Make sure that this examination has 12 numbered pages

Cornell University
Final Examination
August 8, 2006

Mathematics 135
The Art of Secret Writing

Time: 2 hours

Name: _____

Instructor: Michael Kozdron **Section:** 01

Read all of the following information before starting the exam.

*You have **2** 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.*** *Points will be deducted for incoherent, incorrect, and/or irrelevant statements.*

Calculators are permitted, and a formula page will be provided. There are no other aids allowed.

*This test has **12** numbered pages with **9** questions totalling **120** points. Before you hand in your exam, make sure you have all of the pages.*

DO NOT WRITE BELOW THIS LINE

Page 1 _____	Page 5 _____	Page 9 _____
Page 2 _____	Page 6 _____	Page 10 _____
Page 3 _____	Page 7 _____	Page 11 _____
Page 4 _____	Page 8 _____	Page 12 _____

TOTAL _____

1. (*24 points*) In order to prepare to receive encrypted messages with the RSA cryptosystem, Alice has chosen primes $p = 23$ and $q = 37$. She has also chosen $e = 13$ as her public key (also called her public exponent).

(a) Determine Alice's public modulus m.

(b) Suppose that Bob wants to send Alice the message `BAT`. Determine the base twenty-six representation of the ciphertext that he will send to Alice.

(continued)

(c) Determine Alice's private key (or decryption key) d.

(continued)

(d) Suppose that Bob has also sent Alice the ciphertext $y = 625$. Determine the base twenty-six representation of the plaintext message.

2. (*18 points*) Please supply short answers to the following questions.

(a) If $a = 2^3 \cdot 23^4 \cdot 97^2$ and $b = 2^4 \cdot 13^2 \cdot 23 \cdot 97^4 \cdot 101$, what is $\gcd(a, b)$?

(b) Calculate $4^{2834} \,\text{MOD}\, 2833$. (Note that 2833 is prime.)

(c) The extended Euclidean algorithm was used with the numbers $a = 97$ and $b = 523$ to produce

$$23 \cdot 523 - 124 \cdot 97 = 1.$$

Use this fact to determine $97^{-1} \,\text{MOD}\, 523$.

(d) The security of RSA rests on the apparent time-consuming nature of what mathematical problem?

(continued)

(e) Suppose that the Friedman indices of coincidence for two 10000-letter Vigenère ciphertexts are 0.05 and 0.041, respectively. Which of these is likely to correspond to a longer keyword? Explain.

(f) Hexadecimal is the name given to the base sixteen number system with digits

$$0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F.$$

Find the base twenty-six representation of the hexadecimal number FB.

3. (*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 $\alpha = s^a \,\text{MOD}\, p$. She then sends α to Bob.
- Bob chooses a number b in the range 2 to $p-2$ and calculates $\beta = s^b \,\text{MOD}\, p$. He then sends β to Alice.
- The key is then calculated as $k = s^{ab} \,\text{MOD}\, p$.

(a) Suppose that the public prime is $p = 6679$ and the public base is $s = 29$. Suppose further that Alice chooses $a = 167$ and Bob chooses $b = 80$. Determine the key k that they agree upon. *Hint*: Use (the corollary to) Fermat's Little Theorem to drastically reduce the exponent before starting the repeated squaring procedure.

(b) Find the binary representation of the key k that you calculated in **(a)**.

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 a and b are distinct primes, then a and b are relatively prime.

T F **(b)** William Friedman and Francis Bacon were co-workers during World War II in breaking the Enigma cipher.

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

T F **(d)** If an efficient method for calculating modular exponentials were found, then RSA would no longer be a secure means of encryption.

T F **(e)** A principle of modern cryptography is that the security of a cipher system rests on keeping the method of encipherment secure.

T F **(f)** Fermat's Little Theorem was discovered in 1970 while researchers were looking for an asymmetric cryptosystem.

T F **(g)** The probability of randomly selecting the letter `E` from a sample of English text is approximately $\frac{1}{26}$.

T F **(h)** The World War II Enigma cryptosystem relied on both transposition and substitution for its cipher.

5. (*8 points*) Decipher `SFCXZY NSJFUW SMKEYY` which was enciphered using the Vigenère method with keyword `SURE`.

6. (*12 points*) Suppose that the plaintext `CRYPTO` becomes `AVKNDW` under an affine cipher

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

Determine a and b.

7. (*8 points*) Answer any **two** of the following four questions. Be sure to clearly indicate which two you would like to have graded.

(a) Briefly describe the role of a Trusted Authority (TA) in modern asymmetric cryptosystems.

(b) Briefly describe what is meant by 128-bit encryption.

(c) Briefly describe the function of a Secure Socket Layers (SSL) Certificate.

(d) Carefully describe the difference between encryption and authentication with regards to modern asymmetric cryptography.

8. (*12 points*) Suppose that the six letters `A`, `B`, `C`, `D`, `E`, `F` are written on six index cards (with each letter appearing on one and only one index card).

(a) How many possible ways are there to select a pair of distinct letters? (For example, the pairs `AB` and `BA` are considered to be the same pair.)

(b) How many possible ways are there to select two distinct pairs of distinct letters? (For example, `AB`–`ED` and `DE`–`BA` are considered the same.)

9. (*14 points*) Let $A = \begin{bmatrix} 4 & 3 \\ 5 & 10 \end{bmatrix}$ be the key matrix for the Hill cipher.

(a) Calculate the inverse of A modulo 26.

(b) If A was used to produce the ciphertext `OO`, decipher the message.

(The End.)