8038 Semester 2 2006

The University of Sydney

FACULTY OF SCIENCE

MATH2068

Number Theory and Cryptography

November, 2006

Lecturer: R. B. Howlett

Time allowed: two hours

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

Calculators will be provided; no other calculators are allowed.

The paper has five questions. The questions are of equal value.

. . . /2

1. (1) Associating the letters A to Z with the numbers 0 to 25 as usual, use a Vigenère cipher with keyword CAT to encrypt the plaintext LEOPARD.

(2) Let $M = c_1c_2c_3\ldots c_\ell$ be a sequence of of letters from the alphabet $\{\mathrm{A}, \mathrm{B}, \ldots, \mathrm{Z}\}$.

(a) What is the definition of the *coincidence index* of M?

(b) If M is typical English text (stripped of spacing and punctuation) approximately what will the value of the coincidence index be?

(c) If M is a totally random sequence of letters approximately what will the value of the coincidence index be?

(d) What is meant by the *decimation of M with period m and index r*?

(3) An intercepted message M is reliably known to have been encrypted with a Vigenère cipher. Describe (in a few sentences) a strategy for decrypting M using decimations and coincidence index.

2. (1) Use the extended Euclidean algorithm to find the inverse of 943 modulo 29311. (Working must be shown.)

(2) Use the Lagrange Interpolation Formula to find a, b, c in $\{0, 1, \ldots, 18\}$ such that the polynomial $f(x) = ax^2+bx+c$ satisfies $f(3) \equiv 11 \pmod{19}$, $f(7) \equiv 2 \pmod{19}$ and $f(16) \equiv 9 \pmod{19}$.

(3) Show that $\mathrm{ord}_{23}(2) = 11$. Are there any other primes p such that $\mathrm{ord}_p(2) = 11$?

(4) Let $n = (d_\ell d_{\ell-1}\ldots d_0)_8$; that is, when the integer n is expressed in base 8 notation its digits are d_ℓ, $d_{\ell-1}$, $\ldots$, d_0.

(a) Explain what this means, using the case $n = (1253)_8$ to illustrate your answer.

(b) Prove that $n \equiv d_0 + d_1 + \cdots + d_\ell \pmod{7}$.

3. (1) Find an integer x satisfying the following three conditions:

$$\begin{aligned} x &\equiv 17 \pmod{29}, \\ x &\equiv 11 \pmod{30}, \\ x &\equiv 6 \pmod{31}. \end{aligned}$$

(2) Let a, b and k be positive integers. Prove that $\gcd(ka, kb) = k \gcd(a, b)$.

(3) The aim is to factorize 12319 via the Pollard Rho method.

(a) Define $t_0 = 1$ and $t_{i+1} \equiv t_i^2 + 1 \pmod{12319}$ for all $i \geq 0$. Make a table of the values of t_i for $0 \leq i \leq 6$, and hence find $t_{2i} - t_i$ for $i = 1$, 2 and 3.

(b) Calculate an appropriate gcd and hence factorize 12319.

(4) RSA user Joe has $(55, 3)$ as his public key.

(a) What is Joe's private key?

(b) Encipher the message $[8, 20, 7]$ using Joe's public key.

4. (1) Show that 2 is a primitive root modulo 19, and calculate value of $\log_{2,19}(a)$ for all nonzero residues a modulo 19.

(2) Suppose that you are user of the Elgamal cryptosystem and that your public key is $(p, b, k) = (47, 5, 14)$ and your private key is $m = 4$.

(a) Check that the necessary relationship between the private key and the public key is indeed satisfied. (It is given that 5 is a primitive root modulo 47; you need not check this.)

(b) You receive the message $\langle 23, [6, 36, 4] \rangle$. Decrypt it.

(3) Let n be an even perfect number, and write $n = 2^k m$ where m is odd.

(a) Prove that $2^{k+1}m = (2^{k+1}-1)\sigma(m)$, where σ is the "sum of divisors" function, and deduce that $m = (2^{k+1} - 1)r$ for some integer r.

(b) Show that $\sigma(m) = r + m$, and deduce that $r = 1$.

(c) Show that m must be prime.

5. (1) Let p be a prime that is congruent to 5 modulo 6, and write $p = 6k + 5$. We split the set $S = \{1, 2, \ldots, \frac{1}{2}(p-1)\}$ into three subsets, as follows:

$$S_1 = \{1, 2, \ldots, k\},$$
$$S_2 = \{k+1, k+2, \ldots, 2k+1\},$$
$$S_3 = \{2k+2, 2k+3, \ldots, 3k+2\}.$$

(a) Observe that if $i \in S_1$ then $3i \in S$. Show that

(i) if $i \in S_2$ then $3i$ is congruent mod p to the negative of an element of S;

(ii) if $i \in S_3$ then $3i$ is congruent mod p to an element of S.

(b) Let $M = \prod_{i=1}^{3k+2} 3i$, the product of all the numbers $3i$ as i runs through S. Use Part (a) to show that $M \equiv (-1)^{k+1}(3k+2)! \pmod{p}$.

(c) Use Part (b) to show that $3^{3k+2} \equiv (-1)^{k+1} \pmod{p}$.

(d) Use Part (c) to show that 3 is a square (mod p) if and only if k is odd.

(2) Devise a similar argument dealing with primes p of the form $6k + 1$, showing that in this case 3 is a square mod p if and only if k is even.