Instructor: Charles Rackoff  
SF2301D, (416)978-4106  
rackoff at cs dot toronto dot edu

Times: Lectures are Mondays 1-3, BA 2135  
In addition, some tutorials will be scheduled at an agreed time.

Tutor: Our TA will be Jaiganesh Balasundaram.

Web site:  [http://www.cs.toronto.edu/~rackoff/2426f18](http://www.cs.toronto.edu/~rackoff/2426f18)

Grading: There will be 4 assignments.

We will cover the fundamental material that is needed for creating or using cryptographic algorithms and protocols. The emphasis will be on rigorous definitions of security, and on constructions whose security can be proven from reasonable assumptions about the security of underlying, more primitive objects. This course contains the basic mathematical background of cryptography, and should be useful and interesting to computer scientists, electrical engineers, and mathematicians. Topics include:

- Pseudo-random generators and one-way functions  
- Secure sessions using a shared private session-key  
- Different kinds of cryptographic families of hash functions  
- Secure digital signature schemes  
- Secure public-key encryption  
- Secure session-key exchange  
- Maybe some "zero-knowledge" stuff

The text for the course will be **Course Notes** that will be available on the web site.

Here are two other texts that might be useful:

*Foundations of Cryptography: Basic Tools*
by Oded Goldreich  
Cambridge University Press

*Introduction to Modern Cryptography: Principles and Protocols*
by Jonathon Katz and Yehuda Lindell  
Chapman and Hall/CRC

However, keep in mind that these books will often use somewhat different notation and definitions than we do in this course.