THESIS REVIEWER'S REPORT

I. IDENTIFICATION DATA

Thesis title:	**Data Security while Using Cloud Services**
Author's name:	**Adelina Akhmedzianova**
Type of thesis :	master
Faculty/Institute:	Faculty of Electrical Engineering (FEE)
Department:	Computer Science
Thesis reviewer:	Alexey Budyakov
Reviewer's department:	Bauman Moscow State Technical University, Department of Computer Science and Control Systems

II. EVALUATION OF INDIVIDUAL CRITERIA

Assignment **extraordinarily challenging**

How demanding was the assigned project?

Widespread cloud storage security policy do not provide the desired level of data protection, including protection from cloud service providers themselves. The most critical disadvantage of the existing solutions in client-side encryption is the low level of security in the implementation of the encryption key management process. The thesis aims to increase the level of data security in the client-side encryption process while using cloud storage services. In order to address this aim, the work proposes the methodology for client-side encryption systematically builds upon the methods to derive an encryption key from both an image and a password.

Fulfilment of assignment **fulfilled**

How well does the thesis fulfil the assigned task? Have the primary goals been achieved? Which assigned tasks have been incompletely covered, and which parts of the thesis are overextended? Justify your answer.

The author proposed new methods for encryption key derivation based on both image and password that provide a higher level of protection from Man-in-the-middle attacks over the baseline. The experiments demonstrated good statistical properties of generated sequences. The author also describes the model and implementation of the software that provides data security while using cloud storage services. The obtained results completely correspond to the assignment.

Methodology **correct**

Comment on the correctness of the approach and/or the solution methods.

The student has chosen correct approach, the proposed methods were properly formulated and the computational results were thoroughly analyzed.

Technical level **A - excellent.**

Is the thesis technically sound? How well did the student employ expertise in the field of his/her field of study? Does the student explain clearly what he/she has done?

The author proved his knowledge of the problematics of encryption key management process and methods of key derivation.

Formal and language level, scope of thesis **A - excellent.**

Are formalisms and notations used properly? Is the thesis organized in a logical way? Is the thesis sufficiently extensive? Is the thesis well-presented? Is the language clear and understandable? Is the English satisfactory?

The text is well written, well structured and quite well organized. The language level is above normal.

Selection of sources, citation correctness	**A - excellent.**
Does the thesis make adequate reference to earlier work on the topic? Was the selection of sources adequate? Is the student's original work clearly distinguished from earlier work in the field? Do the bibliographic citations meet the standards?	
All resources properly cited. The author have cited enough related works published recently. I have not found any violation of citation ethics during reading of the text.	

Additional commentary and evaluation (optional)
Comment on the overall quality of the thesis, its novelty and its impact on the field, its strengths and weaknesses, the utility of the solution that is presented, the theoretical/formal level, the student's skillfulness, etc.
The thesis has good practical implementation. The results are readily used for data protection on the cloud storage. Adelina Akhmedzianova has demonstrated strong knowledge, good programming skills and sense of the purpose.

III. OVERALL EVALUATION, QUESTIONS FOR THE PRESENTATION AND DEFENSE OF THE THESIS, SUGGESTED GRADE

Summarize your opinion on the thesis and explain your final grading. Pose questions that should be answered during the presentation and defense of the student's work.

The grade that I award for the thesis is **A - excellent.**

1. What is the function of the fractal curves in the algorithm?
If their main property (self-similarity) is not used, what advantages do we achieve using these curves?
2. Why the Feistel networks used in the thesis?

Date: **8.6.2020** Signature: