Queen Mary
University of London

# MTH6115 Cryptography

## Assignment 7 For handing in on 28th March 2011

Your solutions to Questions 2 (b), 3 and 5 should be handed in to the ORANGE box on the GROUND floor by 3:30 pm on Monday 28th 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).*

**1** Prove that 2 is a primitive root (element) modulo 131 (which is prime). Find numbers $a$ with $0 \leqslant a \leqslant 129$ such that $2^a \equiv 101, 27, 44, 84 \pmod{131}$. Is there any quick way to do this?

**2** (a) Prove that 2 is a primitive root (element) modulo 107 (which is prime).
(b) Find a number $a$ with $0 \leqslant a \leqslant 105$ such that $2^a \equiv 85 \pmod{107}$. Is there any quick way to do this?
(c) Find a number $a$ with $0 \leqslant a \leqslant 105$ such that $2^a \equiv 14 \pmod{107}$.

**3** Prove that 2 is a primitive root (element) modulo 163 (which is prime). Throughout the following, the symbols $\log_a(b)$ denote discrete logarithms, where $a$ and $b$ are both integers modulo 163. Someone has told you that $\log_2(2) = 1$ [do you really need to be told this?], $\log_2(3) = 101$, $\log_2(5) = 15$ and $\log_2(7) = 73$, where $\log_2(a)$ is only well-defined modulo 162. (We also have $\log_2(-1) = 81$.) Calculate $\log_2(a)$ for $a \in \{20, 90, 11, 161, 26, 67\}$. [Hint: It will be helpful to note that $\log_2(a) = \log_2(a + 163m)$ for all integers $m$, and sometimes to use integers $m$ other than 0.]

**4** Bob uses the Miller–Rabin Primality Test to generate two large numbers $p_B, q_B$ which are likely to be prime. He then uses them to construct his public and secret keys for the RSA cipher system. How would it affect the implementation of the cipher system if $p_B$ turned out not to be prime?

**5** Let $G$ be a abelian group, and let $p \neq q$ be primes. Suppose that $g, h \in G$ are such that $g$ has order $p^a q^b$ and $h$ has order $p^c q^d$ where $a > c$ and $b < d$. Prove that $gh$ has order exactly $p^a q^d$. Compute the [multiplicative] orders of 2 and 3 modulo 251. Hence find a primitive root modulo 251.

**6** Compute the orders of 2 and 3 modulo 5153. Find a primitive root modulo 5153. Can you guarantee that this element is primitive without directly computing its order from scratch?

**7** In this question we analyse the algorithm for finding $p$ and $q$, provided we know the RSA data $N = pq$, $e$ and $d$ (where $2 < p < q$ primes and $de \equiv 1 \pmod{\lambda(N)}$). For each triple $(N, d, e)$ below calculate the proportion of $x$ with $1 \leqslant x \leqslant N - 1$ and $\gcd(N, x) = 1$ such that the method of factorising $N$ described in Lectures (or on-line Notes) succeeds for that value of $x$. [You will find the Chinese Remainder Theorem useful.]

(i) $(N, d, e) = (10033, 697, 1591)$, where $N = 79 \cdot 127$.

(ii) $(N, d, e) = (11413, 719, 479)$, where $N = 101 \cdot 113$.

What happens if I change $d$ and $e$? Justify your answers. Can you generalise your observations to other triples $(N, d, e)$?
[Merely searching through all possible values of $x$ is unnecessary, and unhelpful to understanding the underlying mathematics—I could have asked these questions for much larger values of $N$.]

**8** For each of the Carmichael numbers $N$ given below, calculate the proportion of $x$ with $1 \leqslant x \leqslant N-1$ and $\gcd(N, x) = 1$ such that the Miller–Rabin Primality Test returns 'possibly prime.'

(i) $561 = 3 \cdot 11 \cdot 17$.

(ii) $1105 = 5 \cdot 13 \cdot 17$.

(iii) $1729 = 7 \cdot 13 \cdot 19$.

(iv) $8911 = 7 \cdot 19 \cdot 67$.

Do the same for the following non-Carmichael numbers, indicating also the proportion of $x$ for which the Fermat Primality Test returns 'possibly prime.'

(v) $2479 = 37 \cdot 67$.

(vi) $3589 = 37 \cdot 97$.

(vii) $3599 = 59 \cdot 61$.

[Merely searching through all possible values of $x$ is unnecessary, and unhelpful to understanding the underlying mathematics—I could have asked these questions for much larger values of $N$.]