A TOOL FOR PRACTICING ABOUT CLASSIC CRYPTOGRAPHIC ALGORITHMS INTEGRATED IN VIRTUAL LEARNING ENVIRONMENTS

Alberto Caballero, Patricia López, Fernando Pereñíguez
Universidad Católica San Antonio de Murcia (SPAIN)

Abstract

Classic cryptographic techniques and algorithms are typically taught in all basic courses of cybersecurity because they are the foundations of modern cryptographic techniques used to implement symmetric encryption or hashing algorithms. The correct comprehension of the operation of these algorithms can be facilitated if students get familiar with classical encryption algorithms. This paper shows a tool that has been specially conceived for practicing with classic cryptographic algorithms. The main functionalities of this tool rely on its ability to graphically illustrate the operation of the algorithms in a step-by-step way accompanied with detailed explanations about the basis of the algorithms are offered. The proposed tool also evaluates the most relevant metrics related to the performance of the classical algorithms such as consumed time, entropy, strength or weakness, among others. Furthermore, a set of predefined illustrative examples are included in order to allow the student compare several configurations taking into account these metrics. These examples could be used to discuss the robustness of each algorithm against cryptanalytic attacks, like those based on language statistics. Nevertheless, the tool also allows teachers or students to define new examples in order to study the internal details of each algorithm. The tool has been deployed as a web-based system and integrated in a virtual learning environment in order to enhance the usefulness and effectiveness when assisting the teaching-learning process.

Keywords: teaching tool, classic cryptographic algorithms, Playfair, Vigenère.

1 INTRODUCTION

Nowadays, cybersecurity is an essential matter present in a large amount of degrees in Information and Communication Technologies. Classical cryptography models and algorithms are usually studied in these courses. Classical systems are the foundation of today's cryptographic systems [1,2].

Several classic systems have fallen into disuse because of their vulnerability and easiness of cryptanalysis. However, they retain their theoretical interest. After studying some of their properties, the operation of modern algorithms can be understood better. From a didactic point of view, two classic encryption algorithms stand out: Playfair and Vigenère [3]. They are very interest because several reasons: their simplicity of operation, the variety of encryption concepts involved, the variants regarding to the definition of the encryption key, the vulnerabilities in front of certain characteristics of the language, among others [4].

This work presents, on the one hand, PatriCipher, a new tool used for teaching the fundamentals of cryptography through the explanation and experimentation with two concrete methods: Playfair and Vigenère. On the other hand, it shows how PatriCipher has been used in two courses lectures at the Universidad Católica San Antonio de Murcia (UCAM). This tool was also integrated in the university's Virtual Learning Environment (VLE). So, it can be accessible by all students, at any time, according to their learning requirements.

The rest of the paper is organized as follows. Section 2 explores main characteristics of similar tools reported in the literature. Section 3 depicts the most relevant functional and educational requirements considered into the development of our tool. Next, section 4 shows an example of how our teaching tool has been used into two courses in our university. Finally, conclusion and future work are given in section 5.
2 SOFTWARE TOOLS FOR CYBERSECURITY TEACHING

There are several applications developed for practicing about cybersecurity basic methods. Specifically, regards to classic cryptography models, we can highlight Vigenère Cipher [5], CrypTool Online [6], The Black Chamber [7] and Rumkin [8].

Vigenère Cipher is a very simple web application. It offers a textual explanation about the Vigenère algorithm and the possibility to perform encryption examples. Users can encrypt several messages using several keys. In a separate section, decryption is allowed. However, it only implements a unique algorithm; it does not explain its operation step by step neither allows the storage of the treated examples. It is not possible to compare various decryption encryption configurations. It does not provide metrics on algorithm performance.

CrypTool Online gives the possibility of performing both encryptions by Vigenère method and Playfair. It exhibits the same functionalities and deficiencies as the previous tool. Additionally, against it, it offers a navigation model that is not very intuitive and does not support the decryption process.

The Black Chamber and Rumkin are similar tools can be used to encrypt and decrypt by means of two algorithms Playfair and Vigenère. They do not have any significant difference respect to the previous ones.

In general, all the known tools are mainly engaged in performing encryption and decryption processes based on certain parameters. Thus, for example, students could try with several combinations and see the result of the encryption / decryption processes with a specific text and key. However, these tools lack functionalities related to the detailed explanation of the inner operations of the algorithm. To cite just one example, knowing the inner operations of a classic algorithm could be interesting when basic cryptanalysis techniques are studied.

3 LEARNING REQUIREMENTS

From our point of view, the tools mentioned in the literature lack the didactic-educational potential necessary in our cybersecurity classes. As a fundamental limitation we find the impossibility of performing class exercises that consist of comparative tests of the operation of the algorithms against various configurations or problems. Here we present a tool that (1) allows the analysis of the operations of these algorithms and (2) performs small experiments with them. For instance, it might be interesting to analyze the significance of key election and size against different alphabets or messages to be encrypted.

Among others, lectures of cybersecurity subjects require a tool that supports the following actions:

- To provide step-by-step explanation of the algorithms operations allowing the study of basic cryptanalysis techniques.
- To store and retrieve previously setting in order to be used in future exercises.
- To obtain statistics and metrics about the operation of each algorithm allowing efficiency and effectiveness analyses. (This is a feature that is not reported in any of the known tools).
- To compare several configurations allowing the assessment of the strength and weakness of each algorithm against different configurations. The graphical representation of such comparisons could be adequate to discuss the performance of each algorithm.

Considering the requirements listed above, PatriCipher was developed as an educational tool to support the teaching and practicing about two classic encryption algorithms: Vigenère and Playfair. It is integrated in the VLE of the university so that it is accessible for all students enrolled on the subjects could require this resource.

The main view of PatriCipher is offered in Figure 1. This tool is available via Web from the VLE of UCAM.
Fig. 1. The main view of PatriCipher, available from the Virtual Learning Environments of UCAM.

4 A CASE OF USE

PatriCipher has been successfully used in two courses taught at UCAM: Cybersecurity in Computer Sciences Degree and Cybercrime in Criminology Degree.

In both cases, PatriCipher was used to explain the basics of classic cryptographic algorithms. The functionality of the two algorithms was detailed step by step. Figures 2 and 3 show two views of PatriCipher when the operations of Palyfair and Vigenère were respectively exhibited.

Fig. 2. Explanation step-by-step of Playfair algorithm.
Once the algorithms operations were explained, the same interface has been used to comment features should have a key to get a good encryption. For example, it has been experienced using different key sizes and different types and variety of characters in the key. For each configuration, the tool offers the most relevant metrics that can be used to evaluate the performance of each algorithm. Figures 4 and 5 show two types of metrics offered by PatriCipher: entropy and percentage of characters, respectively.

**Fig.4. An example of the comparison of entropy generated for two types of key: a short key and a large one.**

**Fig.5. An example of the comparison of the percentage of characters presented in the encrypted text using two types of key: a short key and a large one.**
Encryption and decryption examples can be stored by the tool. This way, they can be retrieved in the future in order to continue with them or to perform comparative analysis respect to others. Figure 6 shows a view of such functionality.

Fig. 6. The view used to store and retrieve studies in PatriCipher.

5 CONCLUSION AND FUTURE WORKS

In this work we present a web-based application used to assist the teaching-learning process in cybersecurity courses. It had been successfully used in two different courses of Universidad Católica San Antonio de Murcia. Experiences gained in these two courses could be generalized for other cybersecurity courses taught in other universities. Additionally, because the tool is offered as web-based system, it can be deployed as part of any VLE in order to enhance the usefulness and effectiveness of the teaching-learning process.

In the future, PatriCipher could be extended by inclusion of other algorithms and new functionalities reported by lectures used the tool in their courses. Gamification techniques could be also included in the tool in order to stimulate the participation of students or to assists teachers in evaluation processes.

ACKNOWLEDGEMENTS

This work is partially supported by the Spanish MINECO under grant TIN2016-78799-P. The first author would also like to thank to the Ecuadorian Prometeo Project through the Secretaría de Educación Superior, Ciencia, Tecnología e Innovación.

REFERENCES