CryptoBase
A cryptography-based learning application

Vedran Juričić
Faculty of Humanities and Social Sciences
Ivana Lučića 3, Zagreb, Croatia
vedran.juricic@gmail.com

Ian Christian Hanser
Faculty of Humanities and Social Sciences
Ivana Lučića 3, Zagreb, Croatia
cryptobase11235@gmail.com

Dino Smrekar
Faculty of Humanities and Social Sciences
Ivana Lučića 3, Zagreb, Croatia
dino.smrekar@outlook.com

Summary

The authors are exploring the possibility of creating a cryptography-based educational application intended for the classroom and personal use. The basic idea is to help students or people interested in cryptography in their learning activities by providing them with an application capable of presenting basic information about codes and ciphers. Another goal is to give the users a chance to test out all of the ciphers contained within the application. One positive aspect of this kind of software is the fact that it can be adjusted to the user by using different languages and their alphabets in the learning process. Aside from personal use, this software can be incorporated in the classroom as an educational aid. It can also be used by teachers as an aid in grading student's tests.

Keywords: cryptography, ciphers, encryption, decryption, education, security, classroom aids

Introduction

In these modern times, we consider information as one of our most valuable resources. This idea evolved through history as technology developed. Since we view information as an extremely valuable resource, the need for masking and hiding information from unwanted interceptors arose quite fast. The solution to this problem was the development of cryptography.
Other key advances were made in terms of teaching and learning by developing different presentation techniques to accommodate different learning styles. We

have also seen a drastic change in student's learning habits with the rise of the World Wide Web.

The purpose of this project is to present CryptoBase, a cryptography-based learning application that can be used as a personal learning aid, an educational tool in classrooms or as help for teachers while evaluating student's tests. The application focuses on the user's interaction by allowing him to choose between three languages and presenting the user with a form which encrypts or decrypts an input message. The reason for creating such a project stems from the idea of incorporating different learning aids to enhance the student's learning experience[1]. The application is not intended only for students and focuses on anyone interested in learning about cryptography.

Cryptography and its contemporary use

Cryptography is a scientific discipline which focuses on studying and developing methods of sending messages in a concealed form, that is, in such a way that they can be read only by the person for whom the message is intended[2]. The two main methods of concealing messages in cryptography are codes and ciphers, which are defined as[3]:

- A cipher refers to an algorithm which replaces the order of letters or replaces each letter with a symbol or a different letter based on a key. The algorithm consists of encryption and decryption steps (steps required to make a message readable or unreadable.) The second important factor which affects the cryptographic algorithm is the key (a single word, phrase or string used for encrypting and decrypting messages.) This way, the encrypted messages may be read only by people who know the key.
- A code refers to a method of replacing words in a message with certain symbols, numbers or individual letters. A code always requires the use of a code book, as it serves as a reference in both the encryption and decryption process.

A code book is a lookup table consisting of words or phrases, and their corresponding code[4] (there also may be multiple codes intended for one word or phrase.)

Although cryptography was first used for military purposes, we can see its presence in every aspect of our lives, ranging from bank transactions, data encryp-

[1] Manichander, T. Emerging Trends in Digital Era Through Educational Technology, Second Edition. Solapur: Ashok Yakkaldevi. 2016. pp. 42-45.

[2] Stinson, Douglas Robert. Cryptography: Theory and Practice, Third edition. Ontario: Chapman and Hall/CRC, 2006. p. 1.

[3] Churchhouse, Robert. Codes and Ciphers: Julius Caesar, The Enigma, and the Internet. Cambridge: Cambridge University Press, 2002. p. 5.

[4] Anderson, Ross. Security Engineering: A Guide to Building Dependable Distributed Systems, First edition. John Wiley and sons 2001. p. 79.

tion and the majority of our day-to-day communication. Reliance on this certain technology also means that it is one of the key factors of online privacy[5].

CryptoBase project overview

The application currently contains 8 traditional ciphers which belong into the subcategories of monoalphabetic, polyalphabetic and transposition ciphers. All subcategories and its containing ciphers are organized in order of their complexity and each cipher introduces a new cryptographic method. This is because some of the advanced traditional ciphers incorporate simple cryptographic methods. It also gives us the ability to produce new ciphers by combining different ciphers. This application provides the users an interface which enables him to encrypt or decrypt custom message. The user can also change the key used in the cipher and the algorithm will also provide the result of encryption or decryption and a detailed overview how each letter has changed. This data may also vary from cipher to cipher because of different methods used in the processes of encryption and decryption.

- In the case of monoalphabetic ciphers, the displayed data includes both the plaintext and the ciphertext alphabets along with the encrypted or decrypted message.
- In the case of polyalphabetic ciphers, since the encryption process calculates a new letter based on the plaintext letter and a key letter, the displayed data includes each letter of the plaintext, along with the corresponding key letter and, of course, the resulting ciphertext letter.
- Finally, in the case of transposition ciphers the program calculates a matrix with the same number of columns as the key's length, and fills it up with the plaintext letters. This way the users have a clear view of how these types of ciphers operate because, aside from the result ciphertext, the program displays a step by step description of the encryption or decryption process.

Another key feature of this application is that it is currently translated into the English, Croatian and German language. The user is given a choice to switch between languages while the app is running and all of the data is displayed in the user's preferred language[6]. While a language is selected, the program also alerts the user if any of the input letters do not exist in the selected language's alphabet.

Application layout – navigation bar

The navigation bar always contains the back button and the language selection drop box. This is to enhance navigation between different windows of the appli-

[5] Cobb, Chey. Cryptography For Dummies, First edition. Indianapolis: Wiley Publishing, Inc. 2004. p. 23.

[6] Vigdorchik, Igor. WPF localization for dummies 13 December, 2011. https://www.codeproject.com/Articles/299436/WPF-Localization-for-Dummies (17 May 2017).

cation and to allow language changing. Another additional drop box appears when inside the cipher specific view. This drop box contains ciphers that belong in the same subdivision as the selected cipher.

Application layout – the main menu

The main menu consists of a tab bar which is divided into three subdivisions of traditional ciphers. Currently present categories include: monoalphabetic, polyalphabetic and transposition ciphers. When a category is selected, the tab bar container fills up with the ciphers of the selected category. Links to specific ciphers are displayed in the form of a button which contains an icon and the cipher's name[7].

Figure 1. The main menu

Application layout – specific cipher view

This view is divided into two equal halves. The left half represents the interactive part of the application and it consists of:

- the cipher's name
- the message input field – This field is intended for the user's input, it can be either a plaintext or a ciphertext
- The key input field – This field enables the user to enter a key which will be used while decrypting or encrypting a message, sometimes it will be disabled since some ciphers do not require a key
- the output field – The result of encryption or decryption (based on the user's choice) is written here
- The encryption data field – after the application has encrypted or decrypted a message it will also print out a detailed description of how each letter was calculated. The look of this box varies from cipher to cipher.

[7]Stovell, Paul. WPF Navigation 2 October 2009. www.paulstovell.com/blog/wpf-navigation (17 May 2017.)

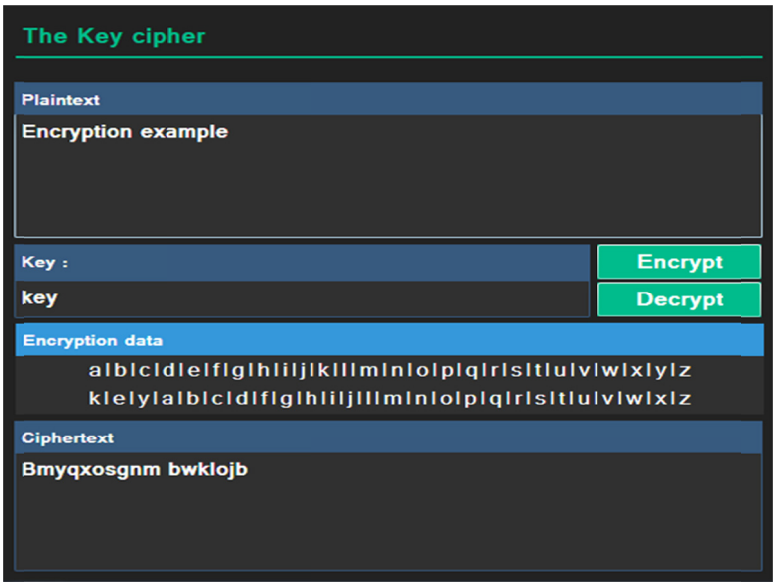

Figure 2. Specific cipher view – left half

In the case of monoalphabetic ciphers, the cipher always refers to one plaintext and one ciphertext alphabet. Because of that, the data is divided into two rows, with the first one containing the plaintext alphabet and the second one containing the ciphertext alphabet, while the number of columns varies based on the user's selected language.

In the case of polyalphabetic ciphers, every letter is calculated by assigning each letter of the alphabet a number and adding a key letter's value to a plaintext or ciphertext letter's value. That way we can print out the input, key and result letters, along with their numerical representations.

Finally, in the case of transposition ciphers, the resulting message is calculated by rearranging the letters of the input message. The program draws a different table based on the key and input message lengths along with indicators of how letters should be rearranged.

The Right side of this view is consisting of three different drop-down menus. The first menu is titled "about the cipher" and holds historical information about the cipher, such as: author details, historic use and development. The second menu is titled "encryption steps" and the third one "decryption steps" and each of these drop down menus holds a detailed description of the encryption and decryption processes presented in the user's preferred language. These drop boxes always contain one example of a message being encrypted or decrypted and all the data linked to the process.

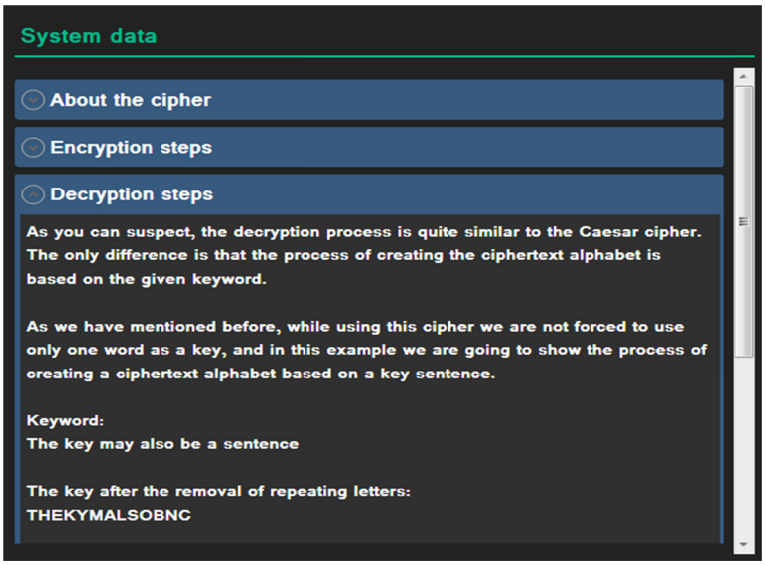

Figure 3. Specific cipher view – right half

Conclusion

Although these present features serve a purpose and contribute to one's personal learning, there is still room for improvement. The first important step in advancing this application is to incorporate more languages, as to accommodate a wider audience. Also, to make the app run on different devices, it is possible to write a server API which can be accessed both by personal computers and mobile devices. In order to aid the users even more, it is necessary to build a question based system so the user can test his knowledge. In this mode, the program will provide the user with a random message from a database and will task him with encrypting or decrypting the given message.

References

Manichander, T. Emerging Trends in Digital Era Through Educational Technology. Second Edition. Solapur: Ashok Yakkaldevi. 2016.

Stinson, Douglas Robert. Cryptography: Theory and Practice, Third edition. Ontario: Chapman and Hall/CRC, 2006.

Anderson, Ross. Security Engineering: A Guide to Building Dependable Distributed Systems, First edition. John Wiley and sons 2001.

Cobb, Chey. Cryptography For Dummies, First edition. Indianapolis: Wiley Publishing, Inc., 2004.

Vigdorchik, Igor. WPF localization for dummies 13 December, 2011. https://www.codeproject.com/Articles/299436/WPF-Localization-for-Dummies (17 May 2017).

Churchhouse, Robert. Codes and Ciphers: Julius Caesar, The Enigma, and the Internet. Cambridge: Cambridge University Press, 2002.

Stovell, Paul. WPF Navigation 2 October 2009. http://www.paulstovell.com/blog/wpf-navigation (17 May 2017).