# Mathematics 124 Midterm – March 19, 2009

**This exam has 12 problems on 6 numbered pages and is worth a total of 75 points**.

*You have 75 minutes to complete this exam. Please read all instructions carefully, and check your answers. 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.*

*This exam is closed-book. 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.*

*You must answer all of the questions in the space provided. Note that blank space is NOT an indication of a question's difficulty.*

*Good luck!*

Name: _____

Instructor: Michael Kozdron

| Page | Score |
|---|---|
| 1 | |
| 2 | |
| 3 | |
| 4 | |
| 5 | |
| 6 | |

TOTAL: _____

## Part I: A Brief History of Cryptology

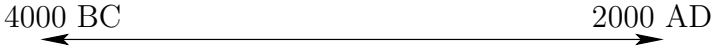
**1.** (*6 points*) Below are 3 cryptosystems. For each cryptosystem, identify whether the cipher it uses is a monoalphabetic substitution (MA), a polyalphabetic substitution (PA), or a transposition (T). Circle your choice.

| | | | |
|---|---|---|---|
| Caesar Cipher | MA | PA | T |
| Spartan Scytale | MA | PA | T |
| Jefferson's Cipher Wheel | MA | PA | T |

**2.** (*4 points*) In a cryptological context, define what is meant by a **one-time pad**.

**3.** (*8 points*) On the following timeline, identify (approximately) the period when each of the following cryptosystems was introduced. Use the abbreviations E, S, C, A as indicated.

| | |
|---|---|
| Enigma (E) | Spartan Scytale(S) |
| Alberti's Cipher Disk (C) | ADFGVX (A) |




**4.** (*2 points*) Which is the earliest known cryptographic system to implement a polyalphabetic substitution?

**Answer**: _____ *(continued)*

## Part II: Arithmetic

**5.** (*6 points*) Determine the smallest positive value of $x$ such that

$$(6x + 2) \equiv (2x + 3) \pmod{9}.$$

**6.** (*4 points*) Compute $13 \operatorname{DIV} 11$ and $-13 \operatorname{DIV} 11$.

**7.** (*4 points*) Convert the number with base twenty-six representation `BEET` to decimal (base ten). *See page 4 for a table of the numerical equivalents of the letters.*

**8.** (*6 points*) Let $a = 11010$ and $b = 1001$ be two binary numbers. Compute the binary numbers $a + b$ and $a - b$.

*(continued)*

## Part III: Enciphering and Deciphering

**9.** (*7 points*) Use the following ADFGVX grid to encipher the message `MATH IS FUN` if the keyword is `TAG`.

| | A | D | F | G | V | X |
|---|---|---|---|---|---|---|
| A | F | L | 1 | A | O | 2 |
| D | J | D | W | 3 | G | U |
| F | C | I | Y | B | 4 | P |
| G | R | 5 | Q | 8 | V | E |
| V | 6 | K | 7 | Z | M | X |
| X | S | N | H | 0 | T | 9 |

*Note that the letter* `O` *is in the first row, while the number* `0` *is in the last row.*

**Answer**: _____ *(continued)*

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 |

The following formulas may be helpful for this problem:

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}, \qquad \det(A) = ad - bc, \qquad A^{-1} = \det(A)^{-1} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.$$

**10.** (*7 points*) The ciphertext `OMNIVAJI` resulted from a Hill encipherment of the plaintext `THE RAVEN`. Based on this information, determine the key matrix $A$.

**Answer**: _____ *(continued)*

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 |

**11.** (*7 points*) Suppose that the affine cipher $E(x) = (7x + 2) \,\mathrm{MOD}\, 26$ produced the ciphertext `C B J C F R W Y Y`. Determine the plaintext.

**Answer**: _____ *(continued)*

## Part IV: Cryptanalysis

**12.** (*14 points*) The following ciphertext was produced from plaintext by a columnar transposition. Determine the plaintext.

```
TIATE ETDIW VWOLL HEFOE OOEEA AFRRO KSDTL EOGDT SBHLR AEAHT YATED DNERA
SHNSI DOANM ECDNI NVDAD E
```

**Bonus**: From which poem is this quote an excerpt?

**Answer**:_____ *(The End.)*