8038 Semester 2 2005

The University of Sydney

FACULTY OF SCIENCE

MATH2068

Number Theory and Cryptography

SAMPLE EXAM ONLY

Time allowed: two hours

Lecturer: R. B. Howlett

No notes or books are to be taken into the examination room.

Calculators will be provided. No other calculators are allowed.

1. In this question, assume that all plaintext messages consist of English text, written in upper case letters, with punctuation and spaces removed.

(*i*) Encipher the plaintext CRYPTOGRAPHY using a Vigenère cipher with enciphering key CAB.

(*ii*) Describe Friedman's attack on Vigenère ciphers. In answering this, you should

(a) describe the statistics one should calculate;

(b) state typical approximate values for these statistics in the various cases that may arise;

(c) explain how to use this data to find the key.

(*iii*) An *affine cipher* is a substitution cipher defined by a rule of the form

$$i \mapsto mi + n \pmod{26},$$

for some fixed integers m, n, where the letters A to Z are identified with residues modulo 26 in the usual way (A $\leftrightarrow$ 0, B $\leftrightarrow$ 1, etc.). The pair (m, n) is called the *key*.

(a) What condition must the integer m satisfy to ensure that no two distinct plaintexts yield the same ciphertext?

(b) A sample of ciphertext known to have been produced by an affine cipher is found to consist of 1000 letters altogether, of which the two most common are G (137 occurrences) and Z (101 occurrences). Assuming that these represent the most common letters in English, determine the key.

. . . /2

2. (*i*) Solve the following system of simultaneous congruences:

$$\begin{aligned} x &\equiv 3 \pmod 7 \\ x &\equiv 2 \pmod 9 \\ x &\equiv 5 \pmod{11}. \end{aligned}$$

(*ii*) Suppose that $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, where the p_i are distinct primes and the k_i are positive integers. Write down the formulas for $\tau(n)$ (the number of divisors of n) and $\sigma(n)$ (the sum of the divisors of n).

(*iii*) Suppose that x_n is defined whenever n is a divisor of 1000, and suppose that the equation $\sum_{d|n} x_d = n^2$ is satisfied for all $n|1000$. Use Möbius inversion to find x_{1000}.

(*iv*) Let p be an odd prime. A number $t \in \{1, 2, \ldots, p-1\}$ is called a *quadratic residue* mod p if the congruence $x^2 \equiv t \pmod p$ has a solution, and is called a *quadratic nonresidue* mod p if $x^2 \equiv t \pmod p$ has no solution.

(a) Show that if $a^2 \equiv b^2 \pmod p$ then $a \equiv \pm b \pmod p$.

(b) Show that the equation $x^2 \equiv t \pmod p$ has exactly two solutions in $\{1, 2, \ldots, p-1\}$ if t is a quadratic residue, and no solutions otherwise.

(c) Show that exactly half the numbers in $\{1, 2, \ldots, p-1\}$ are quadratic residues mod p.

3. (*i*) Let k, a, b be positive integers. Show that $\gcd(ka, kb) = k \gcd(a, b)$.

(*ii*) Xavier uses an RSA cyptosystem with public key $(4425247, 13)$, but his rival Yvonne finds the number 4417416 scribbled on a piece of paper on Xavier's desk. Correctly guessing that this number is $\phi(4425247)$, and that 4425247 is the product of two distinct primes, Yvonne is able to factorize 4425247.

(a) Describe the process that Yvonne uses to do this, and

(b) find the factors.

(*iii*) If Yvonne in Part (*ii*) wished to decrypt Xavier's incoming messages she would not need to know the factors of 4425247, but would merely need to determine Xavier's private key.

(a) Describe how she can do this, and

(b) do the calculation, and find the private key.

4. (*i*) Joe uses the Elgamal cipher system, the encryption (public) key being $(17, 5, 8)$. Plaintext messages must be sequences of residues modulo 17.

(a) What is Joe's decryption (private) key?

(b) Joe receives the enciphered message $\langle 6, [16, 3, 12]\rangle$. What is the plaintext?

(*ii*) In the cipher system used by a secret society, messages are even length sequences of residues mod 27, which for encryption purposes are split into blocks of length 2. The encryption process replaces the block (a, b) by the block (a', b') defined by

$$\begin{pmatrix} a' \\ b' \end{pmatrix} = \begin{pmatrix} 1 & 3 \\ 2 & 7 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \end{pmatrix}.$$

(a) Encrypt the plaintext $(13, 7, 0, 1, 5, 0)$.

(b) Describe how to recover the plaintext from the ciphertext.

5. Let k be a positive integer and let $m = 4k + 3$.

(*i*) Show that the even numbers $2k + 2$, $2k + 4$, ..., $4k$, $4k + 2$ are congruent modulo m to the negatives of the odd numbers $2k + 1$, $2k - 1$, ..., 3, 1, and deduce that

$$2^{k+1}(k+1)(k+2)\cdots(2k+1) \equiv (-1)^{k+1}(2k+1)(2k-1)\cdots 3\cdot 1 \pmod{m}.$$

(*ii*) Use Part (*i*) and the fact that $2^k(k!)$ is the product of the even numbers from 2 to $2k$ to deduce that $2^{2k+1}(2k+1)! \equiv (-1)^{k+1}(2k+1)! \pmod{m}$.

(*iii*) Assume now that m is prime. Use Part (*ii*) to show that if k is odd then $2^{\frac{1}{2}(m-1)} = 2^{2k+1} \equiv 1 \pmod{m}$

(*iv*) Suppose that k is odd and that m and $p = 2k + 1 = \frac{1}{2}(m - 1)$ are both prime. Use Part (*iii*) to show that the Mersenne number M_p is divisible by m.