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.

	Arts and Sci	ences		Х	Busin	ess			Educa	atioi	n	
Proposal Submitted By	: Randall D. Hel	mstutler			Date P	repar	ed: 9/2	6/2019				
Course Title: Mather	natical Cryptogra	iphy										
Department/discipline a	and course numb	er*: MAT	H 453									
Prerequisites:		MAT	H 431									
*This course number mus	t be approved by t	he Office of th	e Registra	ar <u>befo</u>	ore the p	roposa	al is subr	nitted.				
Number of credits: 3	Will this cours	se meet for a oposed? If n	t least 7 o. provi	00 co i de a i	ntact mi credit h	inutes Iour i	for eac	h <i>tion.</i>	YES	Х	NO	
Will this be a new . repe	eatable "special t	opics" course	e? (Do vo	ou wa	nt stude	ents to	be abl	e to	NO	Х	YES	+
take this new course m	ore than once if	he topic cha	ngès?)						_			
Date of first offering of	this new course:		STER	voar	Sprir	na 20	21					
Proposed frequency of	offering of the co	ourse:	Alterna	atina v	/ears	ig 20.	21					
Proposed enrollment lin	mit for the course	:	15	<u></u>								
List the faculty who will	likely teach the	course:	Helms	tutler.	Lehma	n						
Are ANY new resourc	es required?	NO X	YES		Docun	nent il	n attach	ed imp	act stat	eme	ent	
**The earliest the course	may be offered is t	he fall semest	er of the a	acade	mic year	FOLL	OWING	the year	r in whic	h the	e cour	se
proposal is approved.												
This new course will	be (check all tha	it apply):			r							1
Required in the major		Required	in the m	inor			Genera	I Electi	ve			Х
Elective in the major	X	Elective in	n the mir	nor		Х	Genera	I Educa	ation**			
**AFTER the new course	is approved, a sep	arate proposa	l <u>must be</u>	senti	to the Ge	eneral	Educatio	n Comr	nittee.			
Catalog Description (suggested length	– less than	50 words	s):								
A rigorous developmen	t of modern encr	votion techni				hoon	/ noreno	ctivo i	a a lu valiva	~ ~ ~		
		VI // II // // // E // // //	dues tro	m the	aroun t	TIECH \			ncillain	$(1 \ D)$	ivate-	-
and public-key systems	s kev exchange	protocols an	ques fro d digital	m the signa	e group t iture sch	neory	s Inclue	des crv	nciudin otanalv	g pr vsis l	ivate-	- th
and public-key systems	s, key exchange	protocols, an	ques fro d digital only one	m the signa	e group t iture sch ATH 25:	neory nemes 3 or N	ATH 45	des cry 53 may	nciudin ptanaly count f	g pr sis l towa	ivate- by bo ard	- th
and public-key systems classical message atta degree requirements.	s, key exchange cks and collisions	protocols, an s. Credit for	dues fro d digital only one	m the signa of M	e group t iture sch ATH 253	neory nemes 3 or N	ATH 45	des cry 53 may	ptanaly count f	g pr sis l towa	by bo ard	- th
and public-key systems classical message attac degree requirements.	s, key exchange cks and collisions	protocols, an	dues fro d digital only one	m the signa of M	e group t iture sch ATH 253	aneory nemes 3 or N	ATH 45	des cry 53 may	ptanaly count	g pr sis l towa	by bo ard	- •th
and public-key systems classical message atta- degree requirements.	key exchange cks and collisions Was this course experimental of	e taught prev	dues fro d digital only one	m the signa of M/	e group t iture sch ATH 253	3 or M	ATH 45	des cry 53 may	nciudin ptanaly count f	g pr rsis l towa	by bo ard	- oth
and public-key systems classical message atta degree requirements.	Was this course experimental co	e taught prevourse?	dues fro d digital only one iously as	m the signa of M s a top	e group t iture sch ATH 253 pics or	3 or M	ATH 45	des cry 53 may	NO	g pr rsis l towa	ard	- oth
and public-key systems classical message attac degree requirements. COURSE HISTORY: Course Number and	Was this course experimental co	e taught prev course? course	dues fro d digital only one iously as	m the signa of M/	e group t iture sch ATH 253 pics or	3 or M YE Se Of	S mester	Ales cry 53 may	NO	g pr sis l towa	ivate- by bo ard	- oth
and public-key systems classical message atta degree requirements. COURSE HISTORY: Course Number and MATH 461Q: Cryptolog	Was this course experimental co Title of Previous	e taught prevourse?	dues fro d digital only one iously as	m the signa of M	e group t ture sch ATH 253 pics or	3 or M YE Se Of Fa	S mester fered	X	NO Enro	g pr rsis l towa	ent	- oth
and public-key systems classical message atta- degree requirements. COURSE HISTORY: Course Number and MATH 461Q: Cryptolog MATH 416Q: Cryptolog	Was this course experimental co Title of Previous	e taught prevourse?	dues fro d digital only one	m the signa of M, s a top	e group t ture sch ATH 253 pics or	YE Se Of Fa Sp	mester fered 12016 ring 201	3 may	NO 17 17 18 NO 17 18	g pr rsis l towa	ent	- th
and public-key systems classical message atta degree requirements. COURSE HISTORY: Course Number and MATH 461Q: Cryptolog MATH 416Q: Cryptolog	Was this course experimental co Title of Previous	e taught prevourse?	dues fro d digital only one iously as	m the signa of M,	e group t ture sch ATH 253 pics or	YE Se Of Fa Sp	mester fered 12016 ring 201	9	NO 17 17 18 NO	g pr rsis l towa	ent	- bth
and public-key systems classical message atta degree requirements. COURSE HISTORY: Course Number and MATH 461Q: Cryptolog MATH 416Q: Cryptolog X CHECK HERE if the	Was this course experimental co Title of Previous gy	is to be equat	dues fro d digital only one iously as	m the signa of M/ s a top	e group t ture sch ATH 253 pics or	YE Se Of Fa Sp s or ex	mester fered II 2016 ring 201	des cry 53 may X 9 tal offer	NO NO 17 18 ings. If	g pr rsis l towa llme	ent	- bth
and public-key systems classical message atta- degree requirements. COURSE HISTORY: Course Number and MATH 461Q: Cryptolog MATH 416Q: Cryptolog X CHECK HERE if the students who took t	Was this course experimental co Title of Previous gy gy	is to be equat	dues fro d digital only one iously as	m the signa of M s a top	e group t ture sch ATH 253 pics or lier topics e the new	YE Se Of Fa Sp s or ex y cours	S mester fered 12016 ring 201 sperimen se as a r	ales cry 53 may 53 may 53 may 53 may 53 may 53 may 54 may 53 may 54 may 55 may 55 may 56 may 57 may 59 may 59 may 59 may 59 may	NO NO Enro 17 18 ings. If 2- grade		ated,	
and public-key systems classical message atta- degree requirements. COURSE HISTORY: Course Number and MATH 461Q: Cryptolog MATH 416Q: Cryptolog X CHECK HERE if the students who took the NOTE: If the proposed co	Was this course experimental co Title of Previous gy gy gy	is to be equat	dues fro d digital only one iously as	m the signa of M s a top	e group t iture sch ATH 253 pics or lier topics e the new s or expension	YE Se Of Fa Sp s or ex y cours	s. Inclue ATH 45 S mester fered Il 2016 ring 201 operimen se as a re al course	3 may 3 may 3 may 3 may 4 X 9 9 tal offer epeat (C e, expla	NO Transport NO Enro 17 18 ings. If C- grade in in the	g pri rsis l towa llime equa e or la	ated, ower).	- th
and public-key systems classical message atta- degree requirements. COURSE HISTORY: Course Number and MATH 461Q: Cryptolog MATH 416Q: Cryptolog X CHECK HERE if the students who took th <u>NOTE:</u> If the proposed co rationale statement why	Was this course experimental co Title of Previous gy gy gy e proposed course he earlier "topics" of urse has not been the course should	is to be equat ourse will only previously offe	dues fro d digital only one iously as iously as riously as riously as riously as	m the signa of M, s a top s a top to take topics h it ha	e group t ture sch ATH 253 pics or lier topics e the new s or expenses s not bee	YE Se Of Fa Sp s or ex y cours riment en trie	mester fered Il 2016 ring 201 se as a ri al course d out.	9 tal offer epeat (C e, expla	NO Final Fin	g pr sis l towa llime equa e or la e att	ated, ower).	
and public-key systems classical message atta- degree requirements. COURSE HISTORY: Course Number and MATH 461Q: Cryptolog MATH 416Q: Cryptolog X CHECK HERE if the students who took th NOTE: If the proposed co rationale statement why REQUIRED ATTACHM	Was this course experimental co Title of Previous gy gy gy e proposed course ne earlier "topics" of urse has not been the course should IENTS:	is to be equat ourse will only previously offe	dues fro d digital only one iously as iously as red with th be able ered as a ven thoug	m the signa of M s a top s a top to take topics h it ha	e group t iture sch ATH 253 pics or lier topics e the new s or expenses as not bee	YE Se Of Fa Sp sor ex y cours riment en trie	mester fered II 2016 ring 201 se as a n al course d out.	9 tal offer epeat (C e, expla	NO Enro 17 18 ings. If C- grade in in the	g pr sis l towa llme equa e or la e att	ent	- th
and public-key systems classical message attac degree requirements. COURSE HISTORY: Course Number and MATH 461Q: Cryptolog MATH 416Q: Cryptolog X CHECK HERE if the students who took the statement why REQUIRED ATTACHN 1. Rationale Statement	Was this course experimental co Title of Previous gy gy gy e proposed course ne earlier "topics" co urse has not been the course should IENTS: t – Why is this cou	is to be equat previously offe be adopted ev	dues fro d digital only one iously as iously as viously as red with th <u>v be able</u> ered as a ven thoug	m the signa of Ma s a top s a top to take topics h it ha	e group t ture sch ATH 253 pics or pics or lier topics e the new s or expension s not been will it serv	YE Se Of Fa Sp v cours riment en trie	mester fered Il 2016 ring 201 se as a ro al course d out.	9 tal offer epeat (C e, expla	NO Enro IT	equa	ated, by bo ard	- bth
and public-key systems classical message atta- degree requirements. COURSE HISTORY: Course Number and MATH 461Q: Cryptolog MATH 416Q: Cryptolog X CHECK HERE if the students who took th <u>NOTE:</u> If the proposed co rationale statement why REQUIRED ATTACHM 1. Rationale Statement 2. Credit Hour Justific	Was this course experimental co Title of Previous gy gy gy te proposed course ne earlier "topics" of urse has not been the course should IENTS: t – Why is this cou ation (if required) -	is to be equat ourse will only previously offe be adopted ev rse needed? V	dues fro d digital only one iously as iously as red with th v be able ered as a ven thoug Vhat purp this cours	m the signa of Ma s a top s a top to take topics h it ha	e group t ture sch ATH 253 pics or lier topics e the new s or expen- s not been will it serv comply v	YE Se Of Fa Sp s or ex y cours riment en trie	s. Includ IATH 45 S mester fered Il 2016 ring 201 operimen se as a ro al course d out.	2 2 3 3 3 3 3 3 3 3 3 3 3 3 3	NO Enro 17 18 ings. If <u>C- grade</u> in in the	g pr sis l towa llme equa e or lo e att	ent ated, ower). acheo	-
and public-key systems and public-key systems classical message attac degree requirements. COURSE HISTORY: Course Number and MATH 461Q: Cryptolog MATH 416Q: Cryptolog X CHECK HERE if the students who took the students who	Was this course experimental co Title of Previous gy gy gy the proposed course ne earlier "topics" of urse has not been the course should IENTS: t – Why is this cou ation (if required) - Provide details abo	is to be equat ourse will only previously offe be adopted ever rse needed? V - explain how our the Library	dues fro d digital only one iously as iously as red with th be able ered as a ven thoug What purp this cours , space, s	m the signa of Ma s a top s a top to take topics h it ha oses v staffing	e group t ture sch ATH 253 pics or lier topics e the new s or expen- s not been will it serv comply v g, budget	YE Se Of Fa Sp s or ex y cours riment en trie	s. Inclue ATH 45 S mester fered Il 2016 ring 201 perimen se as a re al course d out.	9 tal offer epeat (C e, expla	NO Enro 17 18 ings. If c- grade in in the ours Po octs crea	g pr sis l towa equa e or la e or la e att	ated, ower). acheo	- bth
and public-key systems classical message atta- degree requirements. COURSE HISTORY: Course Number and MATH 461Q: Cryptolog MATH 416Q: Cryptolog X CHECK HERE if the students who took th <u>NOTE:</u> If the proposed co rationale statement why <u>REQUIRED ATTACHM</u> 1. Rationale Statement 2. Credit Hour Justific 3. Impact Statement – adding this new cours another Department	Was this course experimental co Title of Previous gy gy gy gy te proposed course he earlier "topics" of urse has not been the course should IENTS: t – Why is this cou ation (if required) - Provide details above and the course support	is to be equat ourse will only previously offe be adopted ev rse needed? V - explain how out the Library ting statement	dues fro d digital only one iously as iously as red with th be able ered as a ven thoug What purp this cours , space, s ts from th	m the signa of M, s a top s a top to take topics h it ha oses v se will staffing e Libra	e group t ture sch ATH 25: pics or lier topics e the new s or expen- s not been will it services comply v g, budget ary, IT De	YE Se Of Fa Sp sores y cours riment en trie	mester fered Il 2016 ring 201 perimen se as a ri al course d out.	9 tal offer epeat ((e, expla	NO Count 1 NO Enro 17 18 ings. If C- grade in in the ours Po ours Po ours create bange to ban	g pr sis l towa litowa equa e or la e att licy (ited hat <i>i</i> ,	ated, by bo ard ant ated, by acheo (D.5.3 by mpac	d d
and public-key systems classical message attac degree requirements. COURSE HISTORY: Course Number and MATH 461Q: Cryptolog MATH 416Q: Cryptolog MATH 416Q: Cryptolog X CHECK HERE if the students who took the stu	Was this course experimental co Title of Previous gy gy gy e proposed course ne earlier "topics" co urse has not been the course should IENTS: t – Why is this cou ation (if required) - Provide details abo se. Include suppor	is to be equat ourse will only previously offe be adopted ev rse needed? V - explain how out the Library ting statement	dues fro d digital only one iously as iously as iously as ver thoug vhat purp this cours , space, s ts from th <i>t</i> (such a	m the signa of Ma s a top s a top s a top to take topics h it ha oses v se will staffing e Libra	e group to ture sch ATH 253 pics or pics or lier topics e the new s or expension s not been s not been will it serv comply w g, budget ary, IT De email) from	YE Se Of Fa Sp s or ex y cours riment en trie	mester fered II 2016 ring 201 coperiments a coursed d out.	9 tal offer epeat (C e, expla	NO Enro 17 18 ings. If <u>C- grade</u> in in the ours Po tots creation of the bange to	g pr sis l towa litowa equa equa e or lo e att licy (hat i the c	ated, by bo ard ard ated, <u>ower).</u> acheo (D.5.3 by mpac chang	
and public-key systems classical message atta degree requirements. COURSE HISTORY: Course Number and " MATH 461Q: Cryptolog MATH 416Q: Cryptolog MATH 416Q: Cryptolog X CHECK HERE if the students who took to took to	Was this course experimental co Title of Previous gy gy gy gy te proposed course he earlier "topics" of urse has not been the course should IENTS: t – Why is this course ation (if required) - Provide details above se. Include support t must have a write	is to be equat ourse? course course is to be equat ourse will only previously offe be adopted ev rse needed? V - explain how out the Library ting statement	ques fro d digital only one iously as iously as iously as <i>ted</i> with th <u>t</u> be able ered as a ven thoug What purp this cours , space, s is from th <u>t</u> (such a	m the signa of M, s a top s a top to take topics h it ha oses v se will staffing e Libra	e group t ture sch ATH 25: pics or lier topics e the new s or expen- s not been will it services comply w g, budget ary, IT De- email) from	YE Se Of Fa Sp sores v cours riment en trie ve? vith the t, and epartm om the	s. Includ ATH 45 S mester fered Il 2016 ring 201 ring 201 sperimen se as a ri al course d out.	9 tal offer epeat (C e, expla	NO Count 1 NO Enro 17 18 ings. If C- grade in in the ours Po ours Po ours create bange ti taing to a count 1	g pr sis l towa litowa equa cor la e att licy (lited hat i the c	ated, by bo ard ated, by ated, by acheo (D.5.3 by mpac chang	
and public-key systems classical message atta degree requirements. COURSE HISTORY: Course Number and MATH 461Q: Cryptolog MATH 416Q: Cryptolog X CHECK HERE if the students who took th NOTE: If the proposed co rationale statement why REQUIRED ATTACHN 1. Rationale Statement – adding this new cours another Department 4. Sample Syllabus Department Chair App	Was this course experimental co Title of Previous gy gy gy e proposed course ne earlier "topics" co urse has not been the course should IENTS: t – Why is this cou ation (if required) - Provide details abo se. Include suppor t must have a write proval*:- <u>Randal</u>	is to be equat ourse will only previously offe be adopted even se needed? V - explain how out the Library ting statement ten statement	dues fro d digital only one iously as iously as iously as <i>ted</i> with th <i>t</i> <u>be able</u> ered as a ven thoug Vhat purp this cours , space, s is from the <i>t</i> (such a ider	m the signa of Ma s a top s a top s a top to take to t	e group t ture sch ATH 253 pics or lier topics e the new sor expension sor ot been will it serv comply w g, budget ary, IT be som ail) from	YE Se Of Fa Sp Sor ex Cours riment en trie	s. Includ IATH 45 S mester fered Il 2016 ring 201 ring 201 course d out. e UMW (technolo hent, etc. e Chair(s Date:	2 Stredit H 2 Str	NO Enro 17 18 ings. If <i>C-</i> grade in in the ours Po cts creation of bange to bange to bange to bange to	g pr sis l towa litowa equa equa e or lo e att	ated, ower). acheo (D.5.3 by mpac chang	- th
and public-key systems classical message atta degree requirements. COURSE HISTORY: Course Number and MATH 461Q: Cryptolog MATH 416Q: Cryptolog MATH 416Q: Cryptolog X CHECK HERE if the students who took th NOTE: If the proposed co rationale statement why REQUIRED ATTACHM 1. Rationale Statement 2. Credit Hour Justific 3. Impact Statement – adding this new cours another Department 4. Sample Syllabus Department Chair App CCC Chair Approval:	Was this course experimental co Title of Previous gy gy gy e proposed course ne earlier "topics" co urse has not been the course should IENTS: t – Why is this cou ation (if required) - Provide details abo se. Include suppor t must have a write proval*: Randal	is to be equat ourse vill only previously offe be adopted ev se needed? V - explain how out the Library ting statement ten statement	ques fro d digital only one iously as iously as iously as ven thoug Vhat purp this cours , space, s is from th <i>t</i> (such a ider	m the signa of M, s a top s a top to take topics h it ha oses v se will staffing e Libra	e group t ture sch ATH 25: pics or lier topics e the new s or expension is not been will it server comply v g, budget ary, IT De email) free	YE Se Of Fa Sp sor ex y cours riment en trie	S Include Include	2 Stredit H 2 Str	NO Enro 17 17 18 ings. If C- grade in in the ours Po octs create hange to 2019 19	g pr sis l towa lowa equa equa e or lo e att	ated, by bo ard and ated, <u>ower).</u> acheo chang	

*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.

New Course Proposal Cover Sheet (July 2018)

<u>Rationale</u>

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
Т	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:

А	93	B–	80	D+	67
A–	90	C+	77	D	60
B+	87	С	73	F	< 60
В	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 $\mathbb{A}T_{\mathrm{E}}X$. For a crash course in getting started with $\mathbb{A}T_{\mathrm{E}}X$, visit my personal webpage and follow my $\mathbb{A}T_{\mathrm{E}}X$ 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.

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

Important Dates

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

Course Content