Gmail

Mike Zabrocki <mike.zabrocki@gmail.com>

Mathematical Contest in Modelling

Jane Heffernan <jmheffer@mathstat.yorku.ca> **Tue, Jan 3, 2012 at 12:51 PM**
To: everyone+lnsapproval@mathstat.yorku.ca

Hello All,

Please make an announcement in your classes regarding the upcoming Mathematical Contest in Modeling (MCM).

The MCM is a contest where teams of undergraduates use mathematical modeling to present their solutions to real world problems. Each team can have a maximum of three members who work together to find a solution to one of three posed problems. The solution may include mathematics as well as computer simulation. The team must also write a report on their solution. Problems are designed to be open-ended and are unlikely to have a unique solution. Attention must be focused on clarity, analysis, and design of the solution.

The MCM will take place on February 9-13, 2012. If students have any questions regarding the MCM they may email me (jmheffer@mathstat.yorku.ca) or look at the MCM website http://www.comap.com/undergraduate/contests/ . If they are interested in participating they should email me by Jan 15. There will be an information/training session in late January.

Cheers,

Jane

--
Jane Heffernan
Centre for Disease Modelling
Mathematics& Statistics
York University
Toronto Canada

Mathematics of Cryptography

Course Description : Cryptography deals with the study of making and breaking secret codes.

In this course we will be studying situations that are often framed as a game between three parties: a sender (e.g., an embassy), a receiver (the government office) and an opponent (a spy). We assume that the sender needs to get an urgent message to the receiver through communication channels which are vulnerable to the opponent. To do this communication, the sender and receiver agree in advance to use some sort of code which is unlocked by a keyword or phrase. The opponent will be able to intercept the message. Is he/she able to unlock the message without knowing the key?

In this course we will learn some probability theory, information theory and number theory to answer questions about how vulnerable the methods of sending secrets are. This has a great number of applications to internet credit card transactions, wireless communication and electronic voting. We will start by learning some classical codes (used up through WWI) and analyzing those. The last third of the course we will start to learn the methods that are used in modern cryptography.

The course web page can be found at 4161user password: purple

http://garsia.math.yorku.ca/~zabrocki/math4161w12/

The grades are based on the following components:

Quizzes (drop lowest 1 of 5)	65%
Computer assignment	5%
Final exam	30%
Total	100%

Please note that the grades will be based on a curve and will not use the absolute grading scale.

Below is a rough schedule of how I expect this class to proceed for the first few weeks and important dates. You can expect to see this schedule revised as the course develops. You are expected to show up for lectures and be aware of any changes to the**tentative** schedule that I am providing for you here.

Lecture Schedule	Topics	Remarks
Tuesday, January 3	Introduction-Caesar, Vigenere	
Thursday, January 5	classical ciphers- Rectangular transposition, homophonic, Playfair	
Tuesday, January 10		Quiz 1
Thursday, January 12	classical ciphers- Hill, Vernam, ADFGVX, snail	
Tuesday, January 17	probability theory and the game of craps	
Thursday, January 19	infinite monkeys	
Tuesday, January 24		Quiz 2

Caesar Cipher

Plaintext: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Cyphertext: D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

Plaintext: ATTACK
DWWDFN

Key: R

Plaintext: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Cyphertext: R S T U V W X Y Z A B C D E F G H I J K L M N O P Q

Cyphertext: JVEU DFIV FIVFJ
SENDMORE OREOS

Caesar Cipher

WZOOZ HDYGZ M
XAPP IEZHAN
YBQQ JFAIBO
ZCRR KGBJCP
ADSS LHCKDQ
BETTEMIDLER
CFUV
DGVV
EHWX
FIXX
GJYY
HKZZ
ILAA
JMBB
KNCC
LODD
MPEE
NQFF
ORGG
PSHH
QTII
RVJJ
SVKK
TWLL
UXMM
VYNN

Vigenere Cipher

Key: HANKY   Silly rabbit, trix are for kids.

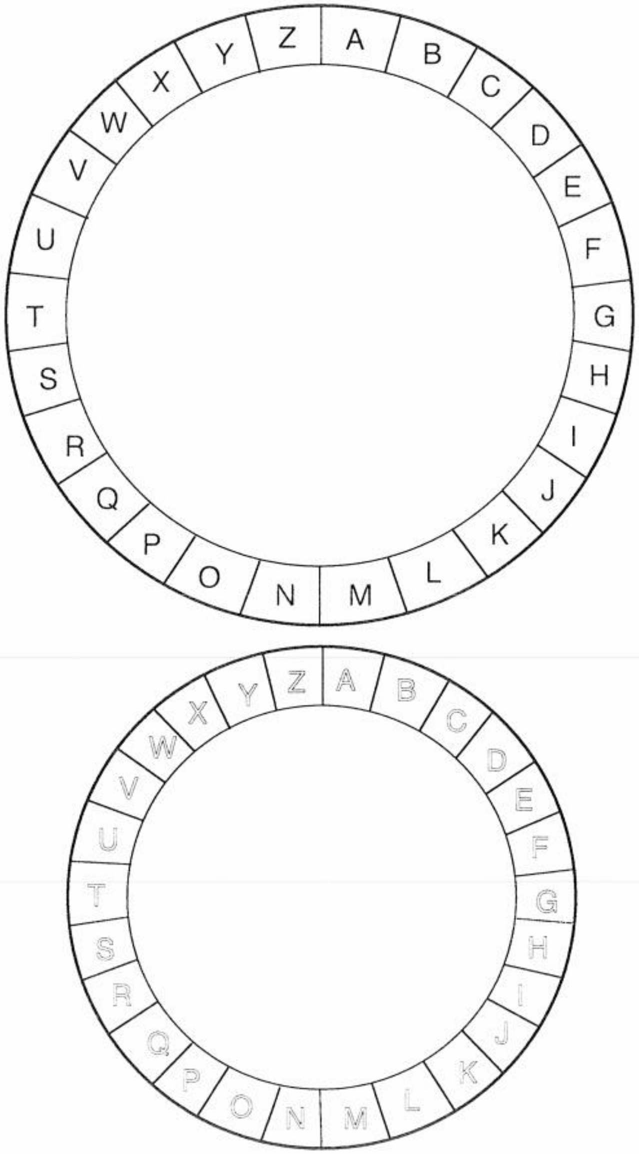
```
            HANKY HANKY HANKY HANKY HANKY
Plaintext:  SILLY RABBI TTRIX AREFO RKIDS

Cyphertext: ZIYVW YAOLG ATESV HRRPM YKVNQ
```

Key: QUIK

```
            QUIK QUIK QUIK QUIK Q
Cyphertext: TLQX ASWE HIDK BNQX U
```

DRINKYOUROVALTINE


A
B
C
D
E
F
G
H
I
J
K
L
M
N
O
P
Q
R
S
T
U
V
W
X
Y
Z