Make sure that this examination has 10 numbered pages

University of Regina
Department of Mathematics & Statistics
Final Examination
200910
(April 21, 2009)

Mathematics 124

The Art and Science of Secret Writing

Name: ______________________________ **Student Number:** ______________

Instructor: Michael Kozdron **Time:** 3 hours

Read all of the following information before starting the exam.

You have ***3*** *hours 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.*** *Some problems require written explanations in context. Only complete solutions written in the context specified by the problem will be awarded full points, and points will be deducted for incoherent, incorrect, and/or irrelevant statements.*

You may use standard notation; however, any new notations or abbreviations that you introduce must be clearly defined.

Calculators are permitted; however, you must still show all your work. Other than these exceptions, no other aids are allowed.

Note that blank space is not an indication of a question's difficulty. The order of the test questions is essentially random; they are not intentionally written easiest-to-hardest.

This test has ***10*** *numbered pages with* ***11*** *questions totalling* ***150*** *points. The number of points per question is indicated. For questions with multiple parts, all parts are equally weighted unless otherwise indicated.*

DO NOT WRITE BELOW THIS LINE

Page 1	____________	Page 2	____________	Page 3	____________
Page 4	____________	Page 5	____________	Page 6	____________
Page 7	____________	Page 8	____________	Page 9	____________
Page 10	____________				
				TOTAL	____________

1. (*8 points*) The following ciphertext was produced from plaintext by a columnar transposition. Determine the plaintext.

```
DTGIH OLEOI MDGOF ETONH RCETE RUION SFE
```

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:

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

2. (*12 points*) The ciphertext `FCUWPZ` is the result of a Hill encipherment using the key matrix

$$A = \begin{bmatrix} 11 & 18 \\ 12 & 17 \end{bmatrix}.$$

Determine the plaintext.

3. (*8 points*) Briefly describe how the German Enigma machine used during World War II worked. Be sure to mention all of its primary cryptographic components.

4. (*12 points*) Decide whether each of the following statements is either true or false. Circle your choice. No explanation is required.

T **F** **(a)** If the greatest common divisor of integers a and b is 1, then either a or b (or both) must be prime.

T **F** **(b)** In any sample of ordinary English text, the letter `E` will be the most frequent.

T **F** **(c)** A scytale is a device that implements a type of monoalphabetic substitution.

T **F** **(d)** If an efficient method for factoring very large numbers is found, then RSA would no longer be a secure means of encryption.

T **F** **(e)** In a substitution cipher, the letters in the plaintext message are rearranged to form the ciphertext.

T **F** **(f)** Public key cryptosystems tend to run more slowly on computers than secret-key systems.

5. (*14 points*) Recall that the ASCII equivalents (in decimal) of the letters are as follows:

A	B	C	D	E	F	G	H	I	J	K	L	M
65	66	67	68	69	70	71	72	73	74	75	76	77
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
78	79	80	81	82	83	84	85	86	87	88	89	90

(a) (*4 pts*) Convert the decimal (base ten) number 124 to binary (base 2).

(b) (*10 pts*) Use as a key the 7-bit binary representation of 124 that you found in **(a)** to decipher

0110000 0110011 0101111 0101000

which was enciphered by a binary Vigenère cipher and interpret the result as four ASCII values. What is the decoded four-letter message? (That is, convert each of the resulting 7-bit strings to a decimal number, and interpret that number as an ASCII equivalent.)

6. (*16 points*)

(a) (*10 pts*) Use the Euclidean algorithm to find $\gcd(131071, 2047)$.

(b) (*3 pts*) Does the inverse of 2047 modulo 131071, exist? If so, find it. If not, explain why it does not exist.

(c) (*3 pts*) From **(a)** we have one pair of integers s and t such that

$$131071s + 2047t = \gcd(131071, 2047).$$

However, we know that the answer is not unique. Find *another* pair of integers s and t such that $131071s + 2047t = \gcd(131071, 2047)$.

7. (*20 points*) For each of the following questions, use Fermat's Little Theorem or Euler's Theorem (or their corollaries) as appropriate.

(a) Compute 7^{18} MOD 17.

(b) Compute 6^{84} MOD 13.

(c) Compute 6^{87} MOD 13.

(d) Compute 5^{163} MOD 51.

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

8. (*12 points*) Suppose that the plaintext FAME becomes RIOK under an affine cipher

$$E(x) = (ax + b)\,\mathrm{MOD}\,26.$$

Determine a and b.

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

9. (*24 points*) In order to prepare to receive encrypted messages with the RSA cryptosystem, Alice has chosen primes $p = 31$ and $q = 1031$. She has also chosen $e = 2377$ as her public key (also called her public exponent).

(a) (*4 pts*) Determine Alice's public modulus m.

(b) (*12 pts*) Determine Alice's private key (or decryption key) d.

(c) (*8 pts*) Suppose that Bob has sent Alice the ciphertext $y = 103$. Determine the base twenty-six representation of the plaintext message.

10. (*12 points*) Recall that the Diffie-Hellman key agreement protocol works as follows.

- A public prime p and a public base s are published (where $0 \leq s \leq p-2$).
- Alice chooses a number a in the range 2 to $p-2$ and calculates $\alpha = s^a \operatorname{MOD} p$. She then sends α to Bob.
- Bob chooses a number b in the range 2 to $p-2$ and calculates $\beta = s^b \operatorname{MOD} p$. He then sends β to Alice.
- The key is then calculated as $k = s^{ab} \operatorname{MOD} p$.

Suppose that the public prime is $p = 5927$ and the public base is $s = 31$. Suppose further that Alice chooses $a = 143$ and Bob chooses $b = 83$. Determine the key k that they agree upon. *Hint: Use Fermat's Little Theorem to drastically reduce the exponent before starting the repeated squaring procedure.*

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. (*12 points*) Decrypt the following English sentence

`BPMUW ABKMZ BIQVE IGBWA CKKMM LQAIT EIGAB WBZGR CABWV MUWZM BQUM`

which was encrypted using a shift cipher. *Hint: The most frequent ciphertext letters are* `B` *and* `M`*, which appear eight and seven times, respectively.*

FOR YOUR WORK:

B	P	M	U	W	A	B	K	M	Z	B	I	Q	V	E	I	G	B	W	A	C	K	K	M	M	L	Q
A	I	T	E	I	G	A	B	W	B	Z	G	R	C	A	B	W	V	M	U	W	Z	M	B	Q	U	M

FOR YOUR WORK:

B	P	M	U	W	A	B	K	M	Z	B	I	Q	V	E	I	G	B	W	A	C	K	K	M	M	L	Q
A	I	T	E	I	G	A	B	W	B	Z	G	R	C	A	B	W	V	M	U	W	Z	M	B	Q	U	M