Math 3320 - Error-Correcting Codes and Cryptography

Syllabus

Spring 2019

1 Course Information

Instructor:	Alex Cameron
Email:	alexander.cameron@vanderbilt.edu
Office:	SC 1224
Office Hours:	Wednesdays 10-11, Thursdays 9-11, or by appointment
Course Webpage:	Brightspace
Meeting Time:	MWF 11-12
Meeting Location:	SC 1431
Textbook 1:	*A First Course in Coding Theory* by Raymond Hill
Textbook 2:	*Introduction to Modern Cryptography* by Katz & Lindell (2nd Ed.)
Prerequisites:	MATH 2410, MATH 2600, or MATH 2501.

2 Course Description

Applications of algebra to reliability and secrecy of information transmission. Error-correcting codes, including linear, Hamming, and cyclic codes, and possibly BCH or Reed-Solomon codes. Cryptography, including symmetric-key, DES and RSA encryption.

This semester we will try to make it through Chapters 1-9 and 11-12 of the coding theory text and Chapters 1-6, 8, 10, and 11 from the cryptography text. Certain chapters might get cut depending on time.

3 Quizzes and Course Grade

The grade for this course will be entirely based on weekly quizzes. Every Friday before the final full week of class I will give a quiz consisting of two questions. One question will be similar (or identical) to a problem the problem set assigned on the previous Friday. The other question will, in general, be new but based on the material covered in the previous week. On the final full week of class I will give the quiz on Monday because of Vanderbilt's ban on quizzes during dead week. There will be 14 quizzes given in all and each will be worth 10 points. Your final grade for the course will be the sum of your ten highest quiz scores. The final letter grade will be assigned according to the following table:

A	93-100	B+	87-89	C+	77-79	D+	67-69	F	0-59
A-	90-92	B	83-86	C	73-76	D	63-66		
		B-	80-82	C-	70-72	D-	60-62		

4 Problem Sets

I will assign problems every week. These problems will not be collected or graded (though I am happy to review any solutions you would like me to check). However, working problems outside of class is one of the most important things you can do to learn the material and ace the quizzes. So please work the problems!

5 Absences

There will be no formal participation component for this course. The only way that absences can negatively impact your grade in the course is if you need to miss a large number of quizzes. The number of quizzes dropped at the end of the semester already takes into account that a student might need to miss an occasional class. If you end up having a documented reason for missing more than four quizzes during the semester, then please let me know as soon as possible.

6 Honor Code

Vanderbilt's Honor Code definitely applies to this course!

7 A Message from the Math Department

"The Open Enrollment Period ends on Monday, January 14th. This is the deadline for students to add a course or to make other changes in YES. Between January 15th and January 21st, any withdrawals or adjustments in level or in grading status must be completed using the add/drop form. If only the "DROP" section of the form is filled out, the instructor may sign the form. If a student wishes to make any change that involves filling in the "ADD" section of a drop/add form (whether or not it also involves filling in the "DROP" section), then the student must see the DUS (John Rafter) or the Assistant DUS (Jakayla Robbins) in person. Per Math Department policy, the only change to a math course that will be approved is a change to the level of the course (e.g. switching from Math 1301 to Math 1300 or vice versa). "