PMAT 329 — Midterm — Fall 2004

November 10, 2004

Name:_____

Please DO NOT write your ID number on this page.

- **Duration:** 2 hours.
- **Total points:** 100.
- 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

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

1. Define the following terms:

   (a) [3 points] Cryptography

   (b) [3 points] Substitution cipher

   (c) [3 points] Monoalphabetic cipher

   (d) [3 points] Product cipher

   (e) [3 points] Nomenclator

2. (a) i. [3 points] Describe the term *confusion*.

ii. [2 points] How is confusion achieved in a cryptosystem?

(b) i. [3 points] Describe the term *diffusion*.

ii. [2 points] How is diffusion achieved in a cryptosystem?

3. (a) [5 points] Describe the *plaintext block chaining* (PBC) mode for block ciphers. Explain how to perform both encryption and decryption.

(b) [3 points] What is the error propagation behaviour of PBC mode? Explain.

4. (a) [3 points] Describe what is meant by a *linear* cryptosystem.

(b) [3 points] Which parts of DES lead one to believe that its algorithm is neither linear or affine?

(c) [2 points] Describe what is meant by Triple DES, i.e. explain how to perform both encryption and decryption using Triple DES (you need not describe any features of DES).

5. (a) [6 points] Encipher the message SURRENDER using the affine transformation

$$C \equiv 11P + 18 \pmod{26}$$
$$(C = \text{ Ciphertext, P = Plaintext}).$$

(a) [6 points] Decipher the following ciphertext, which was enciphered using a Vigenère cipher with key ART:

YFN GFM IKK JXA T.

6. Let $E = \begin{pmatrix} 5 & 17 \\ 4 & 15 \end{pmatrix}$ be the encryption matrix for a Hill cipher.

   (a) [7 points] Find the decryption matrix.

   (b) [7 points] Decrypt the ciphertext GZ SC XN UC.

7. (a) [8 points] What is the ϕ statistic? Explain the use of this statistic in resolving the number of alphabets used in a polyalphabetic substitution cipher.

(b) [5 points] Which of the following ciphertexts have been monoaphabetically enciphered?

i. AOLJH LZHYJ PWOLY PZLHZ PSFIY VRLUX

ii. EXLLH AJRSJ XFEKL OZHJS OLPWW

8. [5 points] Decrypt the ciphertext TONYP OSNTE RSISI AAIS using a columnar transposition with the key CRYPTO.

9. Define

   (a) [4 points]

      i. Entropy

      ii. Unicity distance

   (b) [6 points] Let X be one of the six messages: A, B, C, D, E, F, where:

$$p(A) = p(B) = p(C) = 1/4, p(D) = 1/8, p(E) = p(F) = 1/16.$$

   Compute $H(X)$ and find an optimal binary encoding of the messages.

10. [6 points] What are the strengths of DES?

Extra page for rough work

Extra page for rough work