Math 135 Prelim #1 – July 10, 2006

This exam has 15 problems and 5 numbered pages.

Name: _____ Instructor: Michael Kozdron

*You have **75** minutes to complete this exam. Show all work neatly and in order, and clearly indicate your final answers. Answers must be justified whenever possible in order to earn full credit.*

Unless otherwise specified, no credit will be given for unsupported answers, even if your final answer is correct. *Points will be deducted for incoherent, incorrect, and/or irrelevant statements. Calculators are permitted, but no other aids are allowed.*

You are allowed to use standard notation. However, any new notation or abbreviations that you introduce must be clearly defined.

*This examination consists of **15** problems and is worth **100** total points. You must answer all of the questions in the space provided.*

Good luck!

Page	Score
1	
2	
3	
4	
5	

TOTAL: _____

Part I: A Brief History of Cryptology

1. (*8 points*) Below are 4 cryptosystems. For each cryptosystem, identify whether the cipher it uses is a monoalphabetic substitution (MA), a polyalphabetic substitution (PA), or a transposition (T). Circle your choice.

Vigenère Square	MA	PA	T
Spartan Scytale	MA	PA	T
Alberti's Cipher Wheel	MA	PA	T
Atbash	MA	PA	T

2. (*8 points*) In the context of Math 135, explain the difference between the terms **symmetric cryptosystem** and **asymmetric cryptosystem**. Be sure to give an example of each.

3. (*8 points*) In the context of Math 135, explain the difference between the terms **cryptography**, **cryptanalysis**, and **cryptology**.

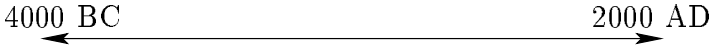
(continued)

4. (*2 points*) In 2006, the Sicilian Mafia boss Bernardo Provenzano was arrested by Italian police. As part of their investigation, police found hundreds of notes written by Provenzano containing encrypted names. Once the notes were decrypted, they were used by the prosecution to convict Provenzano. Which classical cryptosystem had Provenzano used?

Answer: _____

5. (*8 points*) On the following timeline, identify (approximately) the period when each of the following cryptosystems was introduced. Use the abbreviations J, P, A, V as indicated.

Jefferson's Wheel Cipher (J)	Polybius' Checkerboard (P)
Atbash (A)	Vernam's One-Time Tape (V)



6. (*4 points*) In a cryptological context, define what is meant by the term **steganography**. Give an example of a cryptosystem which uses steganography as (part of) its cipher.

7. (*4 points*) In a cryptological context, define what is meant by **nomenclator**.

8. (*2 points*) Give an example of a cryptosystem which uses both substitution and transposition in its cipher.

Answer: _____

(continued)

Part II: Modular Arithmetic

9. (*4 points*) Compute $3^{-1} \pmod 7$.

10. (*4 points*) Compute $8 \,\mathrm{DIV}\, 17$ and $-8 \,\mathrm{DIV}\, 17$.

11. (*6 points*) Determine the smallest non-negative value of x such that

$$(5x + 1) \equiv (2x + 3) \pmod 8.$$

12. (*6 points*) Determine *all* values of a and b such that

$$3a + b \equiv 5 \pmod 9, \text{ and}$$
$$5a + b \equiv 4 \pmod 9.$$

(continued)

Part III: Affine Ciphers

Recall that the numerical equivalents of the letters are as follows:

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

13. (*10 points*) Suppose that the affine cipher $E(x) = (9x + 1) \,\text{MOD}\, 26$ produced the ciphertext `F B W X Q Q M B W W`. Determine the plaintext.

14. (*6 points*) Carefully explain why $E(x) = (4x + 7) \,\text{MOD}\, 26$ does *not* define a valid affine cipher. Does $E(x) = (7x + 4) \,\text{MOD}\, 26$ define a valid affine cipher?

(continued)

Part IV: Cryptanalysis

15. (*20 points*) The following ciphertext was produced from plaintext by a columnar transposition. Determine the plaintext.

```
TROEH KMSEA ITWNS OODEG ODSOD ETBSE OEAPK FRBEO EUERL TPEOI AIVHN SEADL
LVMEY EIEDP LPAR
```

Bonus: From which poem is this quote an excerpt?

Answer:_____ *(The End.)*