Syllabus

Instructor
Jens-Peter Kaps
Science and Tech II, 213
Phone: (703) 993-1611
jkaps@gmu.edu
http://ece.gmu.edu/∼jkaps

Teaching Assistant
Krishna Thirumalasetty
kthirum1@gmu.edu

Date & Time & Place
Wednesdays, 7:20pm–10:00pm, Robinson Hall B201

Course Web Page
The course web page will contain the latest announcements, handouts, assignments, source code and useful/interesting web links.
The web page is accessible via http://ece.gmu.edu/∼jkaps/courses/ece646

Textbooks

- William Stallings, *Cryptography and Network Security: Principles and Practice* by Prentice Hall; 4th edition, 2005, ISBN: 0-13-187316-4.
  If you already own the 3rd edition you don't have to by the 4th edition for this course. However, it is your responsibility to make sure that you read the corresponding material and that errors in the earlier edition do not create wrong results in assignments.

- A. J. Menezes, P. van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography.* CRC Press, 1997, ISBN: 0-84-938523-7.
  (all chapters of this book can be downloaded from the books web page)

You can find links to more interesting books on the class home page.

Prerequisite
Strong math background. Practical programming skills in C or C++.

Office Hours
Please check the class web page for the current office hour schedule. You should feel free to approach Dr. Kaps and the TAs at any time if you need help in addition to the scheduled sessions. The best way to contact us is via email.

Homework
There will be weekly homework assignments. These will include questions, and programming exercises. Homework must be handed in on time. If you can't make it to the class, please e-mail it to the TA. Homework handed in after solutions are posted will receive zero credit.

Laboratory Exercises
Laboratory exercises will involve getting familiar with selected implementations of cryptographic algorithms and protocols. Based on this knowledge and your own experiments, you will be asked to solve a set of simple problems, and prepare a short report including answers to the questions included in the instruction.

Project
An important part of this course is the semester project. The project should give an overview of a special topic in cryptography (e.g. side channel attacks, identity based encryption, biometric authentication systems, etc.) and will result in a report and a presentation. A list of possible presentation topics will be provided. Each project will be completed in groups of two. You are required to perform a literature study on the topic you have chosen and write a journal style report. Towards the end of the semester, you will be required to perform a final presentation of your project.

- **Report Due:** December 5th
- **Presentation:** December 19th

Examinations
There will be two exams during the course, a midterm exam and a final exam. The exams will be open book and open notes and contain a multiple choice test and short problems. The questions will range from mild to difficult.

- **Midterm Exam:** October 24th
- **Final Exam:** December 12th

Grading
The following weight distribution will be used to calculate the final grade:

- 15% Homework
- 15% Laboratory Exercises
- 15% Project
- 25% Midterm Examination
- 30% Final Examination

Topics

Historical ciphers	Digital signatures
Classical encryption (DES, RC5,...)	Public key certificates
Public key encryption (RSA, DH,...)	Secure Internet protocols (PGP, SSL,...)
Hash functions and MAC	Cryptographic standards