Moderation Sheet/Marking Scheme Assignment Block 1

(Moderators, please use black font colour!)

Candidate Name: Hussen Mohamed Ahmed

Moderator Name: Viktor Rosvall

Moderator's points awarded 13 and suggested grade: F

Question 1 (24 points)

Things to look out for:

- (a) Has the candidate clearly explained how a general substitution cipher works (i.e. not just a monoalphabetic one)? (max 4 pts)
- (b)(i) Has the candidate clearly explained how a **general** monoalphabetic substitution cipher works (i.e. not just a shift cipher)? (max 4 pts)
- (b)(ii) Has the candidate clearly explained how a **general** polyalphabetic substitution cipher works (i.e. not merely a Vigenere cipher)? (max 4 pts)
- (c) Is the example given clearly with cipher and key explained?
- (max 3 pts)
- (d) How well is the break explained? Are details given w.r.t how letter distributions are used to break monoalphabetic ciphers? Are details given w.r.t. which are the most frequent letters, digrams and trigrams?
- (max 8 pts)
- How was the answer and explanation of Q1 presented? (max 1 pt)

Moderator comments:

The question hasn't been answered. (0 pt).

Question 4 (24 points)

Things to look out for:

- (a) Is the definition of Euler's Phi-function given or does the candidate just give a formula for the computation of it?
- (10 pts for definition, only 1 pt for formula)
- (b) Are the answers correct? (max 3 pts)
- (b) Are the full calculations shown? (max 9 pts)
- How was the answer and explanation presented of Q4? Was correct mathematical notation used? (max 2 pts)

Moderator comments:

Definition given is lacking. No formula given. The answers are correct, but the calculations are slightly wrong (6 pt).

Question 5 (36 points)

Things to look out for:

- Is it clear that the key length was found by the Kasiski method or a Friedman test? (2 pts)
- Was it clearly explained how and why the method for finding key length works? (max 5 pt)
- Have all calculations for finding key length been shown in full?
- (max 5 pts)
- Has the cipher been broken? (5 pts)
- Has the candidate clearly explained all the steps involved in breaking the cipher? E.g. for each key letter could you clearly identify which letter(s) they had decrypted first? And how they found subsequent ones? (max 15 pts)
- Is the encryption or decryption key given? (3 pts)
- How was the answer and explanation of Q5 presented? (max 1 pt)

Moderator comments:

Plaintext is given, nothing more (1 pt).

Question 6 (36 points)

(a) Things to look out for:

- Was the defintion of Friedman's Index of Coincidence clearly given? (2 pts)
- Was the computation of Friedman's Index of Coincidence for the given cipher clearly shown and correct to 4 d.p.? (3 pts)
- Has the candidate clearly explained why the computation shows the cipher is not monoalphabetic? (max 5 pts)

Moderator comments:

Insufficient definition given. The computation was correct. (4 pt)

(b) Things to look out for:

- Is the use of a Chi-squared test clearly explained? (5 pts)
- Are the calculations for f and z given in full with all working shown? (max 10 pts)
- How well was it justified that f is a better fit than z? (max 3 pts)
- How was the answer and explanation presented? (max 2 pt)

Moderator comments:

Nothing written. (0 pt)

(c) Things to look out for:

- Is answer correct? (2 pts)
- Is the candidate showing their working? (max 3 pts)
- How was the answer and explanation presented? (max 1 pt)

Moderator comments:

Plaintext is given with no explanation of the workings. (2 pt)