Introduction into Cybersecurity through Cryptographic Algorithms

Alfredo Alexander Cruz
Master of Computer Science
Alfredo Cruz, Ph.D.
Electrical and Computer Engineering & Computer Science Department
Polytechnic University of Puerto Rico

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. These instructional modules will be available on a website to provide the tools required to teach and learn basic cryptography and cryptographic algorithms. By using Bloom's Taxonomy to develop the modules, the author assures that each module will function as a straightforward guide for teachers, undergraduate and graduate students, faculty members, and anyone interested in enhancing their mathematical reasoning, critical thinking, and problem-solving skills in cryptography.*

Key Terms *— Cryptography, Cryptosystem, Cybersecurity Education, Encryption.*

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.

To introduce students from K-16 education to this field, the author proposes the creation of cryptographic algorithm modules. They are designed to keep students interested and engaged in the topic during the workshops. The modules are hosted on an online Website, making them easily accessible to educators and school districts. They are organized in various sections: Module Overview, Learning Objective, Module Content, Instructional Tools, and Assessment of Learning. Each module is based on Blooms Taxonomy that allows the implementation of differentiated instruction. It is important to assure that students can learn at their own pace [1].

Project Goals

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.

Research Questions

The following is a comprehensive list of research questions that were used in the development of the different cryptographic algorithm modules.

- Why is cryptography such an important area of cybersecurity education?
- What are some of the most useful cryptographic algorithms?
- How do each one of these algorithms differ from one another?
- What are the important factors when developing an effective lesson module?
- How can the teaching/learning process be streamlined to benefit the educator and the student?
- How can differentiated instruction be applied within the modules?
- What type of instructional tools are best suited for each different algorithm?
- How can the modules be effectively aligned with current cybersecurity concerns?

BACKGROUND LITERATURE

The number of cybersecurity incidents has increased dramatically over the past few years and it's a trend that is expected to continue. The Office of Personnel Management (OPM), Uber Technologies inc., and Equifax are some of the victims among many of the high-profile cyber-data breaches that have occurred recently. Unfortunately, these organizations have access to an outstanding amount of sensitive information. These types of cyber-attacks have triggered an average loss of $4.9 million in 2017 to $7.5 million in 2018, according to the U.S. Securities and Exchange Commission [2]. These numbers continue to increase.

As a direct response to the increasingly alarming number of cybersecurity attacks, 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 [2]. All of this has led to an increased need for cybersecurity specialists, since the demand 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. Even with the actions being taken this could lead to a global shortage of 1.8 million cybersecurity professionals by the year 2022 [3].

The U.S. government has taken important steps to address the cyber threats. 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 [4]. The Department of Homeland Security (DHS) is currently offering its cybersecurity services to all the 2020 U.S. presidential campaigns. The services include scanning computer networks for bugs and doing more complex penetration testing, according to Chris Krebs, director of Department of Homeland Security's Cybersecurity and Infrastructure Security Agency [4].

The efforts by the DHS are critical because in 2016, John Podesta a former White House Chief of Staff and the chair of Hillary Clinton's 2016 U.S. presidential campaign was hacked by a Russian cyber espionage group. The data breach was used to influence the 2016 presidential campaign [5]. This clearly proves the importance of the services being offered by DHS. However, the outlined actions taken by the government do not directly address the core of the problem.

PROBLEM STATEMENT

As stated, one of the most crucial emerging risks in the public and private sectors is the cybersecurity talent shortage. A recent study [6] from McAfee and the Center for Strategic and International Studies (CSIS) found the following "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 [7]. 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 our instructional system including K-12 and university programs.

Even the current IT 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 [8]. This contributes to the scarcity of cybersecurity education in our schools and universities. The demand for cybersecurity experts will continue to grow over the next decade. Furthermore, due to today's global expanding reliance on technology, the United States' educational system needs to update their curriculums at the early stages to address the crucial need for cybersecurity skills to protect personal privacy; and to promote occupations in the field. Governments around the globe and private entities are beginning to understand that this is a serious problem that needs to be addressed as soon as possible.

BARRIERS AND ISSUES

There are many barriers and issues that contribute to the shortage of cybersecurity professionals and the overall lack of skills and knowledge in the field. One of the most important factors is that K-12 students are not being exposed to any area related to cybersecurity during these early stages. This is crucial since many students do not even know about the existence of the field. We know that teens typically make choices about their careers during their 9th-12th grade. Although technology is a topic of interest, many students do not know about the emerging field of cybersecurity. In High School computer classes do not include cybersecurity modules that could at least present it from a social/behavioral perspective. Even many universities still do not include cybersecurity related courses/modules in the Computer Science/Engineering curriculum to provide the required professional skill sets and knowledge in the field.

This leads to another crucial barrier; educators do not have the background or preparation required to teach cyber security courses or include modules in their traditional courses [8]. Since it is part of an emerging technology/field, not many educators are familiarized with the topic, or feel comfortable teaching topics. Likewise, Higher Education institutions are just starting to add new courses, programs, and certifications related to cybersecurity. This is the why we need to provide simple introductory modules for those educators who are interested in integrating them but do not have the background or the resources to learn/teach these topics.

Another issue is that most of the modules related to introductory topics such as cryptography are too complex or uninspired. There is a need for modules that can be easily understood by kids from 6-12th grades. Students should not feel intimidated by the material or concepts covered in these modules. Students prefer dynamic activities and interactive learning; the modules need be made as entertaining as possible. Students need their lessons to be more than just passive learning, they need active learning as well. They need to include many hands-on activities, challenges, competitions or games.

Finally, another barrier that is usually ignored by other online modules that could exist, or by outdated curriculums, is the fact that students require differentiated instruction and assessment.

Differentiated instruction also known as differentiated learning, refers to a philosophy for effective teaching that involves providing students within their diverse classroom community of learners a range of different avenues for learning and understanding new information. This can be seen in terms of acquiring content, processing, constructing, or making sense of new ideas; and developing teaching materials and assessment measures so that all students within a classroom can learn effectively, regardless of differences in ability [9]. This essential for educators to reach students who might otherwise fail to keep up with the material.

PROPOSED SOLUTION

The severe shortage of cybersecurity professionals is an impending risk to national security in the United States and other countries. Since cryptography is one of the main issues in cybersecurity, the cryptographic algorithm modules can help to mitigate the cybersecurity skill shortage by introducing students at an early age into the world of cybersecurity. Cryptography is a stepping stone in the process of teaching/learning cybersecurity.

Cryptography is a key element of security. If we cannot maintain sensitive information safe, we cannot protect the nation. Cryptography is the use of the techniques of encryption and decryption Cryptology is the study of the various techniques of cryptography used in the process of keeping our data secure (using encrypting and decrypting methods), and of obtaining sensitive data from our adversaries (decryption methods). This project creates modules based on Blooms Taxonomy available to educators to teach basic cryptographic algorithms to a wide audience. Students can also access the modules on the Web and learn by themselves. This represents an advancement in cybersecurity and cryptography education as the author aims to impact teaching/learning and target a wider and younger audience through this method.

To address the shortcomings of our educational system in terms of cybersecurity education, a number of three different type of interactive lesson modules were developed. Each specific module will focus on a different type of cryptographic algorithm which includes the following ciphers: Caesars, Vigenere, and Rail Fence. These modules range in difficulty and provide educators with the resources necessary to properly give a lesson to their students in a dynamic and interactive manner. They will also help students learn by themselves if they have the interest. This is imperative in order to get students motivated and interested in the field of cryptography.

The modules are specially designed to be accessible and straightforward to the educator and the student. There are no additional requirements for educators interested on utilizing these resources. Using Blooms Taxonomy, all the modules are constructed to follow a specific structure: Module Overview, Learning Objective, Module Content, Instructional Tools, and Learning Assessment. The Learning Assessment section will include different types of exercises that will allow the educator to implement differentiated instruction. While providing students with information is essential, it is even more important to make sure that every single one of them can learn at their own pace to avoid feeling discouraged [10].

METHODOLOGY

Three different unit modules were created for this project, each one focusing on a different defining cryptographic algorithms; 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 an even stronger and more secure cryptographic algorithms. As shown in Figure 1, each individual module was created with the intention of being taught in a sequential order, as every unit introduces important cryptography concepts that are used throughout the subsequent units.

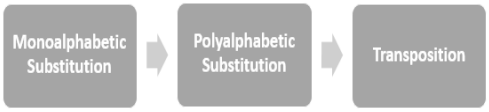

Figure 1
Sequential Order of the Modules

As seen in Figure 2, the structure used for the modules was the following: Module Overview, Module Learning Objectives, Module Content, Module Instructional Tools, and Assessment of Learning:

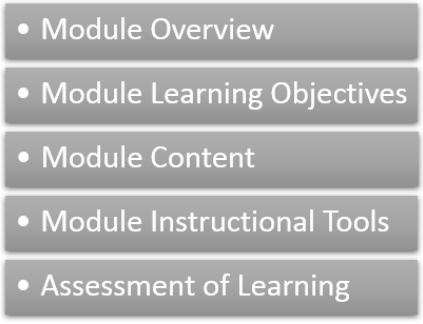

Figure 2
Design Structure of Each Module

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). Every Module Unit includes a PowerPoint Presentation around 25-30 slides long/ This will help the lesson with visual aids and a defined order of information. In the Figure 3, we can see an example of a slide from one of the modules. This slide contains a bar graph representing the relative letter frequencies in the English language, where the most common letters are E, T, and A. Meanwhile, the least commonly used letters are X, Q, and Z.

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.

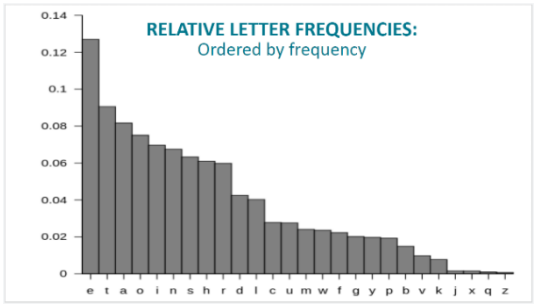

Figure 3
Instructional Tool: Example of a PowerPoint Presentation Slide

The Polyalphabetic Substitution Module has a document with a step-by-step tutorial on how to use the Vigenere Square Table (see Figure 4). This table is one of multiple methods that can be used for encrypting and decrypting Vigenere Ciphers.

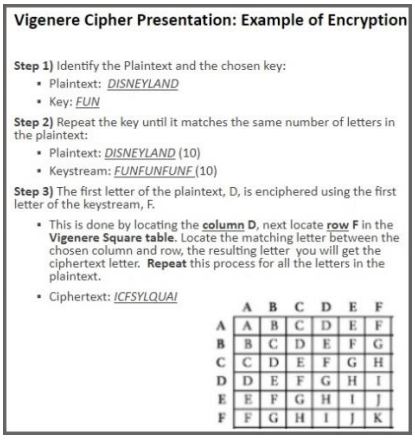

Figure 4
Instructional Tool: Vigenere Square Table Tutorial

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 5) is an essential transformative instructional tool that, if clearly understood and effectively used, can greatly benefit both educators and their students.

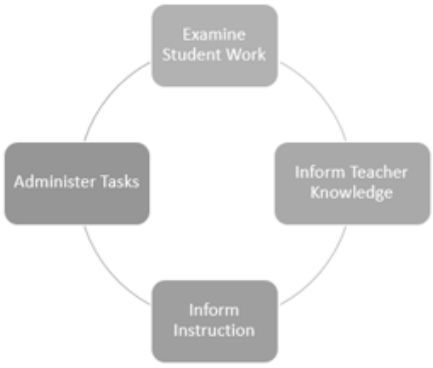

Figure 5
Formative Assessment Learning Cycle

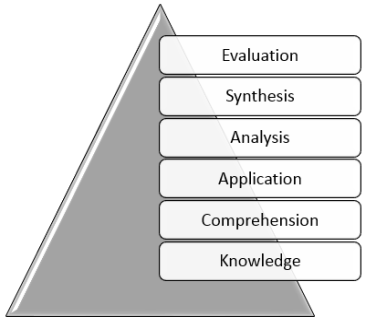

Figure 6
Bloom's Taxonomy: Cognitive Domain Diagram

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 (see Figure 6) within the lesson. The first worksheet (Level 1) assessment will look to evaluate if the knowledge and comprehension levels of the taxonomy have been achieved. Likewise, the following worksheet (Level 2) will evaluate application and analysis. The last worksheet (Level 3) should enable students to demonstrate their mastery of the unit creating and evaluating new cryptographic algorithms.

The cryptographic algorithm modules will introduce students to an essential part of cybersecurity, that is cryptography. The modules will be hosted on the website (see Figure 7), that serves as an online resource for educators and students. This facilitates the teaching/learning process. 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.

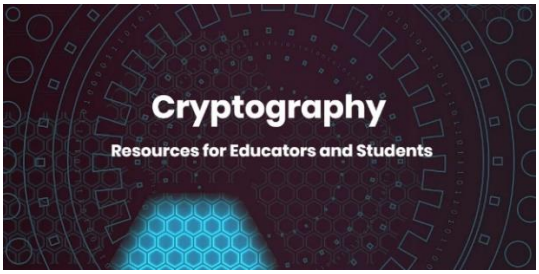

Figure 7
Home Page of The Website Hosting the Modules

For further assessment to enhance the website and instructional materials, the author will validate the modules by visiting five different Intermediate and High Schools to deliver a two-hour workshop. Students will be presented with the modules, presentations, pre-presentation and learning assessment materials. The learning process will be evaluated to determine if the modules are effective in delivering the educational material. 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 students. School officials and educators will also be

surveyed and interviewed to see how they perceive the method and its effect on the teaching/learning process. We will also ask them to suggest other topics of cybersecurity that can be developed into modules. This feedback will help the author assess the effectiveness of the modules and make any required changes, that includes adding more topics. The website will also provide a source for on-line feedback from the persons that access the website to teach and/or learn. All the feedback will be used to include more learning materials and improve the original modules.

The website will continue to be enhanced with additional tools, modules, and other resources as feedback continues to flow. This will increase the efficiency and effectiveness of the modules in the teaching/learning process. 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. This will help to bring more students into this exciting field, being part of the solution to prepare more cybersecurity professionals at the local and national level.

Module 1 Overview: Caesar Cipher: Welcome to the World of Cryptography

This module begins with a discussion of the essential concepts in cryptography. It includes the history of the Caesar Cipher, one of the earliest and simplest forms of encryption. This technique was used by the famous leader of the Roman Empire, Julius Caesar. The lesson explains the importance of secure communication via the use of encrypted messages. Students will also create their own Caesar Shift Wheel during the lesson in order to analyze and apply the fundamental concepts of cryptography such as: Plaintext, Encryption, Decryption Ciphertext, Key, and Frequency Analysis. They will learn to analyze and implement cryptanalysis methods for the Caesar Cipher. At the end of the activities the students will design their own monoalphabetic substitution cryptographic algorithm.

Module 1 Learning Objectives

The learning objectives for Module 1 are:

- Explain the importance of secure communication in today's digital age.
- Introduce students to the area of cryptography.
- Expand the relationship between linguistics and mathematics.
- Provide different methods of decryption for the Caesar Cipher.
  - Cryptanalysis
  - Brute Force
- Challenge critical thinking and problem-solving skills.

Module 2 Overview: Vigenere Cipher: Into the Crypto-Verse

This lesson module begins with a discussion of the inherent weakness of monoalphabetic substitution ciphers. Students will analyze the relationship between the possible number of keys and the strength of the encryption algorithm. They will discuss how the use of frequency analysis and brute force are simple methods of decrypting the monoalphabetic substitution ciphers. As a stronger alternative, they will be introduced to the polyalphabetic substitution ciphers. The lesson will go over a brief history of the Vigenere Cipher. Students will learn how to encrypt and decrypt Vigenere Ciphers with the use of the Vigenere Square Table, and the Cipher Wheel. Students will create their own polyalphabetic substitution cryptographic algorithm.

Module 2 Learning Objectives

The learning objectives for Module 2 are:

- Review the importance of secure communication in today's digital age.
- Expand the relationship between linguistics and mathematics.
- Learn the difference between monoalphabetic and polyalphabetic ciphers.
- Learn the relationship between the key size of a cipher and its security.
- Learn different decryption methods for the Vigenere Cipher:

- Brute force
- Vigenere Square Table
- Cipher Wheel.

- Challenge critical thinking and problem-solving skills through exercises.

Module 3 Overview: Rail Fence Cipher: A New Word Order

This lesson module begins with a discussion about the two general principles cryptographic algorithms are based on: Substitution and Transposition. Students will learn about permutation and how it works within Transposition Ciphers. They will learn about the Rail Fence Cipher and they will employ different methods used to encrypt and decrypt this algorithm. At the end of the lesson the students will evaluate the strengths and weaknesses of Transposition Ciphers and they will create their own Transposition Algorithm Ciphers. At the end of the activities the students will design their own transposition cryptographic algorithm

Module 3 Learning Objectives

The learning objectives for this lesson module are:

- Learn the difference between Transposition and Substitution Ciphers.
- Expand the relationship between linguistics and mathematics.
- Learn different decryption methods for the Rail Fence Cipher using brute force and cryptanalysis.
- Challenge critical thinking and problem-solving skills.

FUTURE WORK

It's important to validate that the modules are meeting their objectives. For this reason, the effectiveness of the cryptographic algorithm modules must be tested. Five different School Officials from Intermediate and High Schools will be contacted to provide the author access to the schools, so he can deliver a two-hour workshop. Students will be presented with the modules, presentations, and assessment materials. The learning process will be evaluated to determine if the modules are effective in delivering the educational material. 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. These are both important parts of the assessment. This feedback will help the author assess the effectiveness of the modules and make any required changes, if necessary. The website will also provide for a feedback from the persons that use it to teach and/or learn. The feedback will be used to ongoingly improve the modules.

With the results from the Student Learning Worksheets and the findings from the survey the current cryptographic algorithm modules will be updated if required. Subsequently, the website will continue to be enhanced with additional tools, modules, and other resources as feedback continues to flow. This will increase the efficiency and effectiveness of the modules in the teaching/learning process. The future modules will focus on intermediate and advanced concepts.

Furthermore, these modules will eventually not be limited to cryptography. The Website will be expanded to include other principles of cybersecurity. This will allow students to experience many of the other exciting areas in this field.

CONCLUSION

The main goal of the cryptographic algorithm modules was to introduce students to an essential part of cybersecurity. These modules are hosted on the website which serves as an additional online resource for both educators and students. They aid to streamline and facilitate the teaching process required for the educator, and to provide interactive workshops for students. The integration of differentiated instruction within the activity is a crucial part of this project. This enables the educator to reach students from diverse backgrounds. Likewise, the numerous dynamic

activities and the simplification of the content will motivate and inspire students to continue learning, as they will not be overwhelmed by the content.

Providing educators and students with a steppingstone into the field of cybersecurity will enable them to look into the diverse number of opportunities that are offered within the area of Information Technology and cybersecurity. This will help to mitigate the strong global demand we are currently facing for cybersecurity professionals and will help us solve the problem at the local and national level.

This effort will be sustained with future work resulting directly from the Module Learning Worksheets; the direct delivery by the Author of the workshops to at least five Intermediate and High Schools for additional teaching/learning assessment; and the feedback from the website. All these will contribute to the continuous enhancement of the modules. Adding additional topics in cryptography and cybersecurity will also increase the effectiveness of the project, impacting larger audiences as it evolves into an efficient and important tool for students and educators interested in entering the field of cybersecurity.

REFERENCES

[1] C. Weselby. (2014). "What is Differentiated Instruction? Examples of Strategies", in *Concordia University-Portland* [Online]. Available: https://education.cu-portland.edu/blog/classroom-resources/examples-of-differentiated-instruction. [Accessed: April 2, 2019].

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

[3] Department of Homeland Security. (2017). *Shaping the Next Generation Cybersecurity Workforce Today* [Online]. Available: https://www.dhs.gov/science-and-technology/blog/2017/10/23/shaping-next-generation-cybersecurity-workforce-today. [Accessed: January 5, 2019].

[4] J. Marks. (2019). "The Cybersecurity 202: DHS is pushing cybersecurity support to presidential campaigns", in *The Washington Post* [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=.94d4ef355e74. [Accessed: April 25, 2019].

[5] B. Barrett. (2018). *DNC Lawsuit Reveals Key Details About Devastating 2016 Hack* [Online]. Available: https://www.wired.com/story/dnc-lawsuit-reveals-key-details-2016-hack/. [Accessed: January 13, 2019].

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

[7] K. Matthews. (2018). *Most U.S. Adults Never Consider Cybersecurity Careers: Why That's a Problem* [Online]. Available: https://www.globalsign.com/en/blog/us-adults-never-consider-cybersecurity-careers/. [Accessed: March 9, 2019].

[8] B. Keogh. (2019). *Kids need to learn about cybersecurity, but teachers only have so much time in the day* [Online]. Available: http://theconversation.com/kids-need-to-learn-about-cybersecurity-but-teachers-only-have-so-much-time-in-the-day-112136. [Accessed: April 3, 2019].

[9] L. Robb. (2019). *What Is Differentiated Instruction?* [Online]. Available: https://www.scholastic.com/teachers/articles/teaching-content/what-differentiated-instruction/. [Accessed: April 14, 2019].

[10] S. Udell. (2018). *How Differentiating Instruction Helps Students Connect to Learning* [Online]. Available: https://www.edsurge.com/news/2018-10-28-how-differentiating-instruction-helps-students-connect-to-learning. [Accessed: March 18, 2019].