Interactive Learning:
Cryptographic Methods

Author: Jorge Silvestrini
Email: jorgem9427@hotmail.com
Co-authors: Dr. Alfredo Cruz, alfredcross@gmail.com
Dr. Jeffrey Duffany, jeffduffany@gmail.com

Introduction

My goal in the Tapia Conferences is to participate with other undergraduate and graduate students, faculty, researchers, and professionals in computing from all backgrounds and ethnicities to: celebrate the diversity that exists in computing; network with others that have common backgrounds, ethnicities, disabilities, and genders; make contacts with computing leaders in academia and industry; participate in the poster session to present my research to the Tapia community. This experience will help me benefit from the diverse groups that that leverage their talents and passions to explore novel ways to change the world through new solutions. These key insights from diverse societies are necessary for broader, more impactful, simply better outcomes. I expect this conference to help me develop a more robust and useful application that will help security experts by accessing it directly on the Web.

The interactive learning in our society is something that has been decaying over time. The way presencial and online courses are being taught many times does not provide us with an instant feedback of the actions the learner performs. In many occasions we can observe how the learning process becomes difficult in some topics and we don t receive an explanation in time of why an action was incorrect and how it could be corrected. This causes frustration among students and teachers and makes it harder to continue on to more complex topics when educating today s generation of IT security scientists. This application targets students, from high school to college, who are interested in a career in security and information assurance. The use of a cryptographic methodology tool is the best way to begin the process of interactive learning in security since these are indeed the basic modules of security. Interactive learning is a way of autodidactic learning that teaches our minds to learn by themselves using the adequate tools. This is an ongoing project with aht future in education in cybersecurity.

Background

Interactive learning is a very important topic open for discussion. Meaning that depending on the field that we are considering, the interactive reading could be for example programmed instruction, interactive multimedia, virtual reality or teaching machines. My research, however, defines how students can interact with the application and the tools they are provided. The path the project has taken is making the student understand a topic first and then practicing the method step by step with a constant feedback of his actions directly from the tool. For this type of interaction, we need a computer with an internet connection capable of accessing the tool which will be available on a Web server. This project will be exploring the development of a tool that can provide a complete process for teaching/learning in and out of the classroom so

students can participate actively in cryptography topics. Eventually the idea is to promote the development of these interactive tools in other disciplines where it could be more beneficial than the traditional mode of learning.

Project Goals and Research Questions

The main goal of this ongoing research is to provide the students in the computer science field an education where their actions are been constantly monitored and commented based on their reactions to questions. The work will accomplish the interaction between students and technology necessary to learn a topic without the intervention of a human educator. This will create a greater independence in the learning process for young students at an early stage of their lives, developing an independent course of study, but secretly being monitored by the system to provide feedback just like a human teacher. Research questions that will arise with interactive learning in technology especially in the computer science field: How can interactive learning improve the education in computer science topics? How can cryptographic methods be taught without the presence of a human teacher? Is the student showing any positive progress in independent studies monitored by a virtual system?

Relevance and Significance

The significance of this project is to contribute the education process of young computer science students or those who are interested in teaching in the field. Education today has some limits that are out of the students hands, for example: educational institutes been short of staff, economic problems, and the fair offerings of online interactive courses. By offering interactive online courses we could help educational institutions and independent learners complete their learning/teaching goals. Currently, in the computer science field we can find a lot of information and courses on cryptographic methods. Yet usually all of these courses are based on explanation and answer giving mechanics. The student doesn t actually practice at all since there is a tool that gives the answer straight away without making the student work. Parting from this case scenario, implementing an online interactive learning tool will give the students the opportunity of practicing what they just learn with constant feedback of their actions.

Approach

To implement this project, a web application is been developed to be used in the interactive learning process. Written in Python with the Django framework alongside with HTML and Javascript, the online tool will feature simple cryptologic methods that are easy to understand and implement. Such cryptologic methods are the Caesar Cipher, Vigenere and Playfair which are all substitution types and also can be extendible to other types of ciphers. Methods will be explained while using the tool and explained in detail. During the development process, the tool has been offered to sophomore students to collect their individual experiences and feedback. With this information, changes are being made to ensure that the interactive tool being implemented meets user expectations in the learning experience, to help them develop independence in their study habits.