PMAT 329 – Quiz 1 – Fall 2004

September 29, 2004

Name:_____

Please DO NOT write your ID number on this page.

- **Duration:** 50 minutes
- **Total points: 50**
- **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

ID number:_____

1. Define the following terms:

a. [2 points] encrypt

b. [2 points] substitution cipher

c. [2 points] authentication system

d. [2 points] cryptanalysis

e. [2 points] *n*-graph

2.

a. [3 points] What are the objectives of the cryptanalyst.

b. [6 points] Describe 3 types of cryptanalytic attack. Provide examples.

c. [3 points] List some means of cryptanalytic attack.

ID number:_____

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

a. [2 points] Caesar cipher, Ciphertext = WXYHIRX, Key = E.

b. [4 points] Vigenère cipher, Ciphertext = WCQDIPI, Key = KEY

c. [8 points] Hill cipher, Ciphertext = OKRU, *Encryption* Key = $\begin{pmatrix} 12 & 5 \\ 3 & 10 \end{pmatrix}$.

ID number:_____

4. [10 points] Decrypt the following Playfair ciphertext using the key MIDTERM. Show your work and present the plaintext without any nulls.

YXQKH DOSAL

ID number:_____

5. [4 POINTS] Give a mathematical formula for the ϕ-statistic. Be sure to define any symbols you use.