Moderation Sheet/Marking Scheme Assignment 0

(Moderators, please use black font colour!)

Candidate Name: My Nordqvist

Moderator Name: Viktor Rosvall

Moderator's points awarded 79 and suggested grade: C

Question 1 (10 points)

Things to look out for:

- Has the cipher been broken? (2 pts)
- Has the candidate clearly explained how cipher was broken? (max 5 pts)
- Is the decryption key given? (2 pts)
- How was the answer and explanation presented? (max 1 pt)

Moderator comments:

Cipher has been broken with a method described in little detail. The decryption key was given, but the presentation could be made clearer. (8 pt)

Question 2 (50 points)

10.6.1

Things to look out for:

- Is answer correct? (1 pt)
- Has the candidate clearly explained how they found the disjoint cycle decomposition? (max 1 pt)
- How was the answer and explanation presented? (max 1 pt)

Moderator comments:

The answer given is corrected and the explanation was clear, with a clear and easy to follow presentation. (3 pt)

10.6.2

Things to look out for:

- Are the five answers correct? (max 5 pts)
- Does the candidate work solely in disjoint cycle notation without writing the permutations in matrix format and is it clearly demonstrated that this is so? (max 10 pts)
- Does the candidate know the difference between $\sigma\tau$ and $\tau\sigma$? (5 pts)

- Has the candidate clearly explained how they found the two inverse permutations? (max 5 pts)
- How were the answers and explanations presented? (max 2 pts)

Moderator comments:

The five answer are correct! The candidate works mostly in cycle notation, exception when presenting the work midway, thus it's unclear if matrix notation was used to get the cycle notation. I assume the candidate knows the difference between $\sigma\tau$ and $\tau\sigma$, as the answers given are correct. The calculation of the inverse wasn't clear, and it's possible it was done in matrix notation. Overall the answers were presented in a clear manner. (18 pt)

10.6.4

Things to look out for:

- Has the candidate clearly explained why there are just 3 such permutations? (max 3 pts)
- How was the explanation presented? (max 2 pts)

Moderator comments:

The answer given is false, and I think you didn't know about the formula to calculate permutations. (xxx)(x) isn't part of S4. (0 pt)

10.6.5

Things to look out for:

- Has the candidate clearly identified and presented the set K? (2 pts)
- Has a good notation been chosen? (max 2 pts)
- Is the composition table given correct? (5 pts)
- Has the candidate clearly shown their working for the table? (max 5 pts)
- How was the answer and explanation presented? (max 1 pt)

Moderator comments:

You haven't made a multiplication table and you haven't correctly identified the set K. (0 pt)

Question 3 (5 points)

Things to look out for:

- Is answer correct? (1 pt)
- Has the candidate clearly explained how they found the answer? (max 3 pts)

- How was the answer and explanation presented? (max 1 pt)

Moderator comments:

The answer given is correct and clearly presented. The thought process of why you divide 15! by 7!3!3! could have been better explained. (4 pt)

Question 4 (30 points)

(a) Things to look out for:

- Are the gcd and the linear combination found correct? (2 pts)
- Has the candidate clearly demonstrated how Euclid's algorithm is used to find both answers? (max 6 pts)
- How was the run of the algorithm forwards and backwards presented? (max 2 pt)

Moderator comments:

The gcd and the linear combination was found to be correct. Euclid backwards wasn't demonstrated, so it's a bit unclear that you used it to find the linear combination. (7 pt)

(b) Things to look out for:

- Is answer correct? (2 pts)
- Is the candidate using correct notation for classes and class representatives? (max 4 pts)
- How well was the answer justified? (max 3 pts)
- How was the answer and explanation presented? (max 1 pt)

Moderator comments:

The answer given is correct, using correct notation for classes. The answer was justified as the candidate pointed out that the gcd must equal 1 for there to be and inverse. And the presentation was well done. (10 pt)

(c) Things to look out for:

- Is answer correct? (2 pts)
- Is the candidate using correct notation for classes and modular arithmetic? (max 3 pts)
- How well was the answer justified? (max 4 pts)
- How was the answer and explanation presented? (max 1 pt)

Moderator comments:

The answer given is correct, using correct notation for classes. The answer was justified as the candidate pointed out that the gcd must equal 1 for there to be and inverse. And the presentation was well done. (10 pt)

Question 5 (25 points)

Things to look out for:

- Has the cipher been broken? (5 pts)
- Has the candidate clearly explained all the steps involved in breaking the cipher? E.g. could you clearly identify which letter(s) they had decrypted first? And how they found subsequent ones? (max 15 pts)
- Is the decryption key given? (3 pts)
- How was the answer and explanation presented? (max 2 pt)

Moderator comments:

The first line of the ciphertext has been broken and presented. The candidate was a bit unclear if CrypTool solved the ciphertext, or gave a frequency analysis. It wasn't clear if you used digrams and trigrams for help. The decryption key is given, but it's a bit unclear what is the ciphertext (A) and what is the plaintext (a). (19 pt)