The University of Sydney

FACULTY OF SCIENCE

MATH2068

Number Theory and Cryptography

November, 2005 Time allowed: two hours

Lecturer: R. B. Howlett

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

1. (*i*) Decrypt the ciphertext PDWKHPDWLFV, given that Julius Caesar's cipher was used.

(*ii*) Two long samples of ciphertext are intercepted, and found to consist of strings of upper case letters, with no spaces or punctuation. The first is found to have a coincidence index of 0.0649 and digraph coincidence index of 0.00723, whereas the second has a coincidence index of 0.0653 and a digraph coincidence index of 0.00452. Independent information suggests that in both cases the plaintext is English (stripped of spaces and punctuation), and that one was encrypted with a substitution cipher and the other with a transposition cipher.

Which is most likely to be the transposition cipher, and which the substitution cipher? In justifying your answer you should explain

(a) how the coincidence index and digraph coincidence index are calculated;

(b) what values for these quantities one would expect to obtain from a random, meaningless, sequence of letters;

(c) why typical unencrypted English yields values different from those in (b);

(d) how substitution and transposition ciphers affect these quantities.

(*iii*) A long piece of ciphertext is to be statistically analysed, in the belief that a block transposition cipher was used. Let M' denote the ciphertext.

(a) What is meant by $\mathrm{Dec}([k,\ell],m)$, the (k,ℓ)-decimation of period m, of the ciphertext M'?

(b) How is the *coincidence discriminant* of $\mathrm{Dec}([k,\ell],m)$ calculated?

(c) If it turns out that the coincidence discriminant of $\mathrm{Dec}([2,5],7)$ is 0.00496 and that of $\mathrm{Dec}([1,4],7)$ is 0.00110, what conclusion(s) would you draw?

... /2

2. (*i*) Use the extended Euclidean Algorithm to find the inverse of 17 modulo 97. (Working must be shown.)

(*ii*) Find a perfect number greater than 5000. Use properties of the "sum of divisors" function proved in lectures to show that your answer is correct.

(*iii*) Let n be a prime and M_n the corresponding Mersenne number.

(a) What is the formula for M_n?

(b) Let p be a prime divisor of M_n. What is the value of $\mathrm{ord}_p(2)$? (Full justification for your answer is required.)

(c) In general, what does Fermat's Little Theorem tell us about the value of $\mathrm{ord}_p(2)$, given that p is prime?

(d) Using (b) and (c) as a guide, and using your calculator, find a prime divisor p of M_{29} such that $1000 < p < 1300$.

3. (*i*) Use Fermat's factorization method to factorize 3139.

(*ii*) Show that if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then $a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$.

(*iii*) Let n be a positive integer, let $a_0 = 1$, and suppose that for every positive integer i the number a_i is the residue modulo n of $a_{i-1}^2 + 1$. Suppose that p is a prime divisor of n.

(a) Show that there exist integers i and j such that $0 \leq i < j \leq p$ such that $a_i \equiv a_j \pmod{p}$.

(b) Using Part (*ii*) above, show that if $a_i \equiv a_j \pmod{p}$ then $a_{i+k} \equiv a_{j+k} \pmod{p}$ for all positive integers k.

(c) Let i and j be as in (a), and suppose that k is a multiple of $j - i$ with $i \leq k < j$. Show that $a_{2k} \equiv a_k \pmod{p}$.

4. (*i*) Show that 3 is a primitive root modulo 17, and draw up a table giving the values of $\log_3(a[17])$ for all nonzero residues a modulo 17.

(*ii*) How many digits are there in the decimal representation of a 1000 bit integer?

(*iii*) Joe uses the RSA cryptosystem, his public key being $(1600453, 257)$. Given that 1103 is a factor of 1600453, use your calculator to verify that his private key is $(1600453, 317093)$. (You must write down the steps you use and the results of any intermediate calculations.)

(*iv*) Two people communicating across an insecure channel wish to agree on three 56 bit keys for future communication using triple DES. Describe how they can do this using the Diffie Hellman procedure. Your answer should include a brief explanation of why the procedure is believed to be secure.

5. Let F_n denote the n-th Fibonacci number. (Thus $F_0 = 0$, $F_1 = 1$, and $F_{i+1} = F_{i-1} + F_i$ for all $i \geq 1$.)

(*i*) Let $\theta_1 = 1+\sqrt{5}$ and $\theta_2 = 1-\sqrt{5}$, the roots of the polynomial $x^2 - 2x - 4$. Use induction on n to show that

$$2^n F_n = \tfrac{1}{\sqrt{5}}(\theta_1^n - \theta_2^n)$$

for all natural numbers n.

(*ii*) Use Part (*i*) and the Binomial Theorem to show that, for all positive integers n,

$$2^{n-1}F_n = \binom{n}{1} + \binom{n}{3}5 + \binom{n}{5}5^2 + \cdots$$

where the last term on the right hand side is either $\binom{n}{n-1}5^{\frac{1}{2}n-1}$ (if n is even) or $\binom{n}{n}5^{\frac{1}{2}(n-1)}$ (if n is odd). [The Binomial Theorem states that $(1+x)^n = \sum_{k=0}^{n}\binom{n}{k}x^k$, where the binomial coefficients $\binom{n}{k}$ satisfy $\binom{n}{k} = \frac{n(n-1)(n-2)\cdots(n-k+1)}{k(k-1)(k-2)\cdots 1}$.]

(*iii*) Let p, k be integers such that p is prime and $0 < k < p$. Show that $p|\binom{p}{k}$.

(*iv*) Show that if p is an odd prime not equal to 5 then $F_p \equiv 5^{\frac{1}{2}(p-1)} \pmod{p}$.