Introduction into Cybersecurity through Cryptographic Algorithms

Author: Alfredo Alexander Cruz
Advisor: Alfredo Cruz, Ph. D.
Electrical & Computer Engineering and Computer Science Department

Abstract

Cybersecurity has become one of the most crucial national security concerns facing the U.S.A. and the rest of the world. This is due to society's ever-growing dependency on technology, which has made it extremely vulnerable to different types of cyber-attacks. These security threats produce an inherent need for cybersecurity specialists in the public and private sectors. It is essential to start providing important elements of cybersecurity at the early stages of education (K-12). This project developed three interactive modules on cryptographic algorithms for the use of educators and students who want to study the fundamentals of cryptography, which is a critical part of cybersecurity. By using Bloom's Taxonomy to develop the modules, the author assures that each module will function as a straightforward guide for teachers, students, and faculty members.

Introduction

In Computer Science, cryptography refers to the use of communication techniques that are derived from algorithms and mathematical concepts to secure information. This is achieved by protecting the data from unauthorized access or modification. With the use of cryptography, we can assure the confidentiality and integrity of information. In the cybersecurity field both concepts are considered essential. Due to an urgent global need for cybersecurity professionals, introducing young students to this topic is imperative. The main goals of the proposed cryptographic algorithms modules are the following:

- Introduce students from K-16 education to fundamental concepts of cryptography and cybersecurity.
- Raise awareness of cybersecurity as a future career alternative, in order to help mitigate the cybersecurity workforce shortage.
- Promote Science, Technology, Engineering and Mathematics (STEM) to those in underrepresented groups.
- Challenge students' problem solving, critical thinking, and mathematics skills.

Background

The number of cybersecurity incidents continues to increase dramatically. Organizations that have access to an outstanding amount of sensitive information such as the Office of Personnel Management (OPM), Uber Technologies Inc., and Equifax are victims of the high-profile cyber-data breaches. According to the U.S. Securities and Exchange Commission [1] this represented an average loss of $4.9 million in 2017 to $7.5 million in 2018. Cyber defense is now considered a necessity for both the public and private sectors. At the corporate level, it means the protection of people and financial information. At the federal level, it means protecting critical infrastructures such as schools, hospitals, and financial services that keep society functioning [1]. The demand for cybersecurity specialists heavily outnumbers the quantity of professionals with the adequate skills. According to the U.S. Bureau of Labor Statistics, the growth rate of jobs in information security is projected to increase 37% from 2012–2022; and an estimated number of more than 209,000 cybersecurity jobs in the U.S. will go unfilled every year. This could lead to a global shortage of 1.8 million cybersecurity professionals by the year 2022 [2]. In 2016, President Obama signed two executive orders to fortify the federal government's ability to defend against cybersecurity attacks and proposed to increase the budget assigned for cybersecurity to $19 billion [3].

Problem Statement

A recent study [4] from McAfee and the Center for Strategic and International Studies (CSIS) found that: "The cyber skills shortage is not just a regional or even a national problem—it's global. Around the world, 82% of respondents reported a lack of cybersecurity skills within their organization and 71% acknowledged that the talent shortfall makes organizations more vulnerable to attackers.". The situation will only worsen if we do not introduce cybersecurity as a possible career choice for kids from an early age. A recent study from the University of Phoenix found that 80% of all adults never considered a career in cybersecurity, over 50% have never heard of penetration testing, and other important cybersecurity concepts such as cryptography, encryption, integrity and confidentiality of data, among others [5]. We can't mitigate the cybersecurity skill shortage when most of the population does not even know about the existence of cybersecurity. The cybersecurity talent shortage is worsened by the lack of cybersecurity education in K-12 and university programs. Current STEM curriculums are already overcrowded with different subjects and an overwhelming majority of our current teachers and IT faculty do not have any type of formal education in the area of cybersecurity. Governments around the globe and private entities are beginning to understand that this is a serious problem that needs to be addressed.

Methodology

Three different modules were created to teach/learn cryptography, each one focusing on a different algorithm: Monoalphabetic Substitution, Polyalphabetic Substitution, and Transposition Ciphers. The monoalphabetic substitution cipher uses fixed substitution over an entire message, whereas a polyalphabetic cipher uses several substitutions at different positions in the message. Meanwhile, the transposition cipher shifts the positions of the units within the plaintext. With the implementation of Bloom's Taxonomy, each one of these algorithms will enable students to use their problem-solving skills to analyze and evaluate various encryption methods and come up with even stronger and more secure cryptographic algorithms. As shown in Figure 1, each individual module was created to be delivered in a sequential order. Important concepts lead to subsequent units.

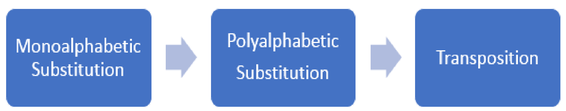

Figure 1. Sequential Order of the Modules

The structure used for the modules was the following: Module Overview, Module Learning Objectives, Module Content, Module Instructional Tools, and Assessment of Learning: The Module Overview provides the educator with a brief description of the unit module; length of the lesson, scope, and background. The Module Learning Objectives defines the expected goals of the lesson in terms of demonstrable knowledge that the student should have acquired as a result of the lesson. The Module Content gives detailed information on how the lesson should be carried out and presents the instructor with points of discussion. The Module Instructional Tools are a series of crafted resources that will aid the educator, these include; PowerPoint Presentation, Pre-Presentation Materials, and the Presentation Exercise Worksheets (formative assessment).

Methodology cont…

Every Module Unit includes a PowerPoint Presentation of around 25-30 slides. This will help the lesson with visual aids and a defined order of information. As previously mentioned, Pre-presentation resources are also included in the Instructional Tool section. These are useful worksheets that will be handed to the students before the presentation. They include important resources that streamline the process of student learning. Formative assessment worksheets are also included. These are simple assessment documents that are meant to be completed during the lesson. They provide feedback to the instructor, who will be able to adjust the ongoing teaching. Basically, allowing students to complete exercises during the lesson will let the instructor know if students are having any difficulty with the presented material. The Formative Assessment Learning Cycle (see Figure 2) is an essential transformative instructional tool that, if clearly understood and effectively used, can greatly benefit both educators and their students.

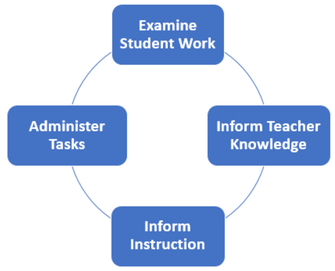

Figure 2. Formative Assessment Learning Cycle

Finally, The Assessment of Learning provides the educator with three different summative assessment worksheets. The worksheet assessments are meant to allow the educator to measure the student's different levels of the Cognitive Domain from Bloom's Taxonomy within the lesson (see Figure 3) .

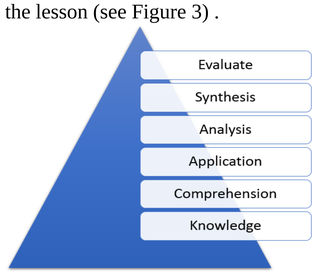

Figure 3. Blooms Taxonomy: Cognitive Domain Diagram

The Level 1 worksheet assessment evaluates if the knowledge and comprehension levels of the taxonomy have been achieved. Level 2 worksheet evaluates application and analysis. The Level 3 worksheet enables students to demonstrate their mastery of the unit creating and evaluating new cryptographic algorithms. The modules are hosted on the website that serves as an online resource for educators and students. Using the website, the educator can provide interactive workshops for students, and students can access the material on their own. This enables the educator and students from diverse backgrounds to have access to the instructional material. Simplification of content and hands-on activities will motivate educators and students to continue learning, making this an invaluable educational experience that introduces educators and students to the world of cryptography. The website will eventually grow in functionality with the input of the users.

Conclusions

Students were introduced to cryptographic algorithms as an essential part of cybersecurity. The website serves as an additional online resource for both educators and students. They streamline and facilitate the teaching process and provide interactive workshops for students. Differentiated instruction is a crucial part of this project. It enables the educator to reach students from diverse backgrounds. The numerous dynamic activities and the simplification of the content motivates and inspires students to continue learning. Providing educators and students with a steppingstone into the field of cybersecurity enables them to realize the diverse number of opportunities that exist in the area of IT and cybersecurity. This will help mitigate the global demand for cybersecurity professionals at the local and national level.

Future Work

Five different School Officials from Intermediate and High Schools will be contacted so the author can deliver a two-hour workshop including the modules, presentations, and assessment materials. The learning process will be evaluated and the Student Learning Worksheets will measure what students learned. A survey will be handed out at the end of the workshop to receive feedback from the target audience. This will help the author assess the effectiveness of the modules and make any required changes for improvement. The website will continue to be enhanced with additional tools, modules, and essential resources. Future modules will focus on intermediate and advanced concepts. Eventually, these modules will not be limited to cryptography. The website will continue to be enhanced with more modules that include other principles of cybersecurity, contributing even more to the field.

Acknowledgements

This material is based upon work supported by, or in part the national Science Foundation Scholarship for Service (NSF-SFS) award under contract/award #1563978.

References

[1] G. Garrett, "Cyberattacks Skyrocketed in 2018. Are You Ready for 2019?", *IndustryWeek*, 2019. [Online]. Available: https://www.industryweek.com/technology-and-iiot/cyberattacks-skyrocketed-2018-are-you-ready-2019.

[2] "Shaping the Next Generation Cybersecurity Workforce Today", *Department of Homeland Security*, 2017. [Online]. Available: https://www.dhs.gov/science-and-technology/blog/2017/10/23/shaping-next-generation-cybersecurity-workforce-today.

[3] J. Marks, "The Cybersecurity 202: DHS is pushing cybersecurity support to presidential campaigns", *The Washington Post*, 2019. [Online]. Available: https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2019/04/24/the-cybersecurity-202-dhs-is-pushing-cybersecurity-support-to-presidential-campaigns/5cbfb5981ad2e52459e24664/?utm_term=.94d4ef355e.

[4] Center for Strategic and International Studies (CSIS), "Hacking the Skills Shortage", McAfee, 2016.

[5] K. Matthews, "Most U.S. Adults Never Consider Cybersecurity Careers: Why That's a Problem", *Globalsign.com*, 2018. [Online]. Available: https://www.globalsign.com/en/blog/us-adults-never-consider-cybersecurity-careers/.