

Moderation Sheet/Marking Scheme Assignment Block 3

(Moderators, please use black font colour!)

Candidate Name: Olivia Edbom

Moderator Name: Viktor Rosvall

Moderator's points awarded (max 24) and suggested grade: 17 pts, C

Question 3c (9 points)

Things to look out for:

- (a) Has the candidate clearly explained the discrete logarithm problem? (max 3 pts)
- (b) is it clear after the explanation why it is categorized as a problem? (max 3 pts)
- (c) Is an example given to illustrate the problem? (max 2 pts)
- (d) How was the answer and explanation presented? (max 1 pt)

Moderator comments:

The candidate has clearly explained the problem (3) and it's been categorized as a hard problem (2). No example given (0). Good presentation (1).

6 pts

Question 3d (15 points)

Things to look out for:

- (a) Is the key generation clearly explained? (max 2 pts)
- (b) Is the encryption clearly explained? (max 2 pts)
- (c) Is the decryption clearly explained? (max 2 pts)
- (d) Is it explained why the decryption works? (max 4 pts)
- (e) Is it more than just a listing of the algorithm, e.g. is the algorithm accompanied by a number example and clarifying explanations of all steps? (max 5 pts)

Moderator comments:

The key generation looks fine but the .pdf file is missing symbols, so understanding what's written is a bit hard (2). Same with encryption and decryption (4).

It is not explained why it works (0), but there is an example (5).

11 pts