Instructor: Charles Rackoff  
SF2301C, (416)978-4106  
rackoff at cs dot toronto dot edu

Times: Lectures are Wednesdays 3-5, BA B025  
In addition, some tutorials will be scheduled at an agreed time.

Tutor: If we are granted a T.A., it will be Jaiganesh Balasundaram.

Web site:  http://www.cs.toronto.edu/~rackoff/2426f14

Grading: There will be 4 assignments.

We will cover the following basic topics in Cryptography:

- 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 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. 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.