Moderation Sheet/Marking Scheme Assignment Block 2

(Moderators, please use black font colour!)

Candidate Name: Olivia Edbom

Moderator Name: Viktor Rosvall

Moderator's points awarded (max 120) and suggested grade: 53 pts, E

Question 2 (48 points)

Things to look out for:

- (a) Has the candidate clearly explained key generation, encryption and decryption? (max 15 pts)
- (b)(i) Has the candidate clearly shown the working and used FastExp? (max 8 pts)
- (b) (ii) Has the candidate used Lambda or Phi in this calculation?
- (b)(ii) if lambda was used, give up to 6 pts.
- (b)(ii) If Phi was used, what was the argument for not using Lambda? (max 4 pts)
- (b)(iii) Has the candidate clearly shown the working and used FastExp? (max 8 pts)
- (c) Points here are given to reflect the depth of the candidate's insight. Have they mentioned all that must be kept secret and why it must be kept secret? Have they mentioned what the size of the primes should be? Have they mentioned how to protect against a Pollard attack?
- (max 10 pts)
- How was the answer and explanations of Q2 presented? (max 1 pt)

Moderator comments:

Key generation, encryption and decryption has been explained in detail (15), and lambda has been used (6). I can't tell if FastExp was used or not, but correct answer was given (3). Candidate mentioned what must be kept secret and what is published, but not why it must be kept secret, and no mention of prime sizes and Pollard was mentioned (5). The answer was presented well (1).

30 pts

Question 3ab (18 points)

Things to look out for:

- (a) Has the candidate clearly explained the concept of **order** of an element modulo p, including the crucial statement about minimality? (max 5 pts)
- (a) Has the candidate corectly defined a primitive element as an element of order p-1? (max 2 pts)
- (b) Has the candidate clearly explained their strategy as to how to look for primitive elements, showed all their working? (max 8 pts)
- (b) Are the computations **efficient** or has the candidate chosen an inefficient strategy of simply computing all powers? (max 3 pts)

Moderator comments:

The statement about minimality was mentioned and the order was defined as p-1 (7). The candidate's strategy for finding primitive elements is unclear (5 pt).

The candidate has made an efficient calculation (3)

15 pts

Question 4cd (30 points)

Things to look out for:

- (c) This proof is given in various places in the notes and book. Is the proof written in the candidate's own words? (no points for copying a proof from book/notes, up to 8 pts for a personal presentation)
- (c) The first crucial steps in the proof are to argue why the Phi(n) elements ax_i are all different where the x_i denote all the invertible elements of **Z**_n. Is a thorough argument given for this? (max 10 pts)
- (c) The second crucial step in the proof is to argue why the product of the Phi(n) elements x_i is invertible, where the x_i denote all the invertible elements of **Z**_n. Is a thorough argument given for this? (max 4 pts)
- (d) The points here depend upon the dept of understanding shown by the candidate. Do they explain what a primality test is? Do they explain about bases? Do they explain about Carmichael numbers? (max 8 pts)

Moderator comments:

The proof is mostly copied from Pia's notes except some flavour text (2). The candidate mentions that ax_i is unique but not why (2). No argument was made as to why the product of x_i are invertible (1).

The candidate hasn't explained primality tests and other points (0).

5 pts

Question 6 (24 points)

Things to look out for:

- (a) This proof is given in various places in the notes and book. Is the proof written in the candidate's own words? (no points for copying a proof from book/notes, up to 6 pts for a personal presentation)
- (a) The first crucial steps is explaining why there can be a maximum of two elements solving x^2=1 MOD p. How well is that explained? Is it proven? (up to 5 points for some explanation, up to max 8 pts for a proof)
- (a) The second crucial step in the proof is to argue why the remaining elements apart from 1 and -1 MOD p pair off and take each other out in the product (p-1)! MOD p. How well is that explained? (max 4 pts)
- (b) The points here depend upon the depth of understanding shown by the candidate. Do they explain what a primality test is? Do they explain about size of RSA primes? Do they explain about the difficulty of computing (n-1)! MOD n for big numbers? Do they justify any complexity value given? (max 6 pts)

Moderator comments:

The proof is mostly copied from Pia's notes (2). A mention of slow computation was made (1).

3 pts
