Teaching interactive cryptography: the case for CrypTool

Saša Adamović[1], Irina Branović[2], Dejan Živković[3], Violeta Tomašević[4], Milan Milosavljević[5]

***Abstract* – The theory and applications of cryptography are complicated and hard to follow for undergraduate students with less mathematical background. For this reason, instead of plain theoretical teaching, we applied different, interactive approach. Open-source CrypTool software allowed us to practically demonstrate all current private and public-key algorithms and protocols. This paper describes our teaching model and experience. Positive feedback received from students confirms the advantages of adopted approach with respect to traditional teaching.**

***Keywords* – education, cryptography, interactive teaching, CrypTool**

I. INTRODUCTION

Cryptography course as part of computer science curriculum has become a necessity, considering that it nowadays serves as the basis for data communication security, information and network security. For today's computer professionals, secure data storage and communication have become vital competencies, unlike before when cryptography was considered to be a secret science. However, since it is directly based on diverse mathematical disciplines (number theory, abstract algebra, probability), students with less mathematical background are often intimidated and could benefit from teaching through practical examples.

Analyzing the results achieved and students' feedback, we noticed that the plain textbook-theoretical approach to teaching cryptography that we used to apply simply was not satisfactory, and subsequently decided to shift to interactive approach by introducing the open-source cryptography software CrypTool [4]. 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. In this paper we describe the teaching experiences and analyze students' results which confirm that teaching cryptography interactive, through practical demonstrations, is indeed advantageous.

[1]Saša Adamović is with the Singidunum University, Danijelova 32, 11000 Beograd, Serbia, E-mail: sadamovic@singidunum.ac.rs.

[2]Irina Branović is with the Singidunum University, Danijelova 32, 11000 Beograd, Serbia, E-mail: ibranovic@singidunum.ac.rs.

[3]Dejan Živković is with the Singidunum University, Danijelova 32, 11000 Beograd, Serbia, E-mail: dzivkovic@singidunum.ac.rs.

[4]Violeta Tomašević is with the Singidunum University, Danijelova 32, 11000 Beograd, Serbia, E-mail: vitomasevic@singidunum.ac.rs.

[5]Milan Milosavljević is with the Singidunum University, Danijelova 32, 11000 Beograd, Serbia, E-mail: mmilosavljevic@singidunum.ac.rs.

II. RELATED WORK

It is well known that cryptography is a hard-to-master discipline, which requires strong mathematical background because the security of a cryptosystem is often based on the inability to efficiently solve a problem in algebra, number theory, or combinatorics. Many instructors have made attempts to adapt their teaching methods to be flexible and to get students interested in the topic; one such approach is described in [1]. In [2], authors analyze 20 selected academic courses in cryptology with respect to their aims, scopes, contents, organization, and literature recommended to students, finally proposing the curricula tailored for different categories of students. In closely related [3], authors propose a "theory-algorithm-practice-application" teaching mode, which has proved to be efficient in achieving better teaching results, and helping students solve practical problems encountered in the engineering practice by using cryptography.

III. INTERACTIVE CRYPTOGRAPHY

Our cryptography course curriculum mainly follows [5] and focuses on cryptographic principles, procedures, mechanisms, and techniques required for secure communications. Fig. 1 shows the building blocks of the course.

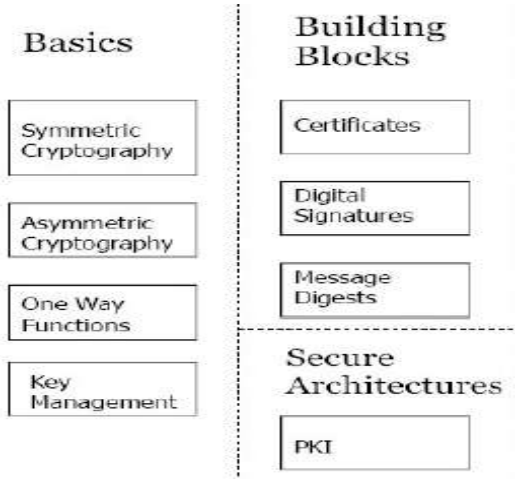

Fig. 1. Building blocks of the course

When implementing the course curriculum for the 2010 school year, our primary goal was to put emphasis on understanding the basics of information security, protection of cryptographic algorithms, and security services (authentication, authorization, confidentiality, non-repudiation and availability), as well as to provide practical examples which integrate theory with practice. For this purpose we have chosen CrypTool, a free, open-source learning application, used worldwide in the implementation and analysis of cryptographic algorithms. From its graphical interface, CrypTool offers numerous interactive demonstrations and visualizations of classic and modern cryptographic algorithms, generation of the secure passwords, authentication, cryptanalysis, and encryption.

Fig. 2 shows an RSA key generation/encryption simulation based on the original algorithms approved by NIST. The simulation was developed by students during laboratory exercises.

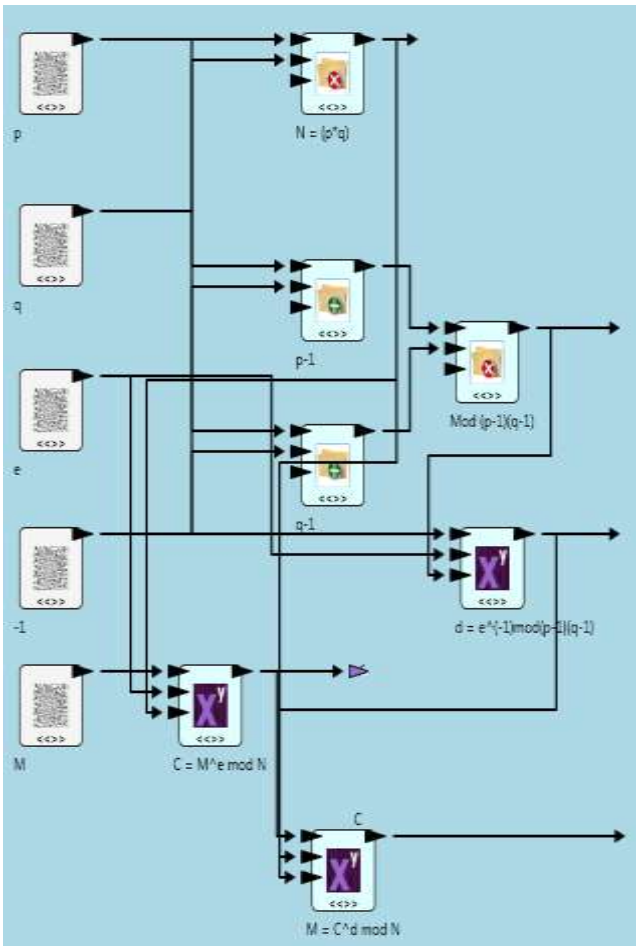

Fig. 2. An example of interactive CrypTool screen illustrating RSA key generation and encryption.

Before using interactive laboratory for complex mathematical operations, students with poor mathematical background were not able to view the simulation in a controlled interactive way. Namely, without CrypTool teacher could only show students the functionality of several commercial programs related to the basic cryptography principles that need to be respected in the construction of a cryptographic solution. This approach has a negative impact on the interest of students for the course and their final success.

Using CrypTool we have got the lab that works in real time with real parameters. Students have been now able to follow every cryptographic system step by step. More important, students can easily and quickly implement their ideas by dragging objects from the palette that contains algorithms and run the simulation in real time. This way students over time could get more experimental experience that not only creates more interest among them for the cryptography overall, but is also positively reflected on their final success.

IV. Analysis of Teaching Results

For the sake of comparison, Fig. 3 shows the student's attendance and grades for the 2008 and 2009 school year in the cryptography course without CrypTool, as well as for the 2010 school year when we started using interactive approach in the course.

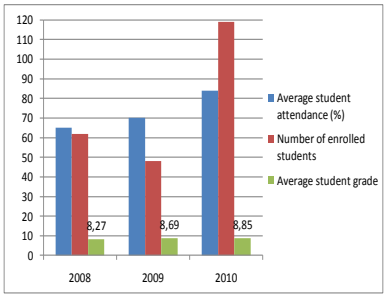

Fig. 3. Students' attendance and grades before and after using interactive approach in the course.

As the diagram clearly demonstrates, student attendance jumped well over 10%, and students grade also slightly improved. With some new ideas and building on previous experience, in the years that follow we hope to further increase students' involvement and learning outcome.

V. Conclusion

In order to combine theory and practice in teaching cryptography, this paper advocates using CrypTool as a powerful instructional tool. Interactive CrypTool software makes up for the students' lack of strong mathematical background and demonstrates inner workings of cryptography algorithms in a user-friendly way. The effectiveness of CrypTool is confirmed by a comparative analysis of students'

attendance and grades, which clearly justifies its use in a cryptography course.

ACKNOWLEDGEMENT

This work has been supported by the Serbian Ministry of Education and Science, projects no. 44006 and 32054.

REFERENCES

[1] X. Song, 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, 2009.

[2] Olejar, D., and Stanek, M., "Some Aspects of Cryptology Teaching", Proceedings of the First World Conference on Information Security Education WISE1, 1999.

[3] Y. F. Zhong, C. Y. MengXiao, H. YiRan, "Teaching Cryptology Course Based on Theory-Algorithm-Practice-Application Mode", Proceedings of the First International Workshop on Education Technology and Computer Science, 2009.

[4] CrypTool, available online at http://www.cryptool.com/

[5] W. Stallings, *Cryptography and Network Security*, Fourth Edition, Prentice-Hall.