MA 591 Section 004, 2019 Spring Semester

Cryptography

December 18, 2018

I. Course information:
Time T. T. 4:30-5:45
Classroom: 216 Daniels
Instructor: Ernie Stitzinger, SAS 4121, stitz@ncsu.edu, 919-515-3258
Technology Expert: Katie Ahrens, kaahrens@ncsu.edu
Webpage: https://stitz.wordpress.ncsu.edu/ma-591-cryptography

Text: An Introduction to Mathematical Cryptography by Jeffrey Hoffstein, Jill Pipher, Joe Silverman. Springer UTM
Supplemental Texts:
1.An Introduction to Number Theory and Cryptography, Neal Koblitz, Springer GTM
2.Introductory Algebraic Number Theory, Saban Alaca and Kenneth Williams, Cambridge University Press

II. Course stream:
The course will study classical and new public key cryptography. Systems, whose hardness is based on factoring, such as RSA; discrete logs in abelian groups , such as the Diffie-Hellman key exchange and El-Gamal with elliptic curves; lattices, such as NTRU and ring learning with errors, will be featured. Featured also will be the standard attacks on these systems.

The grade will be based on homework. +/- grading will be used.

It will be necessary to use a computer algebra system such as MAPLE, SAGE or PYTHON. Help can be obtained in this regard as Katie Ahrens (kaahrens@ncsu.edu) will be available to assist.

III. Student Learning Outcomes:
To learn the ideas of security systems; what makes them good or not so good. The interplay between functionality and security. What are the currently studied problems.

The influence of the pending quantum computer on todays research. The interplay of pure and applied mathematics in an extremely significant area of research is a highlight. Job market preparation.

IV. Statement for students with disabilities:

Reasonable accomodations will be made for students with disabilities. In order to take advantage of avalable accomodations, students must register with Disability Services for Studnts at 1900 Student Health Center, Campus Box 7509, 919-515-7653. For more information, please see the Academic Accomodations for Students with disabilities Regulation (REG 02.20.01)

V. N.C.State University Policies, Regulations, and Rules:

Students are responsible for reviwing the PRRs which pertain to their course rights and responsibilities. These incluse: http://policies.ncsu.edu/policy/pol-04-25-05 (Equal Opportunity and Non-Discrimination Policy Statement), http://oied.ncsu.edu/oied/policies.php (Office for Institutional Equity and Diversity). http://policies.ncsu.edu/policy/pol-11-35-01 (Code of Student Conduct), and http://policies.ncsu.edu/regulation/reg/02-05-03 (Grades and Grade Point Average).