Instructor: Leo Goldmakher

NAME: _____

University of Toronto Mississauga
Department of Mathematical and Computational Sciences

MAT 302: CRYPTOGRAPHY

Problem Set 1 (due January 27th, 2011 at the start of lecture)

INSTRUCTIONS: Please attach this page as the first page of your submitted problem set.

PROBLEM	MARK
1.1	
1.2	
1.3	
1.4	
1.5	
1.6	
Total	

Problem Set 1

NAME: _____

1.1 Decode the following encrypted messages.

(a) Scytale cipher:

TOHDAHNOBSIEUEYSSLE

(b) Caesar cipher:

MGEQIMWEAMGSRUYIVIH

(c) Substitution cipher:

VM KYS GOK JDOI, V GJVNU KYS RVFF PQ DPFQ GY MVZSOQ YSG RJDG GJVW WDKW

1.2 Prove that for all nice functions $f(x)$ and $g(x)$, $f(x) \sim g(x)$ if and only if $\log f(x) = \log g(x) + o(1)$. Give an appropriate interpretation of 'nice'.

1.3 In each of the following, determine which of the following relations hold:

$$f(x) \sim g(x), \quad f(x) = O\big(g(x)\big), \quad g(x) = O\big(f(x)\big), \quad f(x) \asymp g(x), \quad f(x) = o\big(g(x)\big), \quad g(x) = o\big(f(x)\big).$$

Justify your responses.

(a) $f(x) = 5x^3 - 1000x + 2$ and $g(x) = x^3 - 0.01$

(b) $f(x) = 1000x$ and $g(x) = x^3$

(c) $f(x) = x^{1000}$ and $g(x) = 2^x$

(d) $f(x) = \log x$ and $g(x) = x^{0.01}$

(e) $f(x) = x^{\log x}$ and $g(x) = (\log x)^x$

(f) $f(x) = (\log x)^{\log x}$ and $g(x) = x^{\log\log x}$.

1.4 In class, we proved that

$$\log N! = N\log N - N + \frac{1}{2}\log N + 1 + \int_1^N \Big(\{t\} - \frac{1}{2}\Big)\frac{dt}{t}.$$

Prove that

$$\int_1^N \Big(\{t\} - \frac{1}{2}\Big)\frac{dt}{t} = O(1).$$

As discussed in class, this implies that $N! \asymp \sqrt{N}\Big(\frac{N}{e}\Big)^N$.

[*Hint: you may wish to recall the alternating series test: $\sum a_n$ (with n running from 1 to ∞) converges if the a_n's alternate signs and tend to 0.*]

1.5 Consider the function

$$P(N) = 1 \times 2^{1/2} \times 3^{1/3} \times 4^{1/4} \times \cdots \times N^{1/N}.$$

Determine the rate of growth of $P(N)$, analogously to Stirling's formula.
[*No need to get an exact asymptotic; having the same rate of growth (i.e. an $\asymp$ result) is fine.*]

1.6 Euler discovered the following identity, valid for any nonzero x (measured in radians):

$$(*) \qquad \frac{\sin x}{x} = \prod_{n=1}^{\infty} \left(1 - \frac{x^2}{n^2\pi^2}\right).$$

(Recall that $\prod a_n$ is just the product of all the a_n's.) Euler used this to prove that

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}.$$

In this exercise, you will derive a different consequence: Stirling's formula.

(a) Using Euler's identity (*) or otherwise, prove that

$$\frac{(2N)!!}{(2N-1)!!} \sim \sqrt{\pi N}$$

where

$$(2N)!! = 2N \times (2N-2) \times (2N-4) \times \cdots \times 4 \times 2$$

and

$$(2N-1)!! = (2N-1) \times (2N-3) \times (2N-5) \times \cdots \times 5 \times 3 \times 1.$$

(b) Prove that

$$(2N)!! = 2^N N!$$

and

$$(2N-1)!! = \frac{(2N)!}{2^N N!}$$

(c) Prove Stirling's formula:

$$N! \sim \sqrt{2\pi N}\left(\frac{N}{e}\right)^N.$$

[*Hint: First prove that there exists a constant C such that $N! \sim C\sqrt{N}\left(\frac{N}{e}\right)^N$. Now use parts (a) and (b) to show that C must equal $\sqrt{2\pi}$.*]