1–3.2	RSA
3.3	Security of RSA, factorization
3.6	Difference of squares attack
2.7	Collision attacks
2.7	Baby-step/giant-step
2.4	ElGamal encryption
4.1–4.3	Digital signatures
	Zero-knowledge proofs