University of Toronto Mississauga
COURSE OUTLINE
MAT302 – Cryptography

Course homepage:
`http://www.math.toronto.edu/lgoldmak/`
Click on link to `Teaching`, then on the link to `MAT 302` under 'Currently Teaching'.

Instructor: Leo Goldmakher
Office: 4059B William Davis Building (aka South Building)
Phone: 905-569-4880
email: `leo.goldmakher@utoronto.ca`
Office hours: Tuesday 15:00–16:00 & Thursday 15:00 – 17:00; additional office hours by appointment.

Grader: ??
email: `??`

Lectures: Tuesday 12:10–13:00, NE 140 & Thursday 12:10–14:00, CC 2140

Textbook: C. Paar and J. Pelzl, *Understanding Cryptography*, Springer-Verlag, 2010

Syllabus: We will discuss various aspects of historical and modern cryptology. Topics covered will include substitution ciphers, shift register-based ciphers, DES and AES, RSA, Diffie-Hellman key exchange, the discrete logarithm problem, elliptic curve cryptosystems, digital signatures, and primality testing (possibly including the recent breakthrough by Agrawal-Kayal-Saxena). Although implementation will be discussed, we will focus on the mathematics involved in modern cryptography.

Marking scheme:
Your mark will be calculated based on the following three components:

1. Problem sets – 75%

   There will be five problems sets throughout the semester, each worth 15% of your final course mark.

2. Final exam – 20%

3. Participation – 5%

   From time to time, problems will be given during lecture to be worked on individually and submitted. The participation mark will depend solely on submission, *not* on correctness or completeness of the content. Note that you must be present (and conscious) for the entire duration of the 'quiz' to receive participation credit.

Continued on next page...

Team work and plagiarism:

I encourage you to work together on the problem sets. However, **each student must work out and write up their final solutions individually and independently**. Please write up your problems sets in isolation from other students.

Although the internet is a great resource, I urge you to use it wisely. In particular, I ask you not to search for the problems appearing on the assignments. The rule of thumb: **looking up definitions is OK, looking up solutions is not**.

When using ideas which are not your own, please indicate your source. You will *not* be penalized for collaborating with someone else, unless:

(1) your work is identical to that appearing elsewhere; or

(2) you explicitly use an idea without attributing the source.

Both (1) and (2) may have serious consequences. See

`http://www.utoronto.ca/writing/plagsep.html`

for further information.

Problem set policies:

Problem sets are to be handed in within the first five minutes of the lecture on which they are due. If you must be late to a lecture due to circumstances beyond your control, please contact me and (ideally) have another student submit the problem set on your behalf.

The academic regulations of the University are outlined in the Code of Behavior on Academic Matters which can be found at

`http://www.governingcouncil.utoronto.ca/policies/behaveac.htm`