History of Cryptography in Syllabus on Information Security Training

Sergey Zapechnikov, Alexander Tolstoy, Sergey Nagibin

HAL Id: hal-01334298

https://hal.science/hal-01334298

Submitted on 20 Jun 2016

History of Cryptography in Syllabus on Information Security Training

Zapechnikov Sergey, Tolstoy Alexander and Nagibin Sergey

The National Research Nuclear University MEPhI (Moscow Engineering Physics Institute), 31 Kashirskoye shosse, Moscow, Russia

{SVZapechnikov, AITolstoj}@mephi.ru

Abstract. This paper discusses the peculiarities and problems of teaching the historical aspects of Information Security Science (ISS) to the students of the "Information Security" specialization. Preferential attention is given to the ISS area with the longest history, namely cryptography. We trace exactly what ideas of fundamental importance for modern cryptography were formed in each of the historical periods, how these ideas can help students in mastering the training courses' material, and how to communicate these ideas to students in the best way. The conclusions are based on the results of studies conducted over a few years at the "Cybernetics and Information Security" Faculty of the NRNU MEPhI, where our ideas are implemented in the educational process. We teach the history of cryptography in a few educational courses for Specialists in IS and Masters in Business Continuity and IS Maintenance in the form of introductory and individual lectures and seminars. Specific recommendations on the use of the historical facts considered during the classes are given.

Keywords: Information Security Science, Syllabus, Information Security Training, History of Cryptography

1   INTRODUCTION

The study of any science's history is a part of the syllabus for students in disciplines with deep historical roots. Cryptography is one of these areas. The earliest evidence of cryptographic techniques being used for text protection refers to the XX century BC, as is well known from the archaeological data. Thus, cryptography has a history of at least forty centuries. But for a long time this area of activity was not a scientific discipline in the modern sense of the word. Rather, it was an art known to a few people who know how to protect the content of written documents from prying. Information protection (IP), and especially cryptography, began to build actively on a scientific basis only in the late XIX – early XX century. It is due to the fundamental changes in modes of representation, transmission and transformation of information in new technical systems such as the telegraph, telephone and various electromechanical devices. However, the IP method continued to be developed on the old basis until the mid XX century. The appearance of the well-known paper by Shannon, "Communication The-

ory of Secrecy Systems", in 1949 and the rapid development of computer technology caused an irreversible transformation of cryptography in mathematical and computer science.

The exploration of the rich heritage of pre-scientific cryptography has a huge cognitive and wide educational value for modern IS specialists because of the abundance of ingenious solutions and good practices gained during a long quest of many generations. That makes it possible to avoid unnecessary repetition of mistakes and missteps when creating IP tools and to prevent accidents while designing cryptosystems.

Certainly, the history of science should take into account not only the history of ideas in the relevant field of expertise, but also the history of all human activities related to the implementation of these ideas. However, in a few academic disciplines it is possible to track only the most important milestones in this history, i.e. the history of ideas in the field of cryptography and other ways of document protection. The history of the facts can be traced to a much lesser extent because of the limited time allotted for the study of academic disciplines.

Therefore, it is possible to list the following reasons for including classes on the history of cryptology as a part of students' training in the field of IS:

- Such a class demonstrates that cryptography as any other significant area of human activity has not only its own theory, but its own history as well. That history helps to better understand the theory, and vice versa;
- Such a class can help students better understand how modern cryptography (and ISS in general) was formed and developed, and the laws and patterns for the accumulation and generalization of human knowledge;
- Faced with the differences and diversity of forms of man's thought and action through many centuries and countries, students can better understand their own identity and the role of modern science in historical processes.

Thus, the paper is organized as follows. After discussing the purpose of introducing the historical aspects of cryptography into the learning process in Section 2, we note the ways in which the history of cryptography is presented in the syllabus of training Specialists and Masters in the NRNU MEPhI. In Sections 3-6 we discuss in more detail how the most important ideas of the main periods in cryptography development (pre-scientific, classical science, transition phase from classical to modern science and modern science) can best be taught by the lecturers and studied by the students of a few courses on IS. Section 7 briefly presents some related works. The directions of future work are identified in conclusion.

2   FORMS OF HISTORY OF CRYPTOGRAPHY'S CLASSES

In accordance with the state Russian educational standards, courses training Specialists and Masters do not discuss the history of science. The "History and Methodology of Science" discipline is provided only for post-graduate students. In this regard, we have to look for other ways to have the students learn about the history of the field of science in the process of mastering the syllabus. Some ways are:

- introductory lectures on various subjects;
- scientific seminars;
- individual lectures on the "Humanitarian Issues of Information Security" and "Cryptographic Protocols and Standards" disciplines for the Specialists in IS;
- lectures and workshops as a part of the introductory discipline entitled "Fundamentals of Business Continuity and Information Security Maintenance" for the Masters.

Presenting history in the introductory lectures allows the instructor to place the studied disciplines into their general scientific context, to show communications and parallels with the other disciplines, including those devoted to the study of almost exclusively classical science such as basic mathematical and engineering disciplines. For example, it is very useful to draw a time axis with the major periods in the history of cryptography and to show the development of different areas of this science at the second half of the XX century at the introductory lecture on the "Cryptographic Protocols and Standards" discipline (Fig. 1).
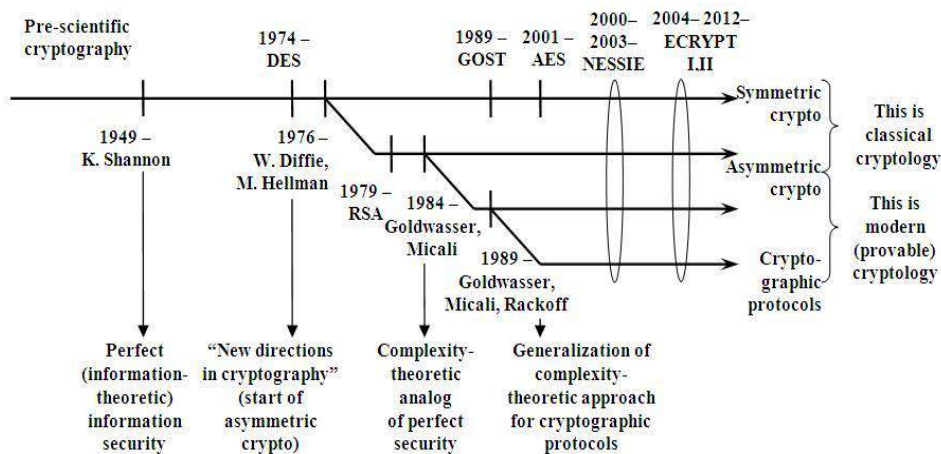

Fig. 1. Scheme's example used during the introductory lecture to the "Cryptographic Protocols and Standards" discipline, showing cryptography's history periodization

Our experience shows that the teachers of classes on the history of cryptography should have a good knowledge not only in the world history, but also in the foundations of cryptography. Since the classes are designed for the students specializing in mathematical and computer sciences, it is better that the teachers' basic education is natural or computer sciences rather than humanitarian sciences.

We recommend seminars in an interactive form. For example, all students take turns preparing reports, discussing them with their teachers and presenting them during the classes. The necessary requirements for getting credits for that part of an educational course that includes one section on the history of cryptography are their own report presentation, reviewing 2-3 reports of other students, and participating in their discussions.

In general, while planning the history of cryptography classes, we divide the history into the following periods:

I. Pre-scientific period (from ancient times to the end of the XVII century);

II. Classical science period, in which the scientific basis of cryptography was formed (XVIII–XIX centuries);

III. Transition phase from classical to modern science (the end of the XIX century – the beginning of the XX century); and

IV. Modern cryptography (the second half of the XX century – the beginning of the XXI century).

The history of related sciences (e.g. steganography and methods of protection against falsification of paper documents and banknotes) is also discussed in parallel with the history of cryptography, using the same periods.

Some recommendations for the study of the main periods in the history of cryptography, as well as a few ideas that can be implemented during lectures and seminars, are presented in the following sections.

3   THE PRE-SCIENTIFIC PERIOD AND ITS LESSONS

The main educational reason for studying the pre-scientific period of cryptography's development is to show the following:

- what main methodological ideas were used in the first known techniques of cryptographic IP;
- how these ideas were developed and generalized as time passed; and
- why they continue to be the foundation of many cryptographic techniques.

This period is illuminated in a number of books on the history of cryptography [1-5]. However, in most modern textbooks on cryptographic IP methods the pre-scientific period's codes serve only as a background against which to present the advanced modern techniques. However, research into the ancient techniques of protecing written communications still cannot be considered completed. The codes used in ancient Greece, ancient Rome, and medieval Western Europe are well-known and described in detail. They overshadow the achievements of many other nations and civilizations that also contribute to the history of cryptography. Therefore, when creating material for our classes, we use not only well-known sources, but also rely on the results of our own research [6-8].

The ancient and medieval methods of protecting written texts are very suitable to demonstrate to the students the basic principles of concealing the text contents from unauthorized persons, as well as the simplest methods of their breaking. The main difference between them and modern ciphers is simplicity meaning that they are easily observable. The basic ideas can be easily explained by the teacher during one lecture and can be understood even by those students who do not specialize in the field of IS or other areas of mathematical and computer sciences.

However, the teacher should be cautioned against too direct a comparison of pre-scientific and modern IP methods. Ancient cryptography should be considered pri-

marily a linguistic phenomenon and a specific method of transmitting thoughts by a community of people, knowing one or another "secret language". Its main feature compared to modern cryptography is that the text was merely a sequence of characters, regardless of its semantic content (coherent text, a set of numbers, etc.), whereas modern cryptography is based on mathematical formalism and formal logic.

In this regard, we recommend the teacher emphasize the following while discussing cryptography of the prescientific period.

1. Almost all ancient civilizations knew cryptography as a special linguistic phenomenon, fixing on physical media the "secret languages" that existed in different social groups since time immemorial. These languages have an origin in magical ritual, but later they were understood as a tool for social communication. In this regard, cryptography has two main application areas in the ancient history:

- "magic" – to conceal a meaning of names, magic rituals, secret ritual knowledge and another taboo information, i.e. for secret communications with the supernatural (that was an integral part of the lives of all ancient civilizations);
- "practical" – to protect military reports, personal correspondence, and perhaps trade secrets, i.e. for secret communication in human society.

2. The most important encryption principles – replacement and permutation of characters – were empirically discovered in the Ancient World. In the Ancient World, these principles exhausted the arsenal of cryptographic protection methods for written texts, and they were realized only for special, very simple cases. Evolution of the cryptographic methods was extremely slow because the existing methods were generally sufficient.
3. Along with cryptography, the ancient civilizations used various methods of physical protection of messages by encoding and steganography. That served different practical purposes such as concealing the fact of message's existence or transfer, hiding the names of senders or recipients, accelerating copying text and reducing the amount of material to be carried or memorized, transmitting messages at a rate greater than a man's speed, and raising the value of the text to the reader. These objectives were often seen as a priority compared to concealing the message's meaning from unauthorized persons.

While studying cryptography in the Middle Ages and the early New Ages (XVI – XVII centuries) it is reasonable to stress the following:

- The encryption methods have become more complex in the Middle Ages: polyalphabetic substitution has been invented. The systematic methods of cryptanalysis have appeared in the Arabian world for the first time;
- Signatures and stamps ensured a document's authenticity for the first time in Byzantium, along with encryption ensuring the confidentiality of documents;
- Ciphers are still considered a linguistic phenomenon: single words, sentences, paragraphs, sections of the document are converted.

One of the techniques that can be used to indicate a close relationship between history and modernity of cryptography and to inspire students who are accustomed to think in terms of modern mathematics and formal logic is to mathematically analyze ancient ciphers (like shift, replacement, affine and permutation ciphers). However, the general cases of substitutions and (or) permutation were not implemented in any classical ciphers and cryptographic devices, and the particular cases used essentially reduce the cipher strength. Nevertheless, a number of examples might illustrate the fact that the most secure classic ciphers such as the Vigenère cipher and "Latin squares" are widely regarded as almost unbreakable until the appearance of computers in the XX century.

Our experience shows that the students analyze classical ciphers with great interest. On the one hand, the examples are readily understandable and the validity of the findings can be checked without using software. On the other hand, similar analysis of the modern ciphers' security such as AES, the Russian standard GOST 28147-89 [9], RC6, etc. is simply impossible in classes because of great complexity of ciphers and the time required.

4   THE PERIOD OF CLASSICAL SCIENCE

The main educational goal in studying the period of classical science is to show how the important mathematical methods were formed during this period. They have become the basis of a variety of protection methods (including asymmetric cryptography) later in the XX century. Many discoverers cannot anticipate the fundamental importance of their works for the future of science.

The classical science period (the XVI century – the end of the XIX century) is a stage of historical development of science, during which the system of the most important natural science concepts and ideas was formed. This system is the foundation of today's scientific knowledge and method. Mathematical knowledge particularly flourished during this period. This is fully applicable to cryptography. Many famous scientists can be mentioned here: Leon Battista Alberti, Francois Vieta, Giovanni Battista Porta, Blaise de Vigenère, Francis Bacon, as well as many interesting ciphers' designs of the time: Cardan grille, Vigenère's cipher and many others. Research about this period of cryptography's development has not been completed. Therefore, while creating lessons for the classes we used our own scientific results [10].

During the classes, we draw students' attention to the following basic ideas related to the period of classical science:

- Encryption techniques become more complicated: combinations of substitutions and permutations in one cipher are used;
- Methods of cryptanalysis are improved and a competition between cryptographers and cryptanalysts is enhanced;
- Pure and applied mathematics, long considered just an abstraction, are developed; later in the XX century they served as the foundation for most of the natural sciences and engineering; and

- Principles of engineering and technical IP begin to be developed as one of the areas of engineering science.

Our experience shows that one of the most effective forms of studying the classical science's period is to obtain an acquaintance with the biographies of the outstanding scientists who greatly contributed to the mathematical foundations of modern cryptography and its creative and scientific methods.

The most striking example that should be included in the syllabus is a study of Leonard Euler's creative heritage. Euler's contribution to world science is truly priceless. He essentially founded several mathematical sciences: analytic number theory, calculus of variations, complex function theory, differential geometry of surfaces, analytical mechanics, rigid body dynamics, as well as many parts of the theory of differential equations, theory of algorithms, theory of elliptic functions, celestial mechanics and other areas of pure and applied mathematics. This scientist had encyclopedic knowledge. His interests extended to many branches of astronomy, acoustics, optics, statistics, botany, medicine, chemistry, linguistics, music, and engineering. Almost all Euler's results belonging to the areas of mathematics that form the foundations of modern cryptology are centered on his discoveries in numbers theory.

At present Euler's works are considered to be the most important and fundamental works for asymmetric cryptography. Of course, Euler himself could not have foreseen the development of the methods and areas of cryptology known today and studied in different courses as the basis of this science. However, the main ways of using Euler's results can be grouped into four categories:

1. Testing the primality of numbers (widely used to generate asymmetric cryptographic parameters);
2. Computationally complex problems in number theory (e.g. the Euler theorem, study of the properties of quadratic residues and the theory of primitive roots; these are closely related to three computationally complex problems in numbers theory, which now form the basis of the most common asymmetric cryptosystems, namely the Rivest-Shamira-Adleman (RSA) problem, the problem of quadratic residues and the discrete logarithm problem);
3. Cryptosystems based on computationally complex problems. The RSA problem is the basis of security of the RSA encryption scheme and the RSA digital signature scheme. Security of cryptosystems such as the Goldwasser-Micali probabilistic open encryption scheme, the pseudo-random BBS (Blum-Blum-Shub) generator and the Paillier open encryption scheme is based on the problem of quadratic residues. The ElGamal encryption scheme and the ElGamal digital signature scheme and its variants DSA (USA digital signature standard) and GOST R 34.10-2012 (Russian digital signature standard) [11] are based on the discrete logarithm problem; and
4. Cryptographic protocols that use primitives based on the above computationally complex problems. Some constructions, the security of which is based on the same computationally complex problems, can be used in addition to the above listed cryptosystems as the building blocks for cryptographic protocols. The most famous example is the Diffie-Hellman public key distribution protocol and numerous pro-

tocols derived from it (e.g. MTI, STS, etc.). Their security is ultimately based on the discrete logarithm problem and the Diffie-Hellman problem. Less well-known examples are the zero-knowledge proof protocols that can use all three of the above problems. For example, security of the Shnorr zero-knowledge authentication scheme is based on the intractabilility of the discrete logarithm problem.

The above examples are enough to make a conclusion about the fundamental significance of Euler's results for modern cryptologic science. The most important results, which seemed during his lifetime to be a game of numbers, have provided the mathematical basis for asymmetric cryptography two hundred years after Euler's death.

Another set of no less spectacular examples that can be discussed in the classroom are the biographies of the great German mathematician Carl Gauss and the brilliant French mathematician Evariste Galois, both far ahead of their time in the creation of group theory and the theory of finite fields.

5   THE TRANSITION PHASE FROM CLASSICAL TO MODERN SCIENCE

From our point of view, the main educational goal of studying the transition phase from classical to modern science is to become familiar with the concepts that became the basis of "new" cryptography at that time. Scientific and technological progress leads to changes in presentation and communication of information, and formation of the most important concepts such as data (as information provided in a computer form), coding (as a system of rules of information transfer in the data), etc. This is due, primarily, to the development of the telegraph, telephone, and electromechanical devices of information transforming.

Thus, during the classes on the history of cryptography it is necessary to identify and explain to the students the following basic ideas related to this period:

- There was a fundamental change in media, the ways of presenting, processing, and transmitting information such as electrical signals and electromechanical machines, replace paper and pencil in this period;
- The perfectly secret cipher was invented in 1917 (by Vernam of the AT&T company), but its perfect secrecy was justified intuitively – that property was not strictly proven for the cipher;
- Construction principles for the ciphers used in practice evolved nearly to modern principles; codes' design became a complex network of substitutions and permutations, but they were realized by means of the mechanical and electromagnetic devices available at that time; and
- Both block and stream ciphers were widely applied in practice.

From our point of view, it is appropriate for the classes to include some materials primarily related to the invention of the one-time cipher pad and the rotor cipher machines.

It is well known that Gilbert Sandford Vernam invented the automated one-time pad (perfectly secret cipher) in 1917. Studying the one-time pad is usually included in the curriculum of the standard cryptologic educational courses. Therefore, to avoid repetition it should be used as a basis to draw parallels with more recent inventions in the field of cryptography as well as to show a specific example of how new discoveries appear as a result of generalization of known results and, in turn, how former discoveries become the special cases of new discoveries. The one-time pad is very useful for that purpose as the inventor of the cipher assumed that it is unbreakable without proving that fact.

The mathematical formulation of the problem of IP, and derivation of the ideal conditions under which its solution is possible, was developed by C.Shannon (1949) [12]. Shannon's theory implies that the Vernam cipher is a special case that provides information-theoretic but not practical security. Thus, more than 30 years passed between an invention with an intuitively reasonable argument, and the rigorous proof of that argument.

However, this date does not mark the end of the history associated with the invention of the one-time pad. At the beginning of the 1980s G.R.Blakley has shown [13] that the Vernam cipher is just a special case of the so-called shadow ciphers.

In addition, with the discovery of the threshold cryptography principle by A.Shamir [14], it became possible to assert that the Vernam cipher is a special case of the threshold secret sharing schemes, namely a 2.2 Asmuth-Bloom threshold secret sharing scheme.

The study of this example helps the students understand better the typical path of development of scientific knowledge from the particular to the general.

The history of the creation and cryptanalysis of perhaps the most famous families of the rotor cipher machines can be used during the classes to illustrate the period. The lecture should note that the rotor cipher machines are already the direct prototypes of the modern block and stream ciphers, implementing the same principles: layered substitution and permutation transforms for the block ciphers and pseudo-random generator for the stream ciphers. The German Enigma machines, the American Hagelin machines (M-209, C-52 etc.) and the Russian Fialka M-125 machines implemented block ciphers. The German Lorenz SZ 40 and SZ 42 machines implemented the stream ciphers.

It is appropriate to discuss a mathematical description of a rather complex transformation implemented by the rotor cipher machines, and a mathematical formulation of the inverse cryptanalytic problem of finding a transformation key. The teacher can ask the students to conduct their own assessment of the algorithm's complexity. Doing so will allow them to get a clear idea of how much more difficult the problem is while comparing it with cryptanalysis of the pre-scientific ciphers, and why the creation of the first computers by the group under Alan Turing supervision was required to solve it.

The software models of some rotor cipher machines presented on the Internet (for example, a good simulator of Hagelin's M-209 machine [15]) can be used here for illustrative purposes.

Finally, to complete the study of the period it is necessary to characterize Shannon's works and above all his famous "Communication Theory of Secrecy Systems" [12] as well as the works of his followers. It should be emphasized that the essential impact of this Shannon's work is that he formulated the idea of information-theoretic secrecy.

The IS concept as a philosophical concept was formulated in the same period. N.J.Danilevsky (1822 – 1885) was the first Russian scientists to address the problem [16]. Our colleagues developed it further in [17].

6   STUDYING MODERN CRYPTOGRAPHY

While studying the history of modern cryptography it should be stressed that the subject of cryptography expanded and became one of the computer sciences, along with the other sciences like the theory of algorithms, programming, the computational complexity theory, etc. The history of its development becomes a part of the IT history. Various computer equipment, information, and telecommunications systems provide the technical basis for the implementation of all basic IP methods and tools. The largest manufacturers of IT products, leading universities, and research centers became the driving force behind the development of ISS.

In addition to paper, new media in the form of a global, distributed, electronic environment for information processing appeared. New "computer" cryptography with its two main branches (symmetric and asymmetric) becomes the basis of most, if not all IP methods.

Modern cryptography almost entirely focuses on the computer processing of information and the development of appropriate algorithmic and technical methods. Works devoted to new methods of securing information using paper as well as encryption algorithms that can be executed manually are few in number.

It should be taken into account that the study of many important discoveries of the second half of the XX century is usually included in standard courses on cryptography. To avoid repetition, we recommend the teacher focus on the personalities and companies that greatly contributed to the development of IS science and practice. In this case, a good example is the history of the highest award in the field of Computer Science and IT – the Turing Award, often called the "Nobel Prize of computing". Five outstanding scientists in the field of mathematical foundations of cryptography, formal and logical methods of IS and related fields have been rewarded over the past 20 years [18]: Manuel Blum, Andrew Yao, Ronald Rivest, Silvio Micali and Shafi Goldwasser, and Leslie Lamport. They are well known to those skilled in IS. These facts indicate that IS is recognized by the community of scientists as an extremely important area of modern computer science.

During the classes we also recommend giving the students an idea of the work of the cryptographic community, which fundamentally changed in the second half of the XX century. Cryptography is no longer a "secret" science. The perception is that the chance of finding a solution that is stable, free from faults and weaknesses is much higher when an open and comprehensive discussion of new cryptosystems occurs by

the whole scientific community. In recent decades, this kind of activity mainly goes through a process of international (and national) standardization.

As an example of the results brought by standardization and its problems, the teacher can mention the development and adoption of the first USA encryption standard DES (1979), the first Russian encryption standard GOST 28147-89 (1989) [9], the new USA encryption standard AES (2001), other USA cryptography standards such as FIPS 140, SHA, DSA, the widely-used international cryptography standard ISO/IEC 18033 (2006-2010), new Russian standards GOST 34.10-2012 (elliptic curve digital signature) [11] and GOST R 34.11-2012 (hash function Streebog) [19], etc.

Another aspect of the history of cryptography is the historiography of cryptography and cryptanalysis. During the second half of the XX century, a number of fundamental works on the history of cryptography from ancient times to the present days appeared. Of course, the greatest impact on the public has been Kahn's book "The Codebreakers: The Story of Secret Writing" [1]. It initiated a number of other works and in general significantly increased interest in the history of cryptography and cryptanalysis. Many researchers around the world began to study their national traditions and achievements of their countries in the field of cryptography in different epochs.

7   RELATED WORKS

Of course, we are not the only ones to include historical aspects of ISS in the students' syllabus. The history of ISS and in particular the history of cryptography is not often highlighted as a separate academic discipline (course), but some sections of "Cryptography" or "Network Security" disciplines, dedicated to the history of cryptography, are taught in several Russian and foreign universities. In particular, a section on the history of cryptography is included in the online "Cryptography I" course by Dan Boneh at the "Coursera" portal [20]. Some other universities worldwide have specific courses on the history of cryptography [21–23], including Russian universities [24].

8   CONCLUSION

Summarizing the results of introducing the history of cryptography into the syllabus for the students' training on IS direction, we conclude with the following.

1. Studying the history of cryptography serves one of the essential aspects of forming the professional expertise for students preparing to become an IS specialist or the Masters in Business Continuity and Information Security Maintenance.

2. Studying the history of cryptography allows the students to deeply understand why ISS has developed the way it has. The theory cannot explain everything; some issues are due to traditions. And this leads to a deeper understanding of the subject.

3. Knowing the history allows to understand the current trends and predict the future.

Most of our findings are original; they are based on our own investigations of the history of cryptography. We are going to continue this research in order to create a tutorial, which will reflect adequately all periods of cryptologic science, with particular attention to the development of this branch of knowledge in Russia. Any historical research is always laborious and requires a long time, but we hope to report the results of our new research in this area at the next WISE10 conference.

9   REFERENCES

1. Kahn, D.: The codebreakers: The story of secret writing. Macmillan, New York (1967)
2. Mollin, R.: Codes: The guide to secrecy from Ancient to Modern Times. Taylor & Francis Group, Abingdon (2005)
3. Bauer, F.: Decrypted secrets: Methods and maxims of cryptology. 4th ed. Springer, Heidelberg (2007)
4. Rusetskaya, I.A.: Istoriya kriptografii v Zapadnoy Evrope v rannee novoe vremya. Tsentr gumanitarnyh initsiativ; Universitetskaya kniga, Sankt-Peterburg (2014) (in Russian)
5. Bauer, C.: Secret history: the story of cryptology. CRC Press, Boca Raton (2013)
6. Zapechnikov, S. V.: Cryptography as the phenomenon of Russian literature language (XII – XVII centuries). Security of Information Technologies. 2, 116-123 (2011) (in Russian)
7. Zapechnikov, S. V.: Protection of documents, cryptography and secret communications in Byzantium (IV–XV centuries). Security of Information Technologies. 2, 49-61 (2012) (in Russian)
8. Zapechnikov, S. V.: Cryptography and secret communications in the Ancient world. Security of Information Technologies. 2, 83-95 (2014) (in Russian)
9. Russian state encryption standard GOST 28147-89, http://en.wikipedia.org/wiki/GOST_(block_cipher)
10. Zapechnikov, S. V.: About the history of cryptography: the Leonardo Euler's contribution in formation of mathematical basis for modern cryptology. Herald of Russian State University of Humanities: Informatics, Information Security, Mathematics. 14(94), 29-52 (2012) (in Russian)
11. Russian state digital signature standard GOST R 34.10-2012, https://tools.ietf.org/html/draft-dolmatov-gost34102012-00
12. Shannon, C.: Communication theory of secrecy systems, http://netlab.cs.ucla.edu/wiki/files/shannon1949.pdf
13. Blakley, G.R.: Key management from a security viewpoint. Advances in cryptography – A report on CRYPTO'81. ECE Rept No 82-04, Dept. of Electrical & Computer Engineering, University of California, Santa Barbara, CA, USA, pp. 82 (1982)
14. Shamir, A.: How to share a secret. Comm. of the ACM. 22, 612-613 (1979)
15. US M-209 Simulator 3.0, http://users.telenet.be/d.rijmenants/en/m209sim.htm
16. Danilevsky, N.J.: Russia and Europe. Moscow, Kniga (1991) (in Russian).
17. Malyuk, A., Miloslavskaya, N.: Information Security Theory Development. In: Proceedings of the 7th International Conference on Security of Information and Networks (SIN2014), September, 9-11 2014 Glasgow (UK), pp. 52-55. ACM, New York (2014)
18. "Turind Award" at Wikipedia, http://en.wikipedia.org/wiki/Turing_Award
19. Russian state hash function algorithm GOST R 34.11-2012, https://tools.ietf.org/html/rfc6986
20. Boneh, D.: "Cryptography" online course, https://www.coursera.org/course/crypto

21. History of computer cryptography and secrecy systems, http://www.dsm.fordham.edu/~mathai/crypto.html
22. Cryptography defined/brief history, http://www.laits.utexas.edu/~anorman/BUS.FOR/course.mat/SSim/history.html
23. Cryptography: The private history of secret codes, https://brooklynbrainery.com/courses/cryptography-the-private-history-of-secret-codes
24. "History of cryptography" course at Higher School of Economics, http://www.hse.ru/edu/courses/126240458.html (in Russian)