

# Network Security and Cryptography

CSI5105 / COMP5406

Winter, 2012

**Professor:** Carlisle Adams (SITE, Office 5035, office hours by appointment)

## Calendar Description

Advanced methodologies selected from symmetric and public key cryptography, network security protocols and infrastructures, identification, secret sharing, anonymity, intrusion detection, firewalls, defending network attacks, and performance in communication networks.

## Course Outline (tentative)

*Foundations of Modern Cryptography: formal security*

- Week 1 Introduction and motivation; syntax of encryption schemes; complexity
- Week 2 Semantic security; indistinguishability of encryptions
- Week 3 Constructions of secure encryption schemes; inadequacy of semantic security
- Week 4 Active attacks (CPA, CCA, CCA2); non-malleability

*Foundations of Modern Security: technologies for access control in network environments*

- Week 5 Introduction and motivation; architecture (components and interactions)
- Week 6 Engineering considerations (authentication, delegation, revocation, efficiency);
- Week 7 CORBA, X.509 Attribute Certificates; Web technologies for access control

*Foundations of Modern Privacy: technologies for private network interactions*

- Week 8 Introduction and motivation; anonymity, pseudonymity, veronymity
- Week 9 Onion routing, MIX networks, Crowds; private information retrieval
- Week 10 Privacy policies (P3P); privacy enforcement; privacy certificates

*Student presentations*

- Week 11-13 Student presentations

**Textbooks (recommended reading to obtain relevant concepts and background)**

- O. Goldreich, *Foundations of Cryptography: Volume II, Basic Applications*, Cambridge University Press, 2004 (draft chapters available for online download)
- O. Goldreich, *Foundations of Cryptography: Volume 1, Basic Tools*, Cambridge University Press, 2001
- W. Mao, *Modern Cryptography: Theory & Practice*, Prentice Hall, 2004
  
- B. Blakley, *CORBA Security: An Introduction to Safe Computing with Objects*, Addison-Wesley, 2000
- D. Ferraiolo, D. R. Kuhn, and R. Chandramouli, *Role-Based Access Control*, Artech House, 2003
- C. Adams, *Understanding PKI: Concepts, Standards, and Deployment Considerations, 2<sup>nd</sup> Ed.*, Addison-Wesley, 2003
  
- S. Brands, *Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy*, MIT Press, 2000
- J. C. Cannon, *Privacy: What Developers and IT Professionals Should Know*, Addison-Wesley, 2005
  
- W. Stallings and L. Brown, *Computer Security: Principles and Practice*, Pearson Prentice Hall, 2008
- C. Pfleeger and S. L. Pfleeger, *Security in Computing, 4<sup>th</sup> Ed.*, Prentice Hall, 2007
- D. Gollmann, *Computer Security, 2<sup>nd</sup> Ed.*, John Wiley & Sons, 2006

**Papers (required reading)**

Selected research papers & technical specifications in the course topics (to be specified in class)

**Grading Scheme**

Assignments (3)	45%
Presentation (1)	15%
Final Examination	40%

## Assignments

- Assignment #1 due **2 weeks after the last class of the crypto unit**
- Assignment #2 due **2 weeks after the last class of the access control unit**
- Assignment #3 due **2 weeks after the last class of the privacy unit**
  
- An assignment for each of the 3 main topics of the course: cryptography; access control; privacy. For each assignment, the student must find a research paper that builds on the foundation presented in class (i.e., extends or takes the next logical step with respect to what we have discussed in some clear and easily-explained way). The student must submit a brief summary of the paper and its main results, along with a 2-3 paragraph discussion of how it builds on what we have done in class.
  
- Length: 3-5 pages (for each assignment)
  
- *NOTE: for those that may be interested, the final assignment can be replaced by an implementation or a critical assessment of a privacy enhancing technology (PET). The PET may currently exist or may be an original proposal. Please discuss with the course instructor if you would like to choose this option.*

## Presentation

- Must be in an area of network security (preferably not cryptography, access control, or privacy, although feel free to discuss with the instructor if you have a special request)
  
- Choose a research paper from a specified list of network security conferences
  
- Presentation must include sufficient background (problem description, survey of main results) for a listener who is familiar with security, but not an expert in the presented topic
  
- Provide a description of the research result(s) achieved in this paper, present a critique of the paper, and propose your own direction for improvement / enhancement of this work (i.e., what direction would you head if you wanted to publish something based on this paper?)
  
- Length: 20-30 minutes
  
- Topic must be **approved by Thursday, February 16**

## General Policies and Procedures

### Plagiarism

- will not be tolerated in any aspect of this course
- see [www.uottawa.ca/plagiarism.pdf](http://www.uottawa.ca/plagiarism.pdf) or [www.uottawa.ca/plagiat.pdf](http://www.uottawa.ca/plagiat.pdf)

### Academic Fraud

- see the following link for important information:  
[http://www.uottawa.ca/academic/info/regist/crs/0305/home\\_5\\_ENG.htm](http://www.uottawa.ca/academic/info/regist/crs/0305/home_5_ENG.htm) or  
[http://www.uottawa.ca/academic/info/regist/crs/0305/home\\_5\\_FR.htm](http://www.uottawa.ca/academic/info/regist/crs/0305/home_5_FR.htm)

### Academic Regulations

- Class attendance is mandatory. As per academic regulations, students who do not attend at least 80% of the classes will not be allowed to write the final examination.
- All components of the course (i.e., assignments, presentation, etc.) must be fulfilled otherwise students may receive an INC as a final mark (equivalent to an F).

### University of Ottawa

- Faculty of Engineering rules and regulations:  
[http://www.engineering.uottawa.ca/en/undergraduate/current\\_students/](http://www.engineering.uottawa.ca/en/undergraduate/current_students/) or  
[http://www.engineering.uottawa.ca/fr/undergraduate/current\\_students/](http://www.engineering.uottawa.ca/fr/undergraduate/current_students/)
- Important dates: <http://www.registrar.uottawa.ca/Default.aspx?tabid=3895#fall> or  
[http://www.registraire.uottawa.ca/Default.aspx?tabid=3894#Automne\\_2011](http://www.registraire.uottawa.ca/Default.aspx?tabid=3894#Automne_2011)

*Students must pass the final exam (i.e., obtain a mark of 50% or higher) in order to receive a passing grade on the course. Late work will receive a mark of zero.*