DEPARTMENT OF DEFENSE

DEFENCE INSTITUTE "PROFESSOR TSVETAN LAZAROV"

Sofia 1592, blvd. "Prof. Tsvetan Lazarov" No. 2, fax: 02/92 21 808, http://di.mod.bg

REVIEW

by Assoc. Dr. **Alexander Asenov Kolev,**

member of the scientific jury of the dissertation work of
Engineer **Andrey Georgiev Ivanov**

on "ANALYSIS OF THE RESISTANCE OF PUBLIC KEY CRYPTOGRAPHIC SYSTEMS"

for the acquisition of an educational and scientific degree "doctor" in the doctoral program "Automated systems for information processing and management", professional direction 5.2 "Electrical engineering, electronics and automation", field of higher education 5. "Technical sciences"

1. Relevance and significance of the developed scientific problem

The use of cryptography to protect sensitive information of state, military and personal importance has been known and widely applied since ancient times. The technological development and progress in the information and communication spheres in our time has significantly expanded the scope and increased the need to use cryptography, reaching practically every person with a need for secure submission of personal data electronically. Thus we are talking about public cryptography, which can be argued to be the basis of the functioning of modern society, states and world processes.

Cryptographic systems for the protection of information based on the informed approach of using a public key are of great practical importance. The relevance and significance of the dissertation work is evident in the set goal and tasks related to determining the degree of sustainability in the functioning of public key cryptographic systems. There is no doubt that the topic of the dissertation is consistent with the main content of the text submitted for review. In his work, Engineer Andrey Ivanov examines and analyzes the most widely applied algorithms and approaches used in public cryptography for the purpose of information protection and evaluates the degree of their resistance to attacks related to the presence of certain weaknesses. As a novelty, I define a part of the research work related to the identification of deliberately created cryptographic vulnerabilities, known collectively as "kleptography". The author develops models by which the probability of the existence or non-existence of vulnerabilities of such a "kleptographic" type can be determined.

2. General characteristics and structure of the dissertation work

The dissertation consists of a total of 144 pages, of which 106 pages are the main part and 21 pages are appendices. In the main part of the dissertation, 10 figures and 25 described algorithms in the form of pseudocode are attached. In his work on the dissertation, the author used 114 cited literary sources.

The dissertation is structured in a standard format consisting of an introduction, three chapters, a conclusion, references, a list of publications made during the development of the dissertation, a list of used terms, mathematical notations and basic functions, a list of figures.

In the first chapter, the mathematical and algorithmic foundations of public cryptography are examined, their applicability and areas of use are described, standards applied in practice and requirements for systems using public cryptography are described. The problems related to the stability of functioning of cryptographic systems with public cryptography are assessed and the purpose and tasks of the research work being developed are formulated.

In the second chapter, two models of solving the problems are proposed. The first solution model was built with the purpose of achieving greater efficiency and reliability of the result for determining the divisibility of a number, by using the Miller-Rabin probability algorithm. The second solution model is designed to determine the mathematical possibility of a more efficient implementation of the Silver-Pohlig-Hellman algorithm, through which attacks are implemented against the currently most widespread cryptographic algorithm in public cryptography, known by the abbreviation RSA and developed by the team of Ron Rivest, Adi Shamir and Leonard Adleman.

In the third chapter, the mathematical foundations and model of a new (proposed by the author) approach for the implementation of an algorithm for kleptographic purposes are described. A comparative analysis was made between the proposed algorithm and other existing kleptographic algorithms. An analysis was made and an assessment was made of the possibility of the existence and use of kleptography in practical-applied systems based on public cryptography. A mechanism is proposed to avoid vulnerabilities related to kleptographic attacks on RSA-based systems. Test results achieved by applying a custom RSA key generation software application using the proposed kleptographic algorithm are presented.

Careful familiarization with the dissertation submitted for review gives an idea of the high quality of the author's scientific and research work. Elements of an applied methodology for scientific research can be systematically and consistently traced in the form of: analysis of a scientific-practical problem, formulation of a scientific hypothesis, synthesis of a solution model, experimental confirmation of the expected results by conducting a software experiment.

3. Characteristics of the scientific and scientific-applied contributions in the dissertation work. Credibility of the material

The contributions of Eng. Andrey Ivanov can be defined as scientific-applied and applied. I accept the contributions indicated in the text of the dissertation, which are:

- A solution model is proposed, allowing to increase the reliability of the result for estimating the divisibility of a number as an addition to the well-known Miller-Rabin algorithm. The proposed solution model is tested by playing two numerical examples presented in Appendix 1;
- A new model is proposed for solving systems of congruent equations, without the feasibility of the model depending on existing limiting conditions. The model allows solutions to be achieved without the need for the numbers with which the modulus is calculated to be mutually prime. Using this model in addition to the RSA attack algorithm proposed by Pohlig-Hellman increases the speed of its execution. In support of the proposed new model for solving systems of congruent equations, a numerical example is played, Appendix 2;
- A mathematical apparatus and a practical solution are presented, which allows the creation of a kleptographic algorithm for attacking RSA-based cryptographic systems. A comparative analysis and evaluation of how kleptographic algorithms of this type threaten the stability of functioning of systems using RSA is done. These results raise a question about the sufficiency

of the conditions in the composition of the currently applied standards for evaluating the quality of a generated RSA key. The operation of the presented mathematical apparatus and the practical solution are illustrated numerically in Appendices 3, 4 and 5.

4. Evaluation of the scientific results and contributions of the dissertation work

I define the scientific-applied and applied contributions in the dissertation work as enrichment of existing knowledge with a significant value effect in a future broad practical application. I define the work carried out in item 3.3 of the dissertation "Comparative analysis and evaluation of the possibility of detection" of built-in kleptographic mechanisms in applied cryptographic systems as an essential scientific and practical application.

In favor of the high assessment of the results obtained so far, the set goals for expanding the research work on the subject of this dissertation speak, which can be summarized as:

- Increasing the stability and reliability of key generation used in public cryptography;
- Qualitative and rapid assessment of the presence of implemented kleptography in systems using public cryptography;
- Creating models to serve as the algorithmic foundation for future high-performance hardware cryptographic solutions.

The results included in the dissertation work with previous scientific justification, as well as the overall harmonious impression of the structure of the material, are the basis of my confidence that the work is the personal work of engineer Andrey Ivanov.

5. Evaluation of dissertation publications and authorship

In the appendices to the dissertation "List of publications related to the dissertation" three headings are indicated. In two of them, Engineer Andrey Ivanov appears as the first author, which speaks of his preferential participation in the preparation of the publications. One of the publications in English is in Springer's international specialized publication, Communications in Computer and Information Science, another publication, also in English, is in the international specialized publication Information & Security: An International Journal. The other listed publication in Bulgarian is in the materials of an international scientific conference "Research and investments in technological innovations - a decisive factor for defense and security".

All publications correspond to the topic of the dissertation. Without a citation list attached, two citations to publications from the list can be traced in the public domain.

6. Literary awareness and competence of the doctoral student

In his work on the dissertation, engineer Andrey Ivanov used 114 literary sources. Of these, 79 sources are publications in specialized scientific publications and materials from scientific forums. The remaining 35 cited items are electronic sources and resources. Two of the literary sources are in Bulgarian, the rest are in English.

All mentioned literary sources are reflected in the main text of the dissertation work and are appropriately used to support the thesis defended by the author. The free handling of such rich in quantity and quality scientific material shows the author's very good knowledge of the subject of his dissertation work.

7. Evaluation of the abstract

The presented abstract of the dissertation consists of 40 pages in Bulgarian. In abstract the essential moments of the three chapters of the work, conclusion, achieved results and a list of publications related to the dissertation are shown.

The abstract corresponds to the requirements of the Law on the Development of the Academic Staff in the Republic of Bulgaria (LAD).

8. Critical Notes

I make the following critical comments on the layout of the dissertation:

- Figure 2, placed in the text of item 1.1.2, has an inappropriate resolution, which makes it difficult to perceive the graphic content presented in it;
- The list of electronic sources and resources cited is not in the typical format for similar materials. For some of the electronic sources, the moment in time when they were accessed is not indicated.

My critical remarks in no way detract from the overall high quality of the peer-reviewed dissertation.

I recommend to Engineer Andrey Ivanov that in the future he directs more of his publications to publications that are indexed in internationally recognized databases with scientific production.

9. Personal impressions

According to the attached autobiographical data, in 2000, Eng. Andrey Ivanov completed his higher education at “Panayot Volov” VVUAPVO, majoring in "Computer Engineering and ASMS" with a master's degree. He worked as an enlisted man in the Department of Defense system until 2019, when he was discharged from military service and transferred to the military reserve. After 2019, he works in IT companies whose activities are related to cryptography and cyber security.

I know Engineer Andrey Ivanov from personal meetings during participation in scientific forums, as well as during his visits in the last few years to the Defense Institute "Professor Tsvetan Lazarov". During conversations held with him on scientific topics and on issues related to his work on the current dissertation, he shows a high level of scientific training and competence in the field of his scientific research.

I believe that Eng. Andrey Ivanov has great potential for development as a young scientist in the chosen professional direction.

10. Conclusion

As a consequence of what has been stated so far, I define the dissertation work of Eng. Andrey Ivanov as meeting the requirements of the "Regulations on the conditions and procedure for acquiring scientific degrees at the Institute of Defense" and ZRASRB for the acquisition of the educational and scientific degree "doctor".

11. Evaluation of the dissertation work

I give a positive assessment of the dissertation work and its appendices. I recommend to the respected members of the Scientific Jury and to the respected members of the Scientific Council to vote **FOR** awarding Eng. **Andrey Georgiev Ivanov** the educational and scientific degree "doctor" in the doctoral program "Automated information processing and management systems", professional direction 5.2 " Electrical engineering, electronics and automation", field of higher education 5. "Technical sciences".

07.02.2023

Reviewer: ..../S/...........
(Assoc. Dr. Alexander Kolev)