The Importance of the Using Software Tools for Learning Modern Cryptography

Article *in* International Journal of Engineering Education · January 2018

CITATIONS
2

READS
2,151

4 authors:

Saša Ž Adamović
Singidunum University
96 PUBLICATIONS **86** CITATIONS
SEE PROFILE

Marko Šarac
Singidunum University
50 PUBLICATIONS **99** CITATIONS
SEE PROFILE

Dušan Stamenković
Singidunum University
12 PUBLICATIONS **7** CITATIONS
SEE PROFILE

Dalibor Radovanovic
Singidunum University
28 PUBLICATIONS **48** CITATIONS
SEE PROFILE

International Journal of Engineering Education Vol. 34, No. 1, pp. 256–262, 2018
Printed in Great Britain

0949-149X/91 $3.00+0.00

The Importance of the Using Software Tools for Learning Modern Cryptography*

SASA ADAMOVIC, MARKO SARAC, DUSAN STAMENKOVIC and DALIBOR RADOVANOVIC
Department of Computer Science, Singidunum University, Belgrade, Serbia. E-mail: sadamovic@singidunum.ac.rs, msarac@singidunum.ac.rs, dstamenkovic@singidunum.ac.rs, dradovanovic@singidunum.ac.rs

Because of the wide application of cryptographic mechanisms in private and business environments, a cryptography course at many universities has the great importance today. An undergraduate cryptography course is mathematically demanding, and it is quite difficult for students with poor background to follow the course syllabus. This paper presents the use of interactive software in demonstrating basic cryptology principles in modern cryptography. The teaching methodology applied fosters students experimental work and engages students in discussions to resolve problems. The data are taken in three consecutive school years (around 150 participants), when we used to apply ordinary teaching practices, and when we switched to the interactive teaching approach. The assessment method was the attendance of students in the classroom, which has increased significantly during the semester. At the grade level of the student we noticed better grade distribution, with higher average grade.

Keywords: cryptography; educational software; interactive teaching

1. Introduction

As information security becomes more and more important, cryptographic mechanisms have become an indispensable component of every information system. Data and information stored in warehouses and passing through communication channels must be protected. The use of cryptographic mechanisms and protocols can solve many security problems (integrity, confidentiality, authenticity and non-repudiation of information). Although cryptography initially originated in the military, nowadays its use has widely expanded to different civil areas, such as Internet banking, electronic commerce, and social networks. Development of cryptographic technologies has a direct impact on economic, sociological and political aspects of the society in general. On the one hand, the ubiquitous cryptography usage today raises importance of a cryptography course at the university. On the other hand, cryptography instructors are faced with some of the following challenges in implementing the course syllabus.

1.1 Insufficient number of class hours

Cryptography is closely related to other sciences; it is an intersection of mathematics, communications, computer science, and data processing. Thus, the fundamentals of cryptography lie deep in applied number theory and abstract algebra. The main application of cryptography is protection of computer networks. Besides different mathematical background, students have different academic interests. These circumstances are quite difficult to overcome in 48 hours, which is the typical duration of one-semester cryptography course.

1.2 Students poor mathematical background

To be able to study the cryptographic systems, students are expected to have strong mathematical knowledge, especially in disciplines such as number theory, abstract algebra, probability and statistics. Also, understanding the basics of computer networks is a necessary prerequisite. For example, a student not taking a course in discrete mathematics will not understand Euler's theorem, which will subsequently cause problems with understanding the RSA algorithm and Advanced Encryption Standard (AES).

1.3 Lack of student's experimental work

Although almost all universities have modern electronic laboratories with networked computers and Internet access, teaching practices in a cryptography course at many universities do not include experimentation. This lack of practical application of cryptography is the main reason for students lack of interest in doing the course work. This paper describes one possible approach to increase students interest in a cryptography course and presents methods which are completely flexible and allow for different approaches to teaching.

2. Related work

Cryptography is a discipline with strong mathematical basis because the security of a cryptosystem is often based on the inability to efficiently solve a

* Accepted 26 August 2017.

problem in algebra, number theory, or combinatorics. Since many students have found cryptography to be a hard-to-master topic, many instructors have made attempts to adapt their teaching methods to be flexible enough. For example, one such approach to get students interested in the topic is described by authors [1, 2] analyze 20 selected academic courses in cryptology with respect to their aim, scope, content, organization, and literature recommended to students, finally proposing the curricula tailored for different categories of students. In closely related paper authors [3, 4] propose a ''theory-algorithm-practice-application'' teaching mode, which has proved to be efficient in achieving better teaching results and in helping students to solve practical cryptography problems encountered in the engineering. Authors [5–7] used different concepts for learning cryptography and algorithms with the help of interactive animations. In this way, significantly better results were achieved in understanding the concept of cryptographic algorithms. Authors [8] various concepts in the cryptographic domain and the relations among them as the ontology, and propose a way of utilizing it in the learning process. Should be remembered that learning domain is cryptography in network security.

3. Interactive cryptography

Students evaluations of our beginning cryptography course have clearly shown that the plain textbook-theoretical approach to teaching cryptography that we used to apply simply was not satisfactory. That's why we subsequently decided to shift to interactive approach by introducing the open-source cryptography software CrypTool 2.0. The course makeover required substantial instructor and teaching assistant efforts, especially when choosing the right examples to illustrate the most commonly used cryptography algorithms and protocols. This section describes our teaching experience and analyzes students results which confirm that teaching cryptography interactively, through practical demonstrations, is indeed advantageous.

3.1 The interactive course methodology

Our cryptography curriculum mainly follows and focuses on cryptographic principles, procedures, mechanisms, and techniques required for secure communications. The beginning one-semester undergraduate cryptography course is designed to introduce students to the basics of cryptography. Within the course time frame, the topics to be covered in the class include modern ciphers, block and flow codes, public key cryptography, key management and distribution, hash functions, digital signature generation, certification and verification, as well as certain cryptographic techniques. Fig. 1 shows the building blocks of the course.

Students enrolled in the course come with different background and face a severe learning difficulty which directly lowers their interest for the course. For that reason, the main idea was to increase students interest for cryptography by using interactive software that is easy to understand. An additional goal was also to try to create an atmosphere in which students better understand theory and at the same time improve their ability to analyze and solve problems. In summary, the new implementation of the course syllabus was to emphasize understanding of the principles of information security, cryptographic algorithms, and security services (authentication, authorization, confidentiality, non-repudiation and availability), as well as to provide practical examples which integrate theory with practice.

There are not many simulation environments for learning cryptography that allows students to develop complex scenarios. For example, the implementation of various security protocols in a real network environment, in which more student computers can participate in the same simulation. Such functionality is provided to network components specially developed in a development environment that allow the exchange of different types of data and network synchronization. Most environments only demonstrate the use of certain cryptographic algorithms. For example, users select the encryption algorithm, then select the key and enter the message they want to encrypt, and after that they get an encrypted message as a result. Such tools are not useful enough if students want to understand complex cryptographic scenarios or scenarios for cryptanalysis more deeply. The most well-known cryptographic environments that besides the development of more complex scenarios allow for visualization are GRASP tool [9] and Cryptool 2 [1], and besides them there is Grace tool [10], Kerberos tool [11] (visualizing Kerberos protocol) and Game tool

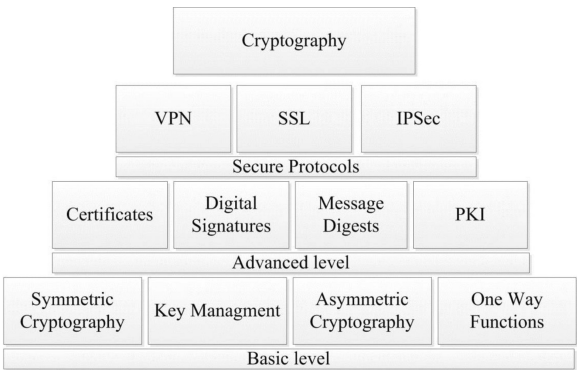

Fig. 1. Building blocks of our cryptography course.

[12]. In addition to these tools, there is one more Cryptol industrial tool [13]. Cryptol has been used by private companies, educators, and the U.S. Government. Cryptol was originally designed for expressing the kinds of cryptographic algorithms that can be efficiently implemented in hardware circuits.

For this purpose, we have chosen CrypTool, a free open-source learning application used worldwide for the implementation and analysis of cryptographic algorithms. The CrypTool laboratory offers easy visualization of key concepts in addition to fundamental data structures and cryptographic methods. It includes all modern algorithms and protocols for encryption, as well as several crypto-analytical methods, which can be used for studying cryptography in the same user-friendly environment. Available methods include both classic and modern encryption systems:

- Caesar, ADFGVX, double-column transposition, and Enigma;
- RSA and AES algorithms, hybrid algorithms for encryption, and encryption algorithms based on lattice reduction and elliptical curves;

The CrypTool laboratory is advanced enough to allow students to use all available algorithms to model a cryptography system or to simulate a variety of cryptanalysis methods. The laboratory uses algorithms recommended by NIST (National Institute of Standards and Technology) standards.

This environment is also giving students an opportunity to exercise different types of cryptographic scenarios an algorithm. Some of them from modern cryptography:

Symmetric and Asymmetric:

- AES, DES, TDES, RC4, TEA, Block modes of symmetric ciphers
- RSA cipher (encryption/decryption), RSA key generator

Protocols:

- Authentication protocols (symmetric and asymmetric) over network
- Diffie-Hellman and RSA key exchange over network
- BB84 key exchange, Zero knowledge protocol

Cryptoanalysis:

- AES analysis using Entropy, DES known-plaintext analysis
- WEP attack, Key searcher, Factorizer

Hash functions:

- CRC, HMAC, MD5, MD5 collider
- SHA-1, SHA-256, Tiger, Whirlpool, PKCS#5

The next two examples illustrate the use of CrypTool and show cryptographic models that were developed by students during lab sessions in our cryptography course.

Example 1: The RSA key generation/encryption

Fig. 2 shows an RSA key generation/encryption model based on the original algorithms approved by NIST. Parameters for the RSA public-key encryption algorithm used in the example are as follows:

- Choose $p = 11$ and $q = 3$, two ''large'' prime numbers,
- Compute $N = pq = 33$ and $(p-1)(q-1) = 20$,
- Select $e = 3$ which is relatively prime to $(p-1)(q-1) = 20$,
- Find d such that $ed = 1 \bmod 20$, which gives $d = 7$,
- Public key: $(N, e) = (33, 3)$, Private key: $(d = 7)$,
- Encrypted message: $C = M^e \bmod N$, Deciphered message: $M = C^e \bmod N$;

Example 2: The DES algorithm

Fig. 3 shows a model of the cryptographic system based on the DES algorithm with CBC mode and block mode for updating PKCS #7. Prior to simulating a cryptographic system in CrypTool, it is necessary to have a theoretically possible model of the system. The construction of a model begins with dragging objects to the workspace. Each object has input and output connectors, which support communication between mutually compatible objects. In case of the DES algorithm, the input connectors are the points where the arguments (plaintext, key, initial vector) are added to the algorithm. Output connector is the point which displays the results of algorithm (DES ciphertext). Clicking on any of the objects allows for choosing option properties, where additional parameters can be configured (for example, the mode of the algorithm).

4. Assessment

The traditional way to measure student's outcome in a cryptography course includes multiple-choice questions, essays, class attendance, and a written final exam. The interactive educational software changes this traditional approach by introducing practical exams. CrypTool allows instructors to construct problems to be solved by students using the same software. Additionally, based on work in [14], we have used the concept of a task to assign problems to the student's step by step. A task has three or more levels, depending on the number of topics covered. If the student does not solve the first-level problem, the student cannot proceed to the next level (or skip a level). Only when a student

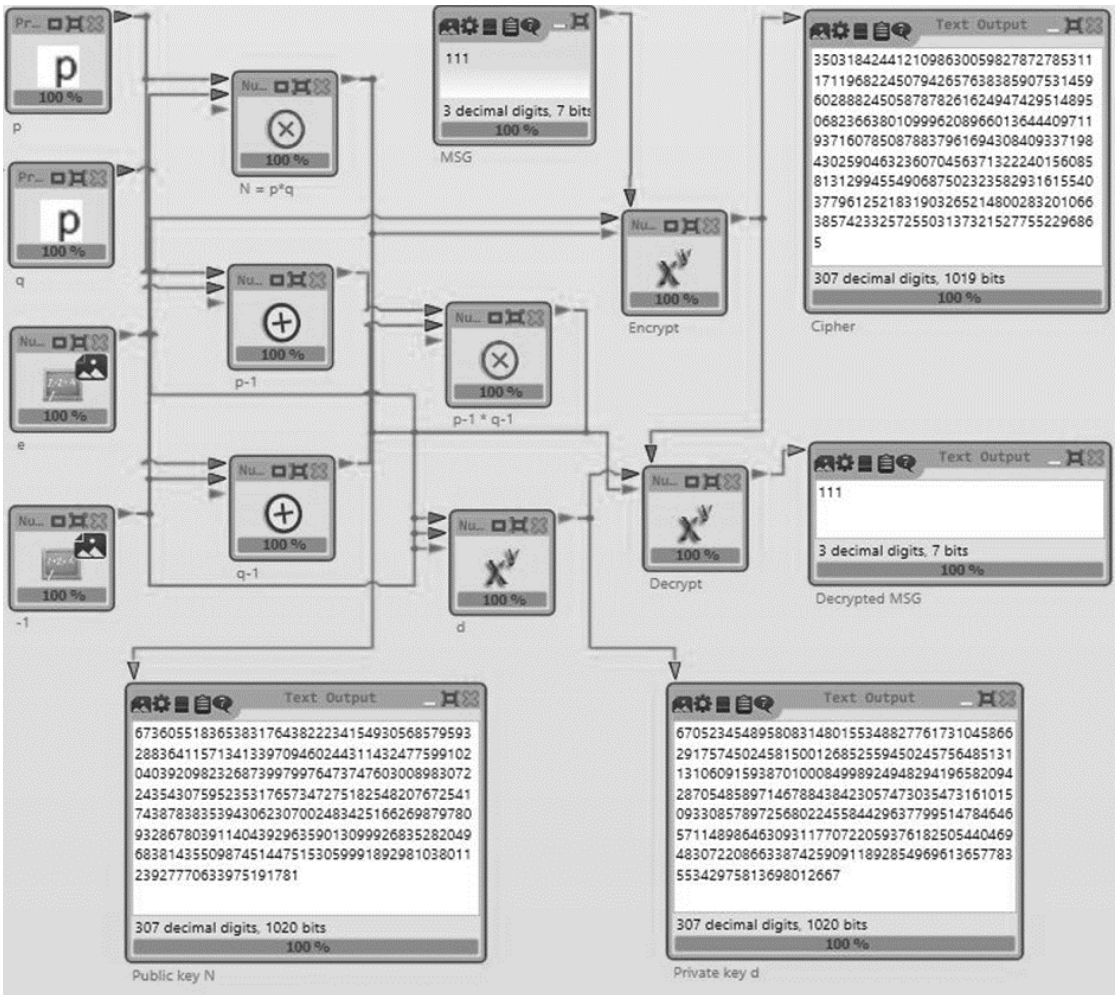

Fig. 2. CrypTool example of the RSA key generation and encryption.

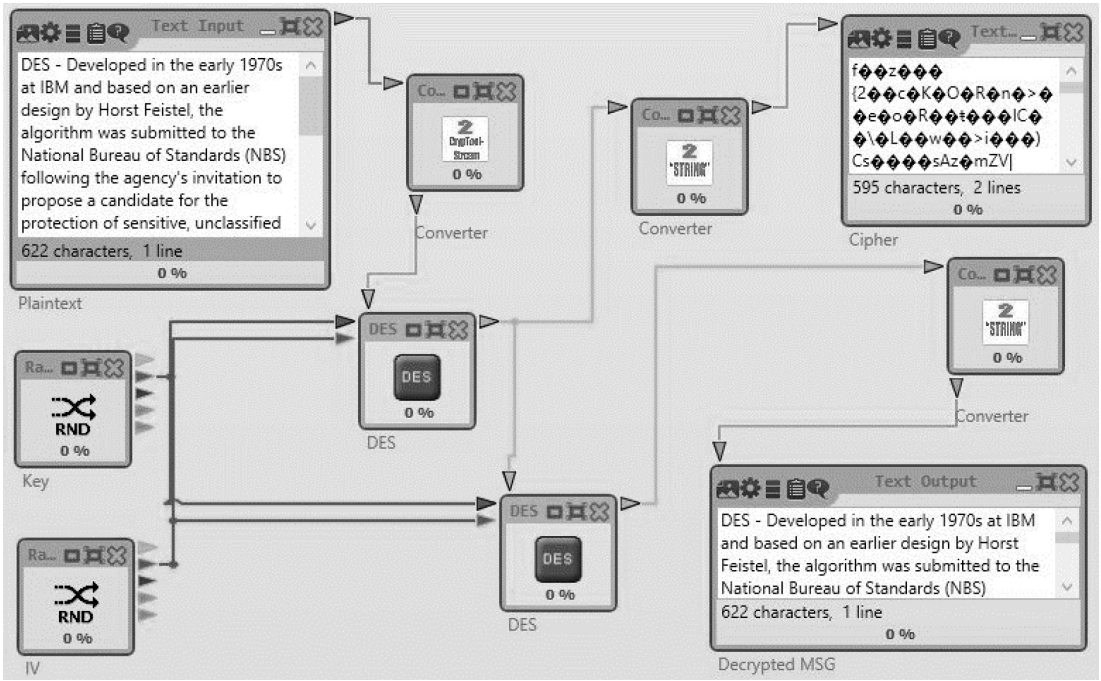

Fig. 3. CrypTool example of the DES encryption algorithm.

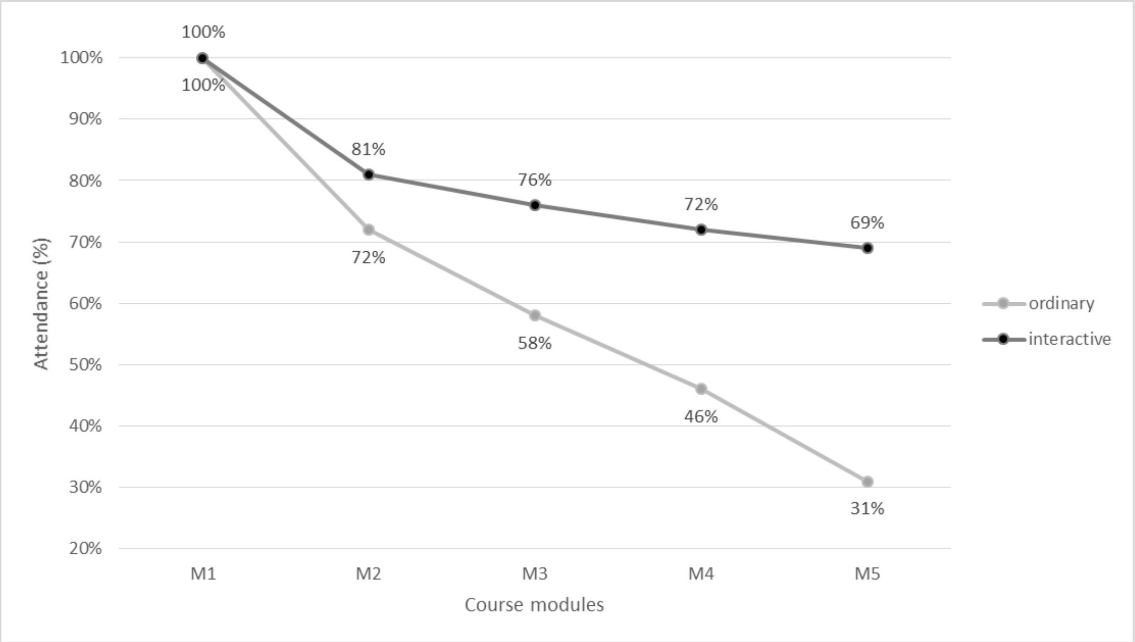

Fig. 4. Students attendance before and after using interactive approach to the course.

successfully switches to another level, he is introduced to the problem for that level.

The idea of a task is inspired by computer games [15] and is used to further engage students in the course. For example, a task consists of a file with basic instructions to students (type of algorithm, key length, standards applied) to solve a problem and another file with encrypted contents. If the student correctly creates a cryptographic system in CrypTool, the result will be plaintext with instructions required to solve the next level problem. Before using the CrypTool interactive laboratory to illustrate complex mathematical operations, students with poor mathematical background were not able to fully understand even the basic encryption principles, for example the DES algorithm and the RSA public-key system. The non-interactive approach proved to have negative impact on the interest of students for the course and their final grades.

CrypTool allows instructors to construct real time labs with appropriate customizations. Students are able to follow every cryptographic function step by step. More importantly, students can easily and quickly implement their ideas by dragging objects from the toolbar that contains algorithms and can run simulations in real time. Students over time gain practical experience which not only raises their interest for cryptography in general, but has also a positive effect to feel comfortable in presenting their work and commenting on other student's work. The discussion encourages students to open-mindedness, which further arouses their enthusiasm in learning cryptography. To quantitatively assess the new interactive approach, we have conducted a survey to compare two aspects of our cryptography course: the students interest and their final grades in the course. The data are taken in three consecutive school years, when we used to apply ordinary teaching practices, and when we switched to the interactive approach.

Fig. 4 reports an increase of student's interest, measured by way of their classroom attendance, for each module of our cryptography course. Percentages of the student's attendance increase on y-axis are given depending on the course modules M1, M2, M3, M4, and M5 on the x-axis of the graph. The module M1 comprises the following topics: history, monoalphabetical ciphers, and Caesar cipher; M2 comprises symmetric cryptography, asymmetric cryptography, one way functions, and key management; M3 comprises certificates, digital signatures, message digests, and PKI; M4 comprises VPN, secure email, SSL, and IPSec; M5 comprises practical cryptography and cryptographic protocols.

The next Fig. 5 shows also an increase of the final grades of students. The passing grade range used in the graph is 6 to 10, where the numeric grade 10 corresponds to the "excellent" grade, 8 to "good", and 6 to "fair". As the bar chart in Fig. 5 clearly demonstrates, the student grades have been improved with the new interactive approach. Building on previous experience and by applying some new ideas, we hope to further increase student's involvement and learning outcome in the years that follow.

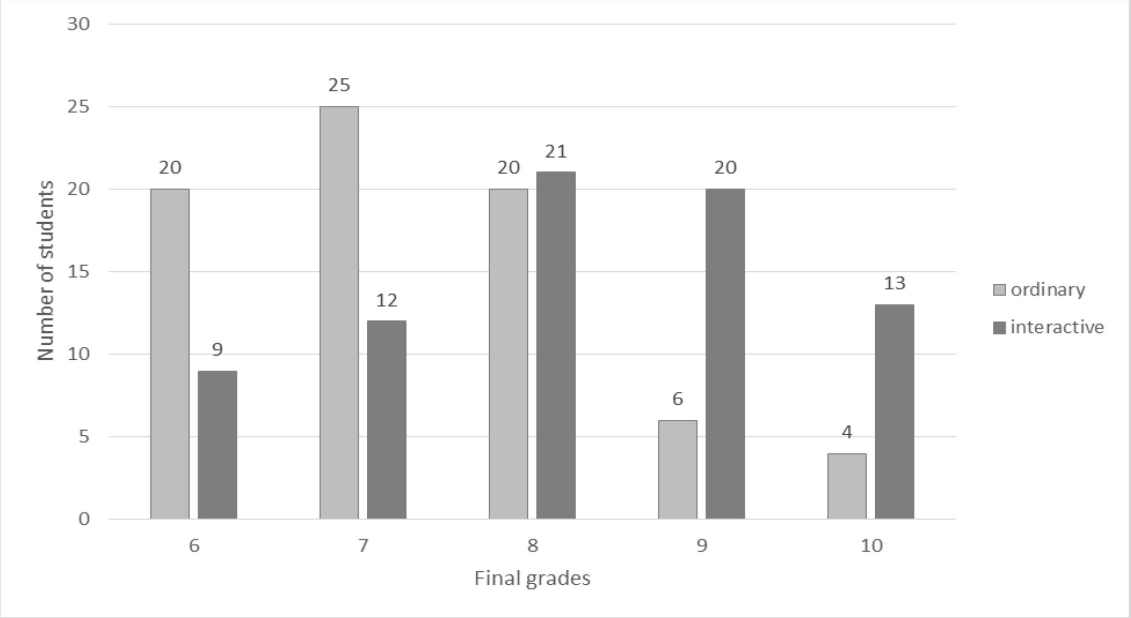

Fig. 5. Students grades before and after using interactive approach in the course.

4.1 Discussions

Cryptool 2 is originally developed for interactive visualization of cryptographic algorithms. It allows designing complex cryptographic scenarios. In addition to the standard components with which it is possible to model the cryptographic protocol, there are network components that allow interactive simulation between two or more computers in the network [1]. In this way, in addition to cryptographic protocols, students can get better acquainted with different scenarios of Man-in-the-middle attack. Professors can also create video tutorials that can be useful for student self-supporting work.

Cryptool does not allow full implementation of modern cryptographic protocols (SSL, IpSec) due to the complexity beyond the capabilities of the environment, but allows the implementation of an abstract protocol scheme for a limited number of parameters and a simulation in a network environment.

5. Conclusions

This paper describes the use of an interactive educational environment for learning cryptology. With use of the CrypTool software tools, provided is an adequate level of abstraction to a more efficient way of learning cryptology rules and principles necessary for the development of modern cryptographic mechanisms. Students are directly aimed at understanding the complex crypto system and practical scenarios that have been identified in their application and implementation. A comparative analysis of student results was observed with significant positive effects indicating the very good quality of the applied educational models in order to successfully overcome the present syllabus of cryptography. The presence of students in the classroom has increased significantly during the semester, as opposed to the traditional way where the number of students rapidly decreases as the material becomes more complex and mathematically demanding. With the increased activity of students in classes, the final estimates tests are significantly better. Student also expressed further interest in the area, and were willing to research cryptography in post-graduate studies.

Acknowledgments—The Department for Informatics and Computing at Singidunum University in Serbia has contributed plugins for network based communication between remote CrypTool 2 environments (https://www.cryptool.org/en/ctp-team-en). These plugins are the result of many years of successful usage of CrypTool for teaching cryptology. The authors gratefully acknowledge support from Ministry of Science and Technological Development of the Republic of Serbia through the project TR32054.

References

1. S. Adamović, M. Šarac, M. Veinović, M. Milosavljević and A. Jevremović, An Interactive and Collaborative Approach to Teaching Cryptology, *Journal of Educational Technology & Society*, **17**(1), 2014, pp. 197–205.
2. V. Uskov and B. Sekar, Gamification of software engineering curriculum, *Proceedings of the Frontiers in Education Conference (FIE)*, Madrid (Spain), 2014, pp. 1–8.
3. D. Olejar and M. Stanek, Some Aspects of Cryptology Teaching, *Proceedings of the WISE1—IFIP WG 11.8 1st World Conference on Information Security Education*, Stockholm (Sweden), 1999, pp. 1–9.
4. X. Song and H. Deng, Taking Flexible and Diverse Approaches to Get Undergraduate Students Interested in

Cryptography Course, *Proceedings of the First International Workshop on Education Technology and Computer Science*, Wuhan (China), 2009, pp. 490–494.
5. C. Kehoe, J. Stasko and A. Taylor, Rethinking the evaluation of algorithm animations as learning aids: an observational study, *International Journal of Human Computer Studies*, **54**, 2001, pp. 265–284.
6. X. Yuan, P. Vega, Y. Qadah, R. Archer, H. Yu and J. Xu, Visualization Tools for Teaching Computer Security, *ACM Transactions on Computing Education*, **9**, 2010, pp. 147–155.
7. C. D. Hundhausen, S. A. Douglas and A. T. Stasko, A meta-study of algorithm visualization effectiveness, *Journal of Visual Languages and Computing*, **13**, 2002, pp. 259–290.
8. Y. Takahashi, T. Abiko, E. Negishi and G. Itabash, An ontology-based e-learning system for network security, *Proceedings of the 19th International Conference on Advanced Information Networking and Applications (AINA)*, Taipei (Taiwan), 2005, pp. 197–202.
9. D. Schweitzer, L. Baird, M. Collins, W. Brown and M. Sherman, GRASP: a visualization tool for teaching security protocols, In the *Tenth Colloquium for Information Systems Security Education*, Adelphi, MD, 2006, pp. 1–7.
10. G. Cattaneo, A. D. Santis and U. F. Petrillo, Visualization of cryptographic protocols with GRACE, *Journal of Visual Languages and Computing*, **19**, 2008, pp. 258–290.
11. X. Yuan, Y. Qadah, J. Xu, H. Yu, R. Archer and B. Chu, An animated learning tool for Kerberos authentication architecture, *Journal of Computing Sciences in Colleges, The Twelfth Annual CCSC Northeastern Conference*, **22**, 2007, pp. 147–155.
12. L. G. C. Hamey, Teaching Secure Communication Protocols Using a Game Representation, In *Australasian Computing Education Conference* (ACE2003), Adelaide, Australia, 2003, pp. 187–196.
13. S. Browning and P. Weaver, Designing Tunable, Verifiable Cryptographic Hardware Using Cryptol. In *Design and Verification of Microprocessor Systems for High-Assurance*, 2010, pp. 89–143.
14. B. Woolf, *Building Intelligent Interactive Tutors: Student-centered strategies for revolutionizing e-learning* (1st Edition), Morgan Kaufmann, 2008.
15. F. Yang, C. Zhong, M. Yin and Y. Huang, Teaching Cryptology Course Based on Theory-Algorithm-Practice-Application Mode, *Proceedings of the First International Workshop on Education Technology and Computer Science*, Wuhan (China), 2009, pp. 468–470.

Sasa Adamovic, PhD is an assistant professor at Singidunum University. His areas of expertise are: Computer Security, Cryptology, Biometrics, Crypto Biometrics, Theory Information and Coding and Digital Forensics. He is certified in administration and database field by many major IT companies such as Google, SAP, IBM, HP and Oracle.

Marko Sarac, PhD is an assistant professor at Singidunum University. His areas of expertise are: Informatics and computing, Electrical engineering and computing, E-Business, Internet marketing and advertising. He is Head of IT department on Singidunum University from November of 2006. He is certified in administration and database field by many major IT companies such as Google, Cisco, SAP, IBM, HP, Solidworks, Oracle.

Dusan Stamenkovic, MSc is teaching assistant at Singidunum University. His areas of expertise are: Computer Networks, Computer Security, Security in Computer Networks and Cybersecurity. He also works as a Senior System Engineer in IT department and he is certified in administration by many major IT companies such as Microsoft, Cisco, Palo Alto Networks, MikroTik, SAP, Oracle and IBM.

Dalibor Radovanovic, PhD is a teaching assistant at Singidunum University from October of 2008. His areas of expertise are: Informatics and Computing, Design of Information Systems, Business Information Systems, Databases, E-Business, Internet marketing and advertising. He is certified in administration and database field by many major IT companies such as Microsoft, Cisco, SAP, IBM and Oracle.