Queen Mary
University of London

MTH6115 Cryptography

Assignment 6 For handing in on 21st March 2011

Your solutions to Questions 4 and 5 should be handed in to the ORANGE box on the GROUND floor by 3:30 pm on Monday 21st 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. For some of these questions, it is advisable to use some computer help with annoying arithmetical operations, but you should try a more 'hands on' approach to such things as calculating x^e, to make sure you understand how to compute this efficiently. You might even like to write your own procedures for calculating x^e, gcd's and so on.

1 Suppose my RSA public key is $(N, e) = (137017, 521)$. Encrypt the message $x = 46980$ for sending to me. Given that my private key has $d = 341$, factorise N.

2 Suppose my RSA public key is $(N, e) = (1234264849, 177893497)$. Encrypt the message $x = 1185565729$ for sending to me. Given that my private key has $d = 291005873$, factorise N.

3 Pick two primes p, q such that $1000 < p < q < 10000$, and let $N = pq$. Calculate $\phi(N)$ and $\lambda(N)$. You should calculate the latter without factorising $p - 1$ and/or $q - 1$. Pick e in the range $37 < e < \lambda(N) - 37$ suitable for use as part of an RSA public key (N, e), and determine the value of d in the corresponding private part of the key. (You should let $0 < d < \lambda(N)$.) Check your working by encrypting each

of the messages $x = 2$, 37, 73, 137 and 191 with your public key, and decrypting the result y (which should be $x^e \pmod N$) using your private key (you should get $x \equiv y^d \pmod N$).

4 Bob's RSA public key is $(N, e) = (713057, 1009)$, where $N = pq$ with $2 < p < q$ primes. Rummaging through Bob's wastepaper basket, Eve finds a scrap of paper on which is written '$\lambda(N) = 88920$,' which is suspected to refer to the aforementioned value of N. Use this information to factor N. [You should also determine the d-part of Bob's private key, but do not hand that part in.]

5 Barry used to use the RSA public key $(N, e) = (7519, 593)$ until Edna discovered the information that $d = 161$ from Barry's private key. Not understanding the nature of the security breach, Barry used an RSA public key with the same value of N and simply changed e. His new key is $(N, e') = (7519, 83)$. Help Edna determine the number d' Barry now uses for decrypting messages. The value of d' should lie in the range $0 < d' < \lambda(N)$. [You will gain no marks if you factor N by trial division, or get a computer to factor it for you.]

6 Basil's RSA public key is $(N, e) = (413714964683, 34819137169)$. Unfortunately, his choice of e was somewhat poor. Exploit this weakness to factorise N.

7 Becky does not have a very good primality prover. Her RSA modulus is $N = p_1 p_2$, where p_1 is a good quality prime someone gave her, and $p_2 = 2^a 3^b 5^c 7^d 11^e + 1$ for some integers $a, b, c, d, e \geqslant 0$.

$$N = 553585308479492029263469648722136035854071937040295473036382975367.$$

Use Pollard's $p - 1$ algorithm to factorise N. You do not need to prove that p_1 and p_2 are prime, and you may assume that $10^{30} < p_1, p_2 < 10^{40}$. [The Pollard $p - 1$ algorithm is described in Old Notes 8, but will not necessarily get lectured this year.]

8 Use the Miller–Rabin primality test to determine whether each of these numbers is definitely composite, or probably prime. You should use several iterations of the test if 'probably prime' is returned.

(a) 85028617,

(b) 50812579,

(c) 92697643,

(d) 12125213,

(e) 62756641.