PMAT 329 – Quiz 2 – Fall 2004

October 20, 2004

Name:_____

Please DO NOT write your ID number on this page.

- **Duration:** 50 minutes
- **Total points: 50**
- Show **all** your work**.**
- **No aids allowed** except calculators.
- The following information may come in handy:

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
0	1	2	3	4	5	6	7	8	9	10	11	12
N	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
13	14	15	16	17	18	19	20	21	22	23	24	25

$$S_2 = \begin{cases} 0.0661 \text{ for English text} \\ 0.0385 \text{ for random text} \end{cases}$$

ID number:_____

ID number:_____

1.

a. [2 points] Define the term *equivocation*.

b. [2 points] What is the *absolute rate R* of a language with *L* characters

c. [2 points] What is the principle of *symmetry of position* used for

d. [2 points] Define what it means for a cryptosystem to provide *perfect secrecy*. (Give the *definition* only.)

e. [2 points] Name at least one cryptosystem that provides perfect secrecy (assuming each key is used with equal likelihood).

ID number:_____

2. [8 points] Is the following ciphertext monoalphabetically encrypted? Justify your answer.

DUPOZ PQPTQ OUFSS TJUJB ZBJTL

ID number:_____

3. For each method of encryption, decrypt the given ciphertext using the given key:

a. [4 points] Coherent Running Key Cipher, Ciphertext = VIZDZGZ,
Key = the text of this question (i.e. “for each method of encryption,…..”)..

b. [2 points] One time pad, Ciphertext = 110101, Key = 110001.

ID number:_____

4. [10 points] Suppose that I guessed that the keyword used for encrypting a Vigenère ciphertext has length 10. The following table gives the value of ϕ for each the 10 subtexts:

Subtext	1	2	3	4	5	6	7	8	9	10
Subtext length	62	62	62	62	62	62	61	61	61	61
ϕ	314	340	214	224	280	210	270	256	291	214

Decide whether my guess is correct. Show your computations and explain your reasoning.

ID number:_____

5. (a) [2 points] Given a set of n outcomes $X = \{ X_1, X_2, \ldots, X_n \}$ where X_i has probability $P(X_i)$ for $1 \leq i \leq n$, define the *entropy* $H (X)$ of X.

(b) [4 points] Suppose we have the following set of messages and their associated probabilities of being sent:

Message	*Sell all stocks*	*Buy Mutual funds*	*Buy gold*	*Buy internet stocks*	*Buy IBM stocks*	*Sell tech funds*
Probability	*1/16*	*1/4*	*1/8*	*1/16*	*1/4*	*1/4*

Compute the entropy of this set of messages.

ID number:_____

(c) Let $n = 2$ and suppose that $p(X_1) = p$ and $p(X_2) = 1 - p$.

i. [1 point] Write down $H(X)$ as a function of p.

ii.[1 point] What is the value of $H(X)$ for $p = 1/2$ (i.e. when X_1 and X_2 occur with equal probabilities)?

iii. [8 points] Prove that $H(X)$ is maximal if and only if $p = 1/2$.

ID number:_____

(part (c) continued)