Cryptography Course Syllabus

Instructor

My name is Dr. Frank Ferrese. Welcome to Cryptography. If you are having trouble or need help with an assignment, or a concept that was covered in class, you can email me at frank.ferrese@gmail.com. I normally respond within 24 hours, often much sooner.

Objective

This class had two main objectives. First, we will gain an understanding of how a number of cryptographic primitives work learn how to use these primitives in application. Second, we will study the application of cryptography in the context of IP based networks.

Required Texts

Cryptography and Network Security, Principles and Practice (Stallings)
Publisher: Prentice Hall
ISBN-13: 978-0-13-335469-0
A Handbook of Applied Cryptography (Menezes, van Oorschot, Vanstone)
Available online

Attendance Policy

Attendance at all exams is mandatory. If you can not make an exam due to extenuating circumstances, you must let me know before the day of the exam.

Assignments and Grading

Grading will be based on a projects, homework, and on examinations. The grading will be as follows:

Exams	40%
Homework	20%
Programming Projects	40%

F $<$ 60% $<$ D- $<$ 62% $<$ D $<$ 65% $<$ D+ $<$ 70% $<$ C- $<$ 72% $<$ C $<$ 75% $<$ C+ $<$ 80% $<$ B- $<$ 83% $<$ B $<$ 85% $<$ B+ $<$ 90% $<$ A- $<$ 93% $<$ A

All assignments must be turned in on Blackboard on time. Late assignments will not be graded. Please turn in all assignments as a single pdf file. Make sure they are neat and professional! Code should be included as an appendix to your report if you wrote code as part of the assignment. Problem sets must be turned in with the problems in order, right side up and legible. Do not turn in anything that is not high enough quality to be given to your employer or client.

List of Topics

- Symmetric Ciphers (DES, AES, Block Cipher operations)
- Number Theory
- Asymmetric Ciphers (Public key Cryptography, RSA, Diffie Hellman Key exchange etc.)
- Data Integrity Algorithms (Hash functions, MAC, Digital Signatures)
- Key Management and Authentication
- Network and Internet Security (SSL, Wireless, Email, IP etc)

Academic Integrity

I take academic integrity very seriously. Villanova's policy can be found here:
https://www1.villanova.edu/villanova/vpaa/studentservices/policies/integrity/code.html