ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

SUPERVISOR'S OPINION OF FINAL THESIS

I. IDENTIFICATION DATA

Thesis name:	**Implementation of Goldwasser-Kilian primality test on elliptic curves**
Author's name:	**Marat Gimadiev**
Type of thesis:	master
Faculty/Institute:	Faculty of Electrical Engineering (FEE)
Department:	Department of Computer Science
Thesis supervisor:	Dr. Bestoun S. Ahmed
Supervisor's department:	Department of Computer Science

II. EVALUATION OF INDIVIDUAL CRITERIA

Assignment **challenging**

Evaluation of thesis difficulty of assignment.

This thesis is dealing with Goldwasser-Kilian primality test to identify the primality of the number. The test can be used for public-key cryptography and security issue. Technically, the thesis is sound and the level of difficulty is fair. The problem that the student is dealing with could be an interesting topic for his future if he decide to go further with the security and cryptography area. The level of programming that the student undertake is also fine.

Satisfaction of assignment **fulfilled**

Assess that handed thesis meets assignment. Present points of assignment that fell short or were extended. Try to assess importance, impact or cause of each shortcoming.

The student assured that the assigned tasks are met. However, the student could have done more in the writing part. Also, he could have done more to declare the problem that he wants to solve.

Technical level **A - excellent.**

Assess level of thesis specialty, use of knowledge gained by study and by expert literature, use of sources and data gained by experience.

Technically, the thesis is good. The level of programming and finding is good.

Formal and language level, scope of thesis **E - sufficient.**

Assess correctness of usage of formal notation. Assess typographical and language arrangement of thesis.

There are many typos in the thesis. Look at the abstract for example. There are also many repeated words. The level of English language could be better than current one in the thesis. The student did not define clearly the aim, objective, scope of the thesis. It is not clear what he wants to do from the beginning. The format of the thesis is not standard. The arrangement of thesis is not good. There are no chapters in the thesis and also the sections are not formatted correctly. The overall structure of the thesis is not that good. Also, the flow of the thesis is boring. The reader cannot read a lot in the thesis. There could be a good literature review section in the thesis.

Selection of sources, citation correctness **C - good.**

This level is fine and the sources used is good. I preferred if the student used more up to date articles and books.

III. OVERALL EVALUATION, QUESTIONS FOR DEFENSE, CLASSIFICATION SUGGESTION

This thesis presents an interesting topic related to the security, cryptography and number theory. The amount of technical work done in the thesis surpass the writing effort. The student should have paid more attention to the

writing of the thesis. The formatting of the thesis is not due to the standard format. Also, it is not clear what are the aim and objective of the thesis. What the student want really to solve? What he conclude from his implementation? Practically, where he can use his implementation? These are not clear.

Also, how the student assure that his implementation is correct? Which kind of testing he used? What are the benchmarks? How he got them?

Overall, the thesis is to the study level of the student.

I evaluate handed thesis with classification grade **B - very good.**

Date: **7.6.2018** Signature: