Queen Mary
University of London

MTH6115 Cryptography

Assignment 5 For handing in on 14th March 2011

Your solutions to Questions 3 and 4 should be handed in to the ORANGE box on the GROUND floor by 3:30 pm on Monday 14th March 2011.

Remember: *The work you hand in should be your OWN work. If you work in groups make sure you YOURSELF understand the answers that have been obtained, and write up your answers YOURSELF. I take a dim view of copied answers, and will penalise them severely when I detect them. You should also endeavour to do ALL the questions, not just those you hand in for assessment. The point of these sheets is to allow you to understand enough material to gain many marks on the exam, not merely to contribute approximately 1% towards your overall grade for the course.*

As usual, you should explain what you are doing (the explanation can be brief at times, but should still be a full explanation). Also, you will gain no marks merely for factoring the numbers below by trial division, or by getting a computer to factor them for you.

1 Prove by direct computation that $\lambda(256) = 64$, where λ is Carmichael's function. (The amount of computation is comparitively minor, if done properly. It may be helpful to inspect the multiplicative (sub-)group $\langle 5 \rangle$.)

2 I claim that $6038068681 \times 9673941253 = 58411921701573197293$, and that the two factors are prime. About how many arithmetic operations are required:

(a) To check that my multiplication is correct;

(b) To check that the factors are prime;

(c) To find the factorisation in the first place?

(You may take an arithmetic operation to be a single addition, subtraction, multiplication or division of integers, however large these integers may be.)

3 Let $N = 7571$. You are informed that N is the product of two primes and that $\phi(N) = 7392$. Use this information to factorise N.

4 In this question, we shall consider tests for proving that a Mersenne number $M_n := 2^n - 1$ is prime for various integers n. To this end we define the sequence u_m for $m \geqslant 0$ by $u_0 = 4$ and $u_{m+1} = u_m^2 - 2$ for $m \geqslant 0$.

(a) Prove for $n \geqslant 1$ that $M_n = 2^n - 1$ prime implies that n is prime.

(b) Show that the converse of the above does not hold.

(c) Approximately how many arithmetical operations are required to show that the numbers M_{31} and M_{61} are prime by trial division?

(d) Let p be an odd prime. Euler observed that if q is prime factor of M_p then we have both $q \equiv 1 \pmod{p}$ [a consequence of Fermat's Little Theorem and $2^1 - 1 = 1$] and $q \equiv \pm 1 \pmod{8}$ [a consequence of the theory surrounding the fact that 2 is a square modulo M_p: we have $(2^{(p+1)/2})^2 = 2^{p+1} \equiv 2 \pmod{M_p}$]. What are the allowed equivalence classes of prime factors of M_p modulo 248 and 488 respectively in the cases when $p = 31$ or 61?

(e) Euler proved the primality of $2^{31} - 1$ by restricting his attention to potential factors satisying the restrictions of the previous part of this question. Approximately how many divisions did Euler require to verify that $2^{31} - 1$ is prime.

(f) Prove that $u_m = (2 + \sqrt{3})^{2^m} + (2 - \sqrt{3})^{2^m}$ for all $m \geqslant 0$.

(g) The Lucas–Lehmer Test states that for p an odd prime, the Mersenne number M_p is prime if and only if $u_{p-2} \equiv 0 \pmod{M_p}$. How many decimal digits are there in u_{29}, and approximately how many decimal digits does u_{59} have? [Hint: $(2 - \sqrt{3})^{2^m}$ is rather small.]

(h) In practice, when establishing the primality of M_p via the Lucas–Lehmer Test, for each m, we calculate u_{m+1} as $u_m^2 - 2$ and immediately reduce the result modulo M_p. Why is this modular reduction important? [Note that the Lucas–Lehmer Test apparently only takes about $O(p)$ arithmetical operations to perform.]

5 Let N be a Carmichael number. Prove:

(a) $N \neq pq$ where $p < q$ are primes;

(b) For all primes p we have $p^2 \nmid N$;

(c) N must be odd.

Results from lectures, such as the formula for $\lambda(n)$ may be used without proof. Find all Carmichael numbers of the form $N = 3pq$, where $3 < p < q$ are primes.

6 Find all Carmichael numbers with just 3 prime divisors whose smallest prime divisor is $5, 7, 11, \ldots$ etc. Use this information to classify all Carmichael numbers up to some reasonable bound, say 10000. (The smallest Carmichael number with more than 3 prime divisors is $41041 = 7 \cdot 11 \cdot 13 \cdot 41$.)

7 Calculate $\lambda(n)$ for $120 \leqslant n \leqslant 130$ and $n = 1000000$.