Cryptography as a Paradigm Proposal for Building the Computer Science Knowledge

LADISLAV HURAJ, VLADIMÍR SILÁDI
Department of Computer Science
University of Matej Bel
Tajovskeho 40
SLOVAKIA
{huraj, siladi}@fpv.umb.sk

Abstract: Information security, and Cryptography as a part of it, is a critical topic for computer science students to understand. Different teaching approaches can be effective in helping the students understand abstract principles.
In this paper, we present our approach to Cryptography education that is based on the idea that the stages of growth of the individual might recapitulate the stages of growth of the science. The Cryptography is apprehended as pilot model for further proposal of Computer Science education.

Key-Words: History, Ontogeny, Phylogeny, Cryptography, CS subjects, Knowledge

1 Introduction

Information security, and Cryptography as a part of it, is a critical topic for computer science students to understand. Different teaching approaches can be effective in helping students understand abstract principles.

In this paper, we present our approach to Cryptography education that is based on the idea that the stages of growth of the individual might recapitulate the stages of growth of the science. Our experience of this approach at all types of schools is described in detail.

In the light of the need to protect information and information systems, Information Security became one of the most important areas of Computer Science. Because of the very features of connectivity and accessibility that make information technology indispensable especially in the networking and e-business, information security has been more important than before [1].

Information Security deals with topics like ciphering, identification and authentication, digital signature, message integrity, authorization mechanisms etc. Our educational approach in this area is not oriented on cryptographic tools (nevertheless, in real life these cryptographic tools are usually used without users realizing it), but on the explanation of the background as well as practising the principles and methods of the techniques for students. Such design of a curriculum leads the students more to the content of the subject [2].

Moreover, parts of Information Security as well as of Cryptography are possible to be found in CS curricula in all types of schools – universities, secondary and primary schools.

Our approach to Cryptography education is based on the idea that ontogeny (the stages of growth of the individual) might recapitulate phylogeny (the stages of growth of the science). The idea arises from Jean Piaget's (1896-1980) philosophy of science where *genetic epistemology* is described as a theory concerning the growth of knowledge both in the individual and in science.

The method of genetic epistemology is often used in mathematics education, e.g. in [3]. Its application to Computer Science education is still open question. The approach arise a question:

- Is it possible to transfer this method to Computer Science Education? For all subjects or just partially?
- How can the history of Computer Science be used for the teaching of Computer Science?
- If a teacher is aware of the history of Computer Science, does this make him/her more able to understand the development of CS topics within the CS syllabus?

Exactly the Cryptography is the part of Computer Science that is especially suitable for such an approach.

Moreover, there are some cryptographic ways of teaching mathematics, e.g. [4, 5], to motivate mathematics learning and to achieve significant improvement in students' understanding of several algebraic, analytical and statistical concepts. However, these ways are focused on mathematical background rather than informatics aspects.

This paper presents one possible approach how to promote understanding of Cryptography as a part of Computer Science and to provide an insight into using of

historical approach in CS Education. We tried to formalize the process.

The paper is organized as follows. In the next section, we shortly describe the theoretical background of the project. In section 3, we give some overall impressions of the way in Computer Science Education and finally section 4 gives the preliminary conclusions and possible future work.

2 Theoretical background

The idea of following of the historical background in education is not new. The binding of both the history of science and the history of knowledge were described in detail in the study of Piaget's genetic epistemology. Piaget's vision of genetic epistemology as a science conjoining historico-critical and psychogenetic methods is based on theoretical presuppositions that touch the relation between cognitive development and history of science [6]. Ontogenesis and historiogenesis, according to this assumption, share functional mechanisms that give both developmental lines a definite shape. In Piaget's theory, development occurs as an ordered evolution of structures, with this structural growth process following a certain logic [7]. He also stated that knowledge consists of structures, and comes about by the adaptation of these structures to the environment. He used the term 'genetic' in its 19th-century sense of 'developmental' and not in today's biological sense of 'depending on genes'.

There are two weaknesses while following the phylogeny in education process:

(i) The first one is based on the fact that historical processes of science are permanent discovering, evolution is not straight, and there is lots of indirectness and impasses, e.g. rediscovering the forgotten cipher or weak cryptosystems in the history of Cryptography. On the other hand, curricula present established direct structures to students that provide faster progress of students but leave less to their autonomy and creativity.

(ii) The second weakness is that historical structure (e.g. asymmetric cryptography, hash function, secret sharing …) was often an intellectually demanding process requiring a great deal of knowledge and is in most cases impossible to be re-executed in ontogeny.

Both weaknesses of genetic epistemology are possible to be overcome (to a certain extent).

The first weakness may be overcome by focusing not on the whole structure process but only on motivational dominants that initialized the process as well as on key impulses inside the process. On the other hand, mistakes help one to grow in cognitive process as well.

The second weakness may be overcome by imitation. On simple cryptographic topic it is possible to explain the structure of hard cryptographic problem or the most significant ideas about it.

3 Course Curriculum

Course curriculum is based on the phylogeny of Cryptography; see Table 1 – timeline of cryptography milestones. For ontogeny, it is important to consider the division into four stages from phylogeny that describes the evolution of cryptography. The first stage, the Early Stage, uses mostly manipulation with substitution and transposition on intuitive level. In the second stage, mechanical and electronic cipher machines stage, the first mathematical descriptions of cipher are established. The third one, the computer stage, brought mainly ciphers belonging to a family labeled “Feistel ciphers”. In the fourth stage, from asymmetrical cryptography to present, the invention of Asymmetrical Cryptography based on Number Theory occurred. The pupils’ activities are tight bound to these stages. Selection of pupils' activities in the order corresponding to the history of the cryptography is shown in Table 2.

For cognitive development, the most significant is the transition from the first stage to the second one, i.e. understanding of principles of ciphering as well as transition from intuitive to systematic using of substitution and transpositions, from Concrete operational to Formal operational.

In parallel, creative thinking, cooperation within team skills is enhanced and various contents are introduced. The cognitive as well as social learning strategies are used. A typical task introduces discovering and demonstrating of certain cipher or cryptographic method. Pupils have to discover the principle of a cipher and make a proposal of similar cipher. Several experiments with cryptographic software are also part of the curriculum. For example, pupils practice the idea of asymmetrical cryptography on PGP software, where the scheme of public and private key is simulated.

There are several projects such as "The Gate to Science Unlocked", where some scientific disciplines such as Cryptography are presented to high-school students in order to popularize the science field. In such project we taught the subject cryptography for high-school as well. At high-schools, we experiment with binding of the cryptography teaching with programming of cipher algorithms in light of previous method. The motivation of students increases when they can use their outputs, for example, for encryption of their e-mails. The students' programs follow the activities from primary school, from classical cryptography to algorithm DES. For modern cryptography the demonstration tools were used.

We have applied the education method where ontogeny recapitulates the history of Cryptography for

the course Introduction to Cryptography for CS undergraduates at our university as well. Instead of partial aids, we use the comprehensive educational program about cryptography and cryptanalysis CrypTool [8] to practice cryptographic issues. In comparison with primary and secondary schools, the mathematical background can be introduced in universities' courses.

4 Discussions

The course attracts pupils towards cryptographic issues and provides the opportunities to apply and evaluate knowledge and methods acquired in mathematics and informatics. The pupils understand the ideas of encryption methods, differences between different types of substitution cipher, and complex cryptographic systems; the continuity of various activities improved. On the other hand, phylogeny of the cryptography showed how the development of the ciphers extended over centuries whilst in school this is done over a very short period.

Similar area to Cryptography, where the idea of genetic epistemology could be applied, is steganography – science of hiding information. The history of steganography includes secret inks, hiding messages in wax tablets, hiding messages on messenger's body, hiding messages in pictures and texts, till modern steganographic digital techniques concealing messages within the lowest bits of noisy images or sound files for human eye/ear undetectable.

But the question of other CS subjects remains open. Cryptography is a discipline of Computer Science, Mathematics and (historically) Linguistic, where the history has been long. The history of many other CS disciplines is shorter.

On one hand there are CS subjects where applying the proposed method will be difficult or impossible, e.g. Multimedia or Programming. On the other hand, there are CS subjects where the application seems to be realistic, e.g. Artificial Intelligence and Neural Computing, Coding Theory, Networks or Computer Architecture. This question is suitable for further investigation and research.

However, in the current situation where the content of CS changes rapidly, the proposed method is of value both in theory and practice.

The last example, Fig. 1, demonstrates what inspired us to establish the Cryptography as a pilot topic of Computer Science in our project. Two eleven-year-old pupils used the exemplified disk in order to accelerate the encryption process between them. They preferred to encrypt messages to protect against the violation of their confidential communication by "enemy" during classes. The example shows the attraction as well as the capability of applying the subject Cryptography at primary schools.

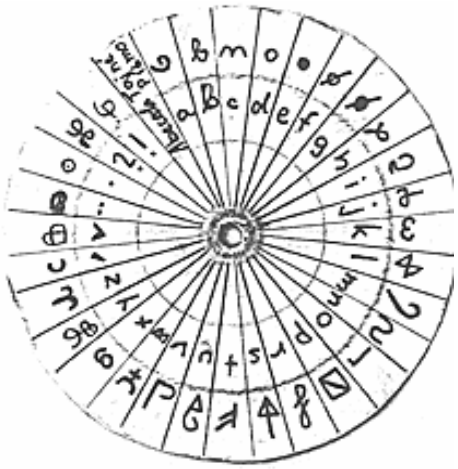


Fig.1: Pupils' cipher disk.

5 Preliminary Conclusions

Cryptography as a part of Information security becomes more important for everyday information technologies. How to provide high quality education in such a field is an important thing for all schools.

In this paper, we describe one way of Cryptography Education based on the theory that ontogeny of intellectual development might recapitulate historical evaluation of ideas. We have described the method requirements and have shown how the course content can be presented.

As this is a work in progress description, and the activities are made firstly, we can only draw some preliminary conclusions: (i) there is definitely great excitement of the kids participating in these activities, (ii) the activities increase pupils' understanding of the cryptographic topics, (iii) pupils were open for discussion about taught topics and to answer following questions: "things that you have learnt" and "thing that you want to know more about"; they were even approachable to spend their break for discussion, (iv) we had to reorganize several groups, which means that more care should be taken for selecting group members, (v) the groups came with different solution to the open ended problems (cipher proposals, methods for ciphering…), (vi) no one of pupils had problem to understand the "new" idea of asymmetrical cryptography after previous activities symmetrical cryptography.

As this activity is not yet finished, we can neither draw final conclusions nor publish research findings at this stage. On the other side, the preliminary results allow us to come to the following conclusion: teaching of CS with the following of historical structure can have positive results. Based on our positive experience, we

are planning on investigating and trying proposed method to use in other Computer Science subjects.

Acknowledgements: This work was supported in part by the Slovak Research and Development Agency under project APVV LPP-0028-06 "The Gate to Science Unlocked".

References:

[1] R. B. Vaughn, D. A. Dampier, and M. B. Warkentin. Building an information security education program. In *Proceedings of the 1st annual conference on Information security curriculum development*, pages 41–45, 2004.

[2] W. Hu, G. Wang, Q. Shi, and T. Chen. The practice of remote education on information security. In *The 9th International Conference for Young Computer Scientists*, pages 2609–2613, 2008.

[3] M. Hejný, G. Littler, L. Kvasz, and D. Peretz. Building structures in mathematical knowledge. In *CERME 4 European Research in Mathematics Education IV.*, pages 287–289. IQS FundEmi Business Institute, 2006.

[4] P. Caballero-Gil and C. Bruno-Castaneda. A cryptological way of teaching mathematics. *Teaching Mathematics and its Applications*, Vol. 26, No. 1., March 2007, pp. 2-16.

[5] M. Fellows and N. Koblitz. Combinatorially based cryptography for children (and adults),. *Congressus Numerantium*, 99:9–41, 1994.

[6] J. Piaget, *Genetic epistemology*. New York: W.W. Norton & Company, 1970.

[7] H. E. Gruber and K. Bödeker. *Creativity, Psychology and the History of Science*. Springer, Netherlands, 2005.

[8] Cryptool – educational tool for cryptography and cryptanalysis. http://www.cryptool.org.

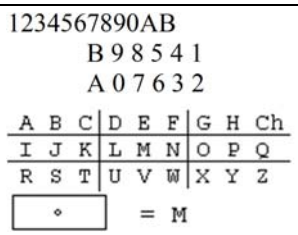
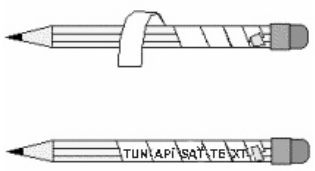
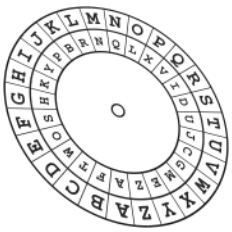
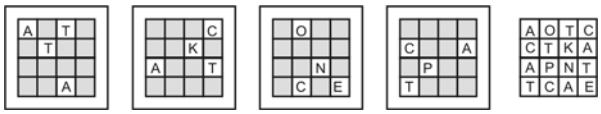
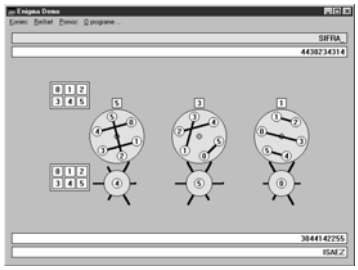
[9] D. Kahn. *The Codebreakers The Story of Secret Writing*, Scribner, New York, 1996.

[10] Huraj L., Siládi, V.: Cryptography and the teaching of informatics, In: *Valuing individual and shared learning*; IFIP WG 3.5 International Working Conference; Charles University, Prague, Czech Republic, June 2008, ISBN-13: 978-80-7290-353-5.

Table 1: Selection of phylogeny milestones – The phylogeny of Cryptography is presented by timeline of milestones. We mentioned not only phylogeny of cryptography, but also the phylogeny of cryptanalysis, because both disciplines are tightly bound [9].

Early stage	about 1900 BC	Egyptian scribe used some unusual hieroglyphic symbols
	600-500 BC	Hebrew scholars make use of simple monoalphabetic substitution ciphers (such as the Atbash cipher)
	600-500	The Greeks used a device called the "skytale" – first mechanical devices for encryption
	60-50 BC	Julius Caesar (100-44 BC) used a simple substitution with the normal alphabet.
	1401	Simeone de Crema in Mantua used homophonetic substitution.
	1466-1467	Leon Battista Alberti invented and published the first polyalphabetic cipher, designing a cipher disk to simplify the process.
	1553	Giovan Batista Belaso introduces the notion of using a key-phrase as the key for a repeated polyalphabetic cipher (called Vigenere cipher)
Mechanical and electronic cipher machines stage	1790	Thomas Jefferson, possibly aided by Dr. Robert Patterson invented his wheel cipher.
	1843	Edgar Alan Poe: Puzzle created by human ingenuity, human ingenuity can solve.
	1881	Fleissner grille – mechanical devices for transposition.
	1917	Gilbert S. Vernam invented a practical polyalphabetic cipher machine capable of using a key which is totally random and never repeats -- a one-time-tape. This is the only provably secure cipher, as far as we know.
	1919	Enigma Machine.
	1929	Hill polygram substitution cipher.
Computer stage	1970	Feistel networks.
	1976	Data Encryption Standard – DES.
From asymmetrical cryptology to present	1976	Whitfield Diffie and Martin Hellman published "New Directions in Cryptography", introducing the idea of public key cryptography.
	1977	RSA algorithm.
	1979	Secret sharing was invented by Shamir and Blakley.
	2000	Rijndael algorithm as the Advanced Encryption Standard.

Table 2: Selection of pupils' activities

Simple substitutions and transpositions pupils discover existing ciphers and develop their own ciphers	
Skytale principle of transposition – it is well demonstrated at a pencil	
Caesar Cipher (monoalphabetic substitution) activity, where the term Alphabetis used first time	
Cipher disk (polyalphabetic substitution) disk accelerate the ciphering process – the term Key is used first time	
Simple Fleissner grille transposition – insight to possible combination of a key space	
Enigma Machine (simulator) as machine with multiple disks	
Asymmetrical cryptography (polyalphabetic substitution)	For simulation of this topic the PGP software was used
Secret Sharing (Visual cryptography) This activity is possible to realize even without computer as we shown in [10.]