An intelligent PBL-based tutoring system for cryptology domain

Aleksandar Jevremovic, Sasa Adamovic, Goran Shimic, Marko Sarac, Mladen Veinovic, Milan Milosavljevic

***Abstract*— Teaching cryptology represents one of the most challenging tasks in contemporary engineering education. Apart from setting high requirement for students (i.e. required mathematical knowledge and skills), teachers are also required to invest a lot in each individual student. In the previous paper on this subject matter we presented a CrypTool extension that enables the interconnection of different simulation environments. In this paper, we present an intelligent, problem based learning based tutoring system that is built upon that extension. The system is capable of generating different (level) problems from cryptology domain, developing adequate solutions, evaluating students' solutions and reffering them to appropriate studying materials.**

***Index Terms*— problem based learning, intelligent tutoring systems, cryptology.**

I. Introduction

TEACHING cryptology represents one of the most challenging tasks in contemporary engineering education. Apart from setting high requirement for students (i.e. required mathematical knowledge and skills), teachers are also required to invest a lot in each individual student.

In the previous paper on this subject matter, we presented a CrypTool extension that enables the interconnection of different simulation environments. We used that extension to create collaborative and interactive learning environment - to enable students to work together in order to solve complex cryptology problems, by using highly abstracted graphical user environment. This approach enabled students to work with the different cryptology models without forcing them to learn complex mathematical foundations at first.

In this paper [1], we present an intelligent, problem based learning based tutoring system that is built upon that extension. The system is capable of generating different (level) problems from cryptology domain, developing adequate solutions, evaluating students' solutions and referring them to appropriate studying materials. The system is developed as a Web application, but is using socket programming for communication with CrypTool environment (which is still used as the main environment for problem solving)..

Aleksandar Jevremovic is with the Singidunum University, Danijelova 32, Belgrade, Serbia (e-mail: ajevremovic@singidunum.ac.rs).

Sasa Adamovic is with the Singidunum University, Danijelova 32, Belgrade, Serbia (e-mail: ajevremovic@singidunum.ac.rs)

Goran Shimic is with the Military Academy, Pavla Jurisica Sturma, Belgrade, Serbia (e-mail: gshimic@gmail.com)

Marko Sarac is with the Singidunum University, Danijelova 32, Belgrade, Serbia (e-mail: msarac@singidunum.ac.rs)

Mladen Veinovic is with the Singidunum University, Danijelova 32, Belgrade, Serbia (e-mail: mveinovic@singidunum.ac.rs)

Milan Milosavljevic is with the Singidunum University, Danijelova 32, Belgrade, Serbia (e-mail: mmilosavljevic@singidunum.ac.rs)

II. PBL in Cryptography

Today the Web is suffering from lots of different kinds of security problems. Contemporary applications depend on powerful technologies and offer various services to the users, but often lack of measures to protect themselves of malicious ones. Therefore, research and education in IT security area is getting more attention than before. As cyber-attacks are getting more complex, the personnel responsible for implementing protection have to be better educated and higher skilled. Residential courses are place and time limited, expensive and hardly affordable for the students.

Problem-based learning (PBL) as a pedagogical approach provides a high level of student engagement during a learning process. Solving problems of different types and difficulty reflects many characteristics of the student's profile. Besides his knowledge and skills, there are others, such as attention, persistence, creativity and resourcefulness [2,3,4] . Problem-based learning in cryptography means the student has to manage new complex and security-sensitive tasks in order to provide safety communication link between users. Fortunately, there are few simulation systems and applications that provide testing of different solutions in safety environments in which students' mistakes cannot do damage to the real systems.

The most of them categorized as Intelligent Tutoring Systems (ITS). They can be split into two groups: focused on practical skills and theoretical fundamentals. First group comprises learning concrete applications and systems. For instance, Tele-Lab IT Security represents a learner-centered ITS that deliver learning content according to the learner profile (ordinary users, IT students and administrators) [5]. It runs separate virtual machines for each user enabling them to use system resources in performing particular tasks (e.g. email manipulation, OS and disk management, etc.).

ITSs focused on theory deal with understanding and knowing how different encryption algorithms work. For instance, DES Tutor is an ITS narrowly specialized for learning DES algorithm [6]. Another example is InfoSec Tutor (also referred as Crypto Tutor) – ITS offers learning of encryption algorithms of different types. Moreover, it applies advanced pedagogical techniques such as learning by examples, case studies, analysis and comparison of cipher text produced by different algorithms [7].

Apart of ITSs mentioned above, there are hybrid solutions that combine theory and practice. They are not belonging to ITS family because they have neither learner models, nor implemented didactics. Nevertheless, they represent powerful solutions for blended learning combining individual work in class learning with collaboration possibilities. Crypt Tool represents one of such solutions[8].

Therefore, we present one case study in this article: Cryptology PBL. The application is developed as an additional module for the Learning Management System (LMS). This way the LMS is extended by PBL functionality and the LMS learning resources can be used in PBL..

III. CRYPTOOL

CrypTool is an open-source software for learning cryptology. Today, after 19 years of development, this software is used by numerous schools, universities and companies. The main advantage of this software is that it doesn't require learners to have a strong understanding of complex mathematical principles and formulae.

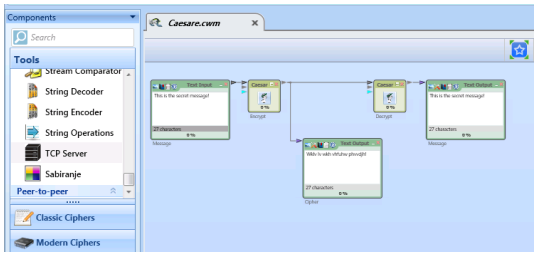

Fig. 1 - CrypTool learning environment

Having a simple graphical interface, CrypTool enables learner to create and test complex cryptological models just by adding, connecting and configuring blocks (that represent cryptographic functions and algorithms, like DES, AES, MD5, etc.).

IV. NETWORK COMMUNICATION AND COLLABORATION

One of the main shortcomings of Cryptool environment was the lack of networking capabilities, which limited it on single-user learning scenarios. However, our team at the Department of informatics and computing at Singidunum University, in 2012. developed an extension that enabled connecting multiple CrypTool environments by using a TCP/IP based network. This extension is based on two components - TCP Client and TCP Sever. Intended use of those components was to easily transport some information (i.e. encrypted message) from one CrypTool environment to another.

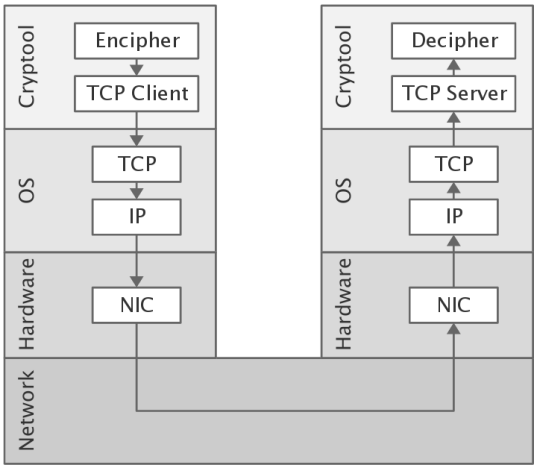

Fig 2. - Network communication between remote CrypTool environments

The aforementioned extension provided us with ability to engage our students with more complex cryptology tasks, and to create a collaborative environment. However, the problem of creating those tasks left. Also, even if students were able to help each other, main part of guiding them and evaluating their work remained for teachers. That's why we started our work on automatizing those tasks, which resulted in an intelligent PBL-based tutoring system that we present in this paper.

V. SOLUTION MODEL

The system presented in this paper is based on two main components - CrypTool environment and Web application. CrypTool environment is already described (both built-in functions, as well as the component for network communication) as a standalone solution. Within this system CrypTool is communicating with the Web application by using standard TCP communication (Fig 3.). This is a two-way communication - CrypTool is able to read some data (i.e. encrypted message) from server, as well to send back some data (usually a solution).

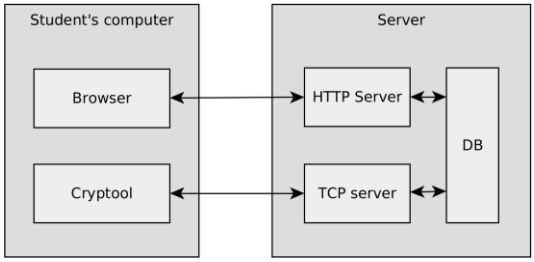

Fig 3. - Communication between student's client and server

On the server site, the system is based on regular HTTP server (Apache Tomcat) with a JSP application. That application is responsible for registering student's attempts, displaying problem description, evaluating student's solution, generating the feedback, and directing student's learning process. All data about this is stored in a relational database (MySQL).

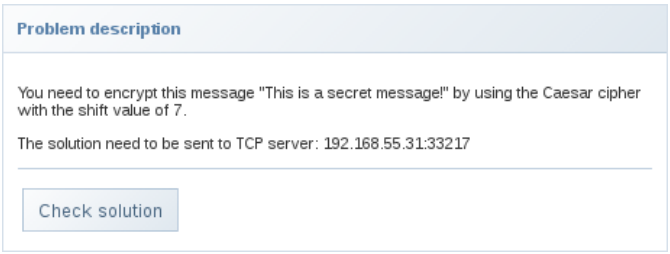

Fig 4. - Web application interface

Another component on the server is a component that serves as a TCP server. This component, also developed in Java, is developed as a UNIX daemon and is used for communication with CrypTool clients. The TCP Server is using parallel processes that are acting as workers. Each worker is using a different port, and ports are used to identify tasks and students. (However, for more complex tasks and larger number of students, default port range will be insufficient, so multiple IP addresses need to be used on server side.)

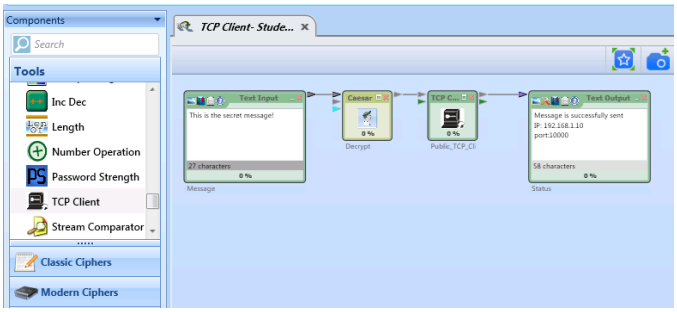

Fig 5 - Student's working environment, CrypTool

The communication between HTTP server and TCP server is done via the database. This means that new TCP workers are started when the main TCP server identifies new tasks in the database. After that, each worker process will remain active (and an associated port opened) until HTTP server marks tasks as finished (solved or canceled), or until given time-to-live (3,600 seconds by default) expires. These workers are very simple processes with function to read/write data that is received or sent over the network. The processing of that data (evaluating, etc.) is performed by the Web (JSP) application.

VI. Conclusion

In this paper, we briefly presented an intelligent PBL-based tutoring system for cryptology domain. The system is developed as a combination of Web (JSP) application and TCP server, and on the client side CrypTool environment (with the network communication extension) is used. The system is capable of generating different problems, where the structure and difficulty depends on the recorded progress of learners. Beside problem generation, the system is capable of evaluating learner's solutions and generating feedback for further learning.

Acknowledgment

Authors of the paper are members of projects TR32054, III44006 and ON174008 which are financed by Ministry of Science and Technological Development of the Republic of Serbia.

References

[1] S. Adamović, M. Šarac, M. Milosavljević, M. Veinović, A. Jevremović, An Interactive and Collaborative Approach to Teaching Cryptology, Educational Technology & Society, Vol. 17, No. 1, pp. 197 - 205, Feb, 2014

[2] G. Šimić, A. Jevremović, N. Šćekić, Case Studies About Problem Based Learning, The International Journal on Informatics and New Media in Education, Vol. 2, No. 1, pp. 15 - 20, Apr, 2009

[3] A. Jevremovic, G. Shimic, M. Veinovic, N. Ristic, IP Addressing: Problem-Based Learning Approach on Computer Networks, IEEE Transactions on Learning Technologies, pp. 0 - 0, Jun, 2016

[4] G. Šimić, A. Jevremović, Problem Based Learning in Formal and Informal Learning Environments, Interactive Learning Environments, Vol. 20, No. 4, pp. 351 - 367, Aug, 2012

[5] Hu, Ji, Christoph Meinel, and Michael Schmitt. "Tele-lab IT security: an architecture for interactive lessons for security education." ACM SIGCSE Bulletin. Vol. 36. No. 1. ACM, 2004.

[6] Elnajjar, Abed Elhaleem A., and Samy S. Abu Naser. "DES-Tutor: An Intelligent Tutoring System for Teaching DES Information Security Algorithm." (2017).

[7] N. Luburić, M. Stojkov, G. Savić, G. Sladić and B. Milosavljević, "Crypto-tutor: An educational tool for learning modern cryptography," 2016 IEEE 14th International Symposium on Intelligent Systems and Informatics (SISY), Subotica, 2016, pp. 205-210.
doi: 10.1109/SISY.2016.7601498

[8] Adamović, Saša, et al. "Teaching interactive cryptography: the case for CrypTool." IEEE Conference, ICEST. 2011.