TEACHING BASIC CONCEPTS OF CRYPTOGRAPHY IN PROFESSIONAL HIGH SCHOOL

ENSINANDO CONCEITOS BÁSICOS DE CRIPTOGRAFIA NO ENSINO MÉDIO PROFISSIONAL

ENSEÑANDO CONCEPTOS BÁSICOS DE CRIPTOGRAFÍA EN LA ESCUELA SECUNDARIA PROFESIONAL

Regina Paiva Melo MARIN[1]
Jackson Gomes Soares SOUZA[2]
Luciano Heitor Gallegos MARIN[3]

ABSTRACT: The cryptography is present in several operations performed daily by people, such as online shopping or in dialogues using computer equipment and the Internet as a proxy. Although cryptography is very important in the contemporary context, the teaching of the cryptography subject is new for students at professional high school. In this regard, one of the biggest challenges is to motivate students in using the cryptographic methods in the classroom. The objective of this work is to investigate the use and learning of cryptography by students at professional high school. For this purpose, the Survey methodology was used with self-evaluative questions about the motivation, understanding and the use of computational tools containing basic cryptography concepts. An analysis of the responses suggests that most students find the cryptography subject difficult to learn, but all of them were able to practice and learn at least one of the cryptographic techniques taught.

KEYWORDS: Practices. Teaching. Learning. Cryptography.

RESUMO: *A criptografia está presente em diversas operações realizadas diariamente pelas pessoas, tais como compras online ou no desenvolvimento de diálogos utilizando equipamentos computacionais e a Internet como meio. Embora a criptografia tenha muita importância no contexto contemporâneo, o ensino do tema é novo para os estudantes do Ensino Médio profissional. Neste aspecto, um dos maiores desafios está em motivar os alunos na utilização dos métodos criptográficos na sala de aula. O objetivo deste trabalho está em investigar o uso e a aprendizagem da criptografia por alunos do ensino médio profissional. Para tanto, foi utilizada a metodologia do tipo Survey com perguntas autoavaliativas sobre a motivação, compreensão, e o uso de ferramentas computacionais contendo conceitos básicos de criptografia. A análise das respostas sugere que a maioria dos alunos considera o tema*

[1] Federal Institute of Education, Science and Technology of Goiás (IF GOIANO), Urutaí – GO – Brazil. Professor in the Computer Science course. Doctorate in Computer Science (CENTRALESUPÉLEC) – France. ORCID: https://orcid.org/0000-0002-1303-052X. E-mail: regina.marin@ifgoiano.edu.br
[2] Federal Institute of Education, Science and Technology of São Paulo (IFSP), Campinas – SP – Brazil. Professor in the Computer Course. Doctoral Student in School Education (UNESP). ORCID: https://orcid.org/0000-0003-4952-8618. E-mail: jackson@ifsp.edu.br
[3] University of Fortaleza (UNIFOR), Fortaleza – CE – Brazil. Professor at the Data Sciences and Artificial Intelligence Laboratory (LCDIA). Doctorate in Engineering (RENNES 1) – France. ORCID: https://orcid.org/0000-0002-4331-6588. E-mail: luciano.gallegos@unifor.br

criptografia de difícil aprendizado, mas todos foram capazes de praticar e aprender pelo menos uma das técnicas criptográficas ensinadas.

***PALAVRAS-CHAVE**: Prática. Ensino. Aprendizagem. Criptografia.*

***RESUMEN**: La criptografía está presente en varias operaciones que realizan diariamente las personas, como la compra online o en el desarrollo de diálogos utilizando equipos informáticos e Internet como medio. Aunque la criptografía es muy importante en el contexto contemporáneo, la enseñanza del tema es nueva para los estudiantes de la escuela secundaria profesional. En este sentido, uno de los mayores desafíos es motivar a los estudiantes a utilizar métodos criptográficos en aula. El objetivo de este trabajo es de investigar el uso y aprendizaje de la criptografía por parte de estudiantes de bachillerato professional. Por eso, se utilizó la metodología tipo Survey con preguntas de autoevaluación sobre motivación, comprensión y uso de herramientas computacionales que contienen conceptos básicos de criptografía. El análisis de las respuestas sugiere que la mayoría de los estudiantes encuentran la criptografía difícil de aprender, pero todos pudieron practicar y aprender al menos una de las técnicas criptográficas enseñadas.*

***PALABRAS CLAVE**: Prácticas. Enseñando. Aprendizaje. Criptografía.*

Introduction

The Internet has revolutionized our society, allowing access to information, on a large scale, and to technological resources that offer great opportunities for business and services (LAUDON; LAUDON, 2014). The activities carried out range from shopping and banking operations to virtual information services. In this heterogeneous and dynamic scenario, information security must allow users to safeguard the services offered involving personal, professional and financial data. In this aspect, cryptography is one of the main mechanisms in use in digital applications, used by individuals and companies to protect information, whether in communication or data storage (CERT, 2012).

Although cryptography can be widely explored in disciplines involving information security for data protection, research in the field of education indicates that students are not motivated in this topic, mainly due to the limited number of class hours, mathematical difficulties and the lack of tools to get practice in cryptography (SONG; DENG, 2009; OLEJAR; STANEK, 1999).

In view of this scenario, this article proposes to investigate the use and learning of cryptography by high school students as a means of realizing the theoretical and practical knowledge of the subject of Information Management and Security of the Federal Institute of Education, Science and Technology of São Paulo (IFSP) – Campus Campinas during the first

semester of 2019. The approach proposed in this research is based on the complementarity of the pedagogical practices of seminars and collaborative practical classes. It is expected that the seminars allow the exhibition of the work developed by the students, counting on the teacher's reflections and constructive debate among the students themselves. According to Masseto (2012), the pedagogical practice of seminars is a very rich learning technique that allows the student to develop their research capacity, knowledge production, communication, organization and foundation of ideas, and the preparation of a research report, collectively.

Practical activities are added to the seminars to help reduce the existence of mechanical classes. Therefore, the proper use of computer technologies combined with collaborative practice can help in the teaching and learning processes, stressing, however, that success in mediated tasks depends on the exchange between participants about learning, going beyond the mere use of technology for the exchange of ideas, experiences and acquired knowledge (GIANOTTO; DINIZ, 2010).

In this work, the Survey methodology was used through self-evaluation questionnaires that aim to obtain information about the use, motivation and learning of cryptography by students, organized in four sections. In the subsequent Sections: in 2, the theoretical foundation is presented, highlighting the theme of cryptography. Section 3 describes the methodological aspects for the formation of work groups, the activities carried out in the classroom, and the process to be followed for the use of cryptography by students. Section 4 presents the qualitative analysis of cryptography learning by high school students. And in Section 5 the final discussions are detailed.

Encryption Basics

Encryption is defined as a set of techniques that make it possible to make incomprehensible a message originally written with clarity, so that only the recipient can decipher and understand it (LAUDON; LAUDON, 2014). Although modern cryptography can be applied to several areas of human knowledge, the concept is the same as its origin: guaranteeing secure communication in an insecure environment (BELLARE; ROGAWAEY, 2005).

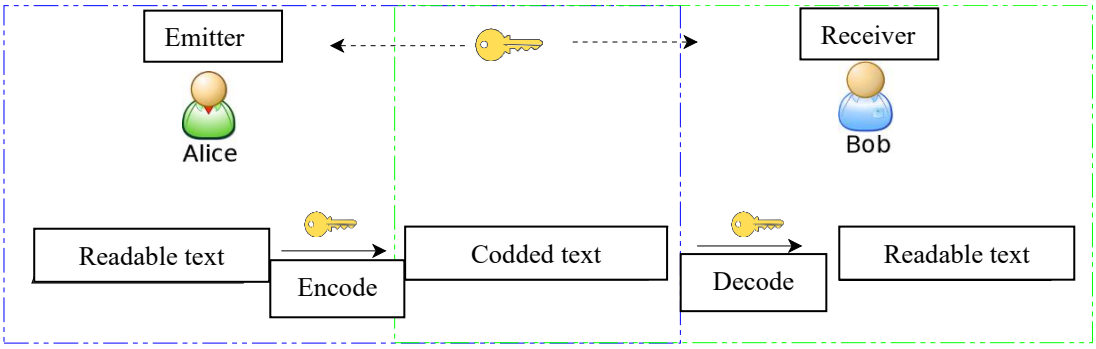
In the field of computer science and information technology, the cryptographic algorithm is a mathematical function applied to information, to perform the encryption and decryption of data. While the encryption process consists of transforming readable data into unreadable data, the decryption process performs the opposite process. These processes are

based on the use of access keys that interact with cryptographic algorithms. Access keys have different sizes and their degree of security is associated with their bit length. According to the Brazilian Association of Technical Standards - ABNT (2013), cryptography can be used to achieve various information security objectives, mainly:

- Confidentiality: ensuring that a message is read only by the authorized recipient;
- Integrity: ensure that a message has not been altered;
- Availability: ensuring that information and services will be available to authorized users when necessary;
- Authenticity: ensuring that the message received actually originated from a sender who is in fact who it claims to be, verifiable and trustworthy.

There are two types of information security cryptography in use: symmetric cryptography and asymmetric cryptography. Symmetric cryptography, or secret key, is the one in which the sender and the receiver of the messages use the same key for the processes of encrypting and/or decrypting. In this process, a message is encrypted at the sender by applying an encryption algorithm, using the key as a parameter. Symmetric encryption results in a set of data, which is known as ciphertext. The decryption process, in turn, occurs through the application of the same encryption algorithm by the receiver, having as a parameter the same key used by the sender in the encryption, as illustrated in Figure 1. The security of these algorithms is based entirely on the key used, and not in technical details of the algorithms (BELLARE; ROGAWAEY, 2005). Some important algorithms for symmetric encryption are: *Data Encryption Standard* – DES; *TripleDES*; and *Advanced Encryption Standard* – AES (BASTA; BASTA; BROWN, 2014).

FigurE 1 – Symmetric encryption

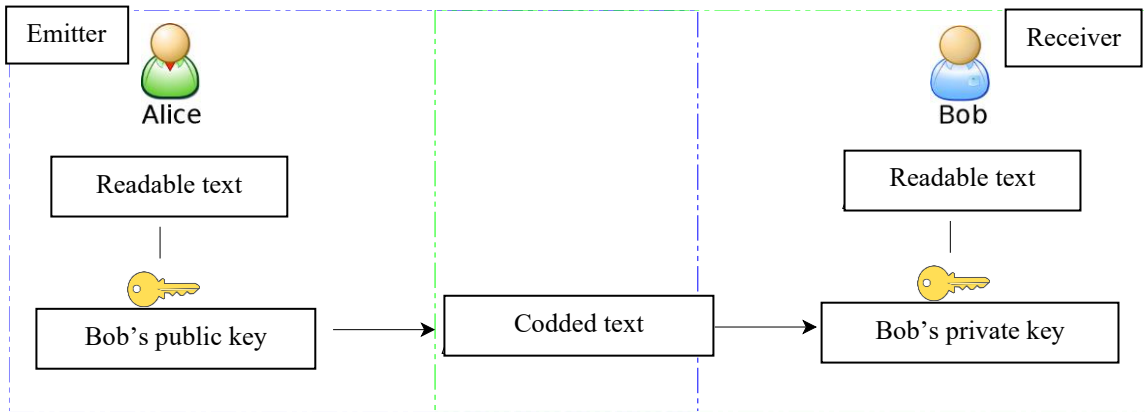


Source: Devised by the authors (2017)

Asymmetric cryptography, unlike symmetric cryptography, is a cryptographic technique that uses a pair of keys for each interlocutor: one key called public and the other key called private. The public key is freely distributed to all correspondents with whom one wants to maintain communication. The private key, in turn, must be kept confidential and known only by its owner. Figure 2 demonstrates how asymmetric cryptography works, in which a message encrypted with the public key can only be decrypted by the corresponding private key. Likewise, a message encrypted with the private key can only be decrypted by its corresponding public key. The main features of asymmetric encryption are:

- The public key is generated from the private key;
- It is computationally impossible to generate the private key from the public key;
- Key management is potentially simpler than systems based on symmetric keys;
- The most classic algorithms employed in asymmetric key cryptography are *Rivest, Shamir e Adleman - RSA, ElGamal, Data Encryption Standard - DES* (BASTA; BASTA; BROWN, 2014);
- The size of cryptographic keys considered secure against attacks is at least 1024 bits and;
- It has the advantage of not having a shared key for each person in a group, drastically reducing the overall number of keys needed when communicating for groups with more than three individuals. However, each user must share a public key and not disclose their private one.

Figure 2 – Asymmetric encryption



Source: Devised by the authors (2017)

The use of an asymmetric encryption algorithm allows the creation of a digital signature. The digital signature guarantees the authenticity of the message. The way to sign a

message is to encrypt it with the private key. That way, anyone who has the public key knows that the message was actually sent by the sender. The three common digital signature algorithms are *Digital Signature Algorithm* (DSA), *Rivest-Shamir-Adleman* (RSA) and *Elliptic Curve Digital Signature Algorithm* (ECDSA).

However, there is the possibility of creating signed random messages using only the public key of an issuer. To avoid this problem, the hash function was created. Hash is a unidirectional mathematical function that is relatively easy to calculate, but quite difficult to reverse.

There are many modern hashing algorithms widely used today. Two of the most popular are MD5 and SHA 256. So, to sign a message, you first create its hash, then the message is sent along with an attachment, which is the output of the hash function encrypted with the sender's private key. The receiver, upon receiving the message, hash and decrypts the signature using the sender's public key. If the value is the same as that obtained from the hash of the received message, we have the authenticated sender.

Methodological procedures

Currently, it is essential to prepare students to work and manipulate digital technologies. In this context, the methodological procedures used in the work with the students were based on two pedagogical practices: classroom seminars and practical classes.

The seminars aim to develop in students competences for reflection, discussion and debate on themes that are often considered complex, stimulating research, argumentation and the sharing of information between students and teachers. This type of practice involves two important activities that are research and creation. Gessinger (2008) defines research as the execution of written reports on a certain topic and creation as the development of content, such as models, experiments, knowledge, etc.

The practical classes are intended for pedagogical work in groups to bring teaching and learning closer together and involve two important activities: debate and presentation. While the debate consists of a discussion between one or more groups involving different points of view, a presentation consists of an oral dissertation on a certain topic through methods such as posters and slides (GESSINGER, 2008).

The seminars and practical classes were conducted in the technical course in information technology in the modalities concomitant/subsequent to high school at the Federal Institute of Education, Science and Technology of São Paulo - IFSP, Campus

Campinas, in the subject of Information Management and Security, during the first semester of 2019. The group of students consisted of seven women and 10 men. Regarding age, 16 students are between 15 and 20 years old, and one student is between 45 and 50 years old. It is noteworthy that this article is the result of a research developed in the Specialization Postgraduate Program – Pedagogical Formation for Unlicensed Graduates of the Paula Souza Center, in São Paulo, during 2019, with the due approval of the IFSP, as well as of all the participants.

Seminar

The seminar activity in the class aimed to assist students in the process of classifying the main types of cryptography. Traditional encryption aimed to study the algorithms of substitution ciphers (letters are replaced), transposition (letters are rearranged) and one-time cipher (clear text, combined with a secret key, creates a new character that is combined with the clear text to generate the encoded text). The classification regarding modern cryptography, on the other hand, contemplates symmetric and asymmetric algorithms using block ciphers and stream ciphers. The execution of the seminars was conducted according to the following work schedule and guidelines contained in Table 1.

Table 1 – Execution of seminars

Period	Seminars
First week (28/03/2019)	Considering that the classroom has the proper characteristics for the establishment of group tasks (SILVA *et al*., 2017), students were organized into small groups regarding the historical context and the functioning of cryptographic techniques. Each group chose a cryptography topic to investigate. Afterwards, the groups were instructed to reflect on the practical use of the types of cryptography, with examples that are simple to understand. The various materials obtained consisted of texts taken from books, magazines and Internet pages.
Second week (04/04/2019)	"First Seminar", in which part of the students presented and delivered reports on the historical or classical context of the development of cryptography. For example, the students who chose the theme 'replacement cipher' noted that this was used by the Hebrews between 500 and 600 BC and had importance in the communications of the Roman Empire (Cesar's cipher, 100-44 BC), especially when few people at the time they knew how to read (ALVARENGA, 2017).
Third week (09/04/2019)	"Second Seminar", aimed at the presentation and delivery of reports, by the groups on modern cryptography. In this seminar, students explained the bases for the calculation of modular arithmetic for the operation and development of cryptographic techniques, as well as understanding their application in electronic transactions

Source: Devised by the authors (2021)

In this way, an approach was applied to bring teaching and learning closer together, expanding the involvement with the content of the discipline, stimulating the cognitive and social development of students who, in turn, satisfactorily achieved the objectives of exercise and knowledge absorption, working collaboratively and showing interest in carrying out the proposed activities.

Practical classes

Currently, the types of encryption used are symmetric and asymmetric (STALLINGS, 2015). Thus, the activities carried out in practical classes consisted of stimulating the development of learning about software for symmetric and asymmetric cryptography, through experimentation and practices in laboratories.

Students were divided into groups and instructed to read the practical guides for using the software. Thus, the success in tasks mediated by the software implies an emphasis on the exchange among participants about learning through information technology resources. The execution was conducted according to the following work schedule and guidelines contained in Table 2.

Table 2 – Execution of practical activities

Period	Practical Activities
First week (23/05/2019)	In the first practical activity, the groups used the practical guide to the *VeraCrypt* symmetric encryption software, with 12 pages, describing the download sites, installation and use of cryptographic algorithms and hash functions (VERACRYPT, 2018). *VeraCrypt* arose from the need to keep information encrypted on hard disks for long periods. Its strength lies in the creation and use of files as virtual volumes (drives or disks) to encrypt entire hard disk or pen-drive partitions, protecting all files contained in the virtual volume. As for the size of the key, it varies according to the set of selected algorithms. Using the software, the students created a file and mounted a virtual volume for display on the file manager's drive. With the end of the work, the students dismantled the entire process carried out.
Second week (06/06/2019)	In the second practical activity, the groups used the *Open Pretty Good Privacy* - Open PGP practical guide, using the *Gnu Privacy Guard* - GPG software, which is free and open source (OPENPGP, 2018). The seven-page how-to guide to GPG software and its likes describes download sites, installing browser plugins, generating public keys, and managing keys for secure emailing. The OpenPGP standard is defined by *Request for Comments* – RFC 4880 (FINNEY et al., 2007). RFC 4880 uses asymmetric cryptography and an appropriately characteristic private key to provide secure electronic communication service. It is important to emphasize that some students used other asymmetric software due to prior knowledge of the subject. Asymmetric cryptography uses the concept of public keys, which are distributed to people

	with whom you want to exchange data or messages, and the private key is on your machine (or preferably cryptographic token or SmartCard) and should not be distributed.

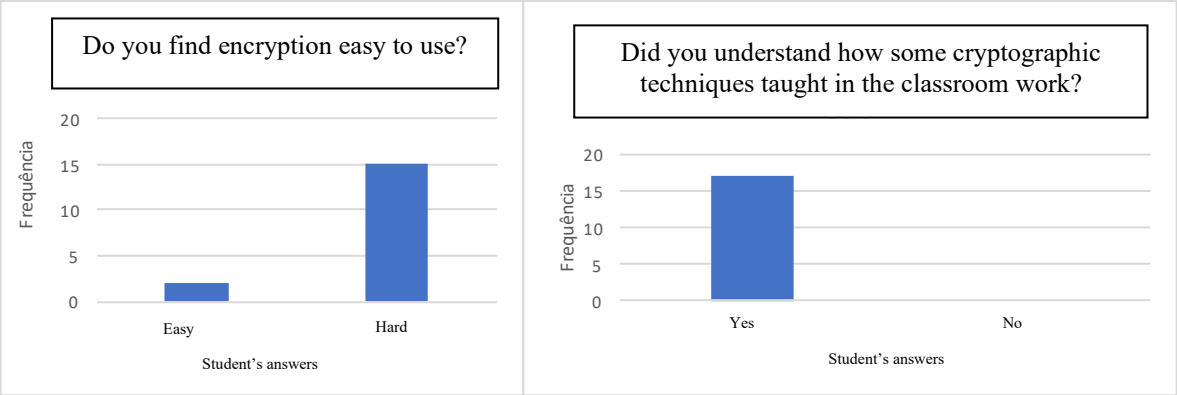
Source: Devised by the authors (2021)

Analysis of results

Aiming to evaluate the learning of the proposed pedagogical practices, two self-evaluative questionnaires were elaborated for students on Google Forms. The first questionnaire is about the theoretical knowledge of cryptography studied in the seminars. The second questionnaire is about the use of cryptographic software used in practical classes. The questionnaires were answered by 17 students, with 10 students claiming to have some prior knowledge about cryptography and the other seven students claiming not to know the subject. The results of the qualitative analyzes are shown graphically below.

Ease of use and learning how encryption works is shown in the graphs in Figure 3. The graph on the left shows that most students find encryption difficult (15 students), only two students find it easy to use. However, the graph on the right indicates that all (17 students) claim to have learned the operation of at least one cryptographic technique taught in the classroom.

Figure 3 – Student Opinions on Ease of Use and Learning Encryption

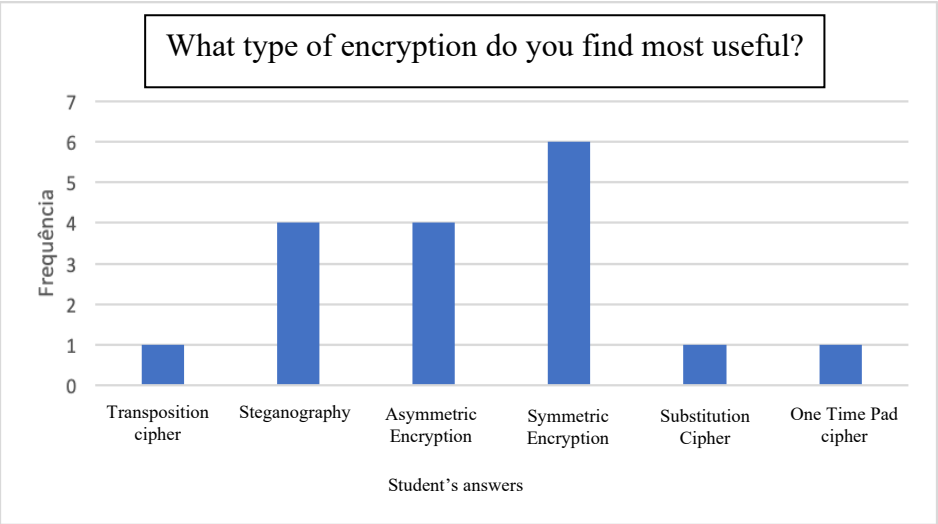


Source: Research results (2019)

The usefulness of the cryptography type is shown in Figure 4. It is observed that symmetric cryptography is considered the most useful by most students (six students), followed by asymmetric cryptography (four students) and steganography (four students). Note that classic encryption types were considered less useful: only one student chose the transpose cipher, one student the replacement cipher, and one student the one time pad cipher. The

results suggest that students understood the importance of modern computer-mediated cryptography and its everyday applications.

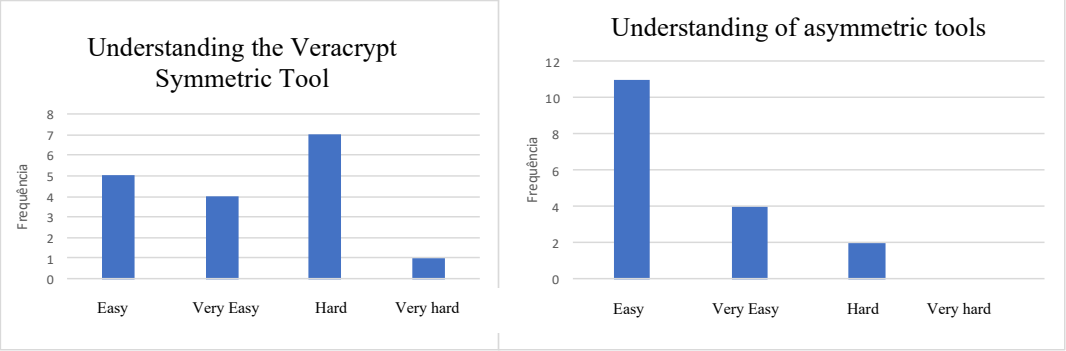
Figure 4 – Students' Opinions on the Usefulness of the Encryption Type



Source: Research results (2019)

The understanding of the cryptographic tools used in laboratory practical classes is presented in the graphs in Figure 5. The graph on the left indicates that most students find the VeraCrypt tool difficult to use for the purpose of encrypting files on disk. The graph on the right shows that asymmetric cryptography was considered easy to use, even though it was necessary to understand the generation and distribution of cryptographic keys to send secure email. This result in relation to asymmetric tools can be explained by the fact that some students have previous knowledge about other asymmetric software, which were allowed in the activity. In this way, students who already knew the subject deepened and updated their concepts, as well as helped other students, who were not familiar with asymmetric cryptography, in the acquisition of new knowledge.

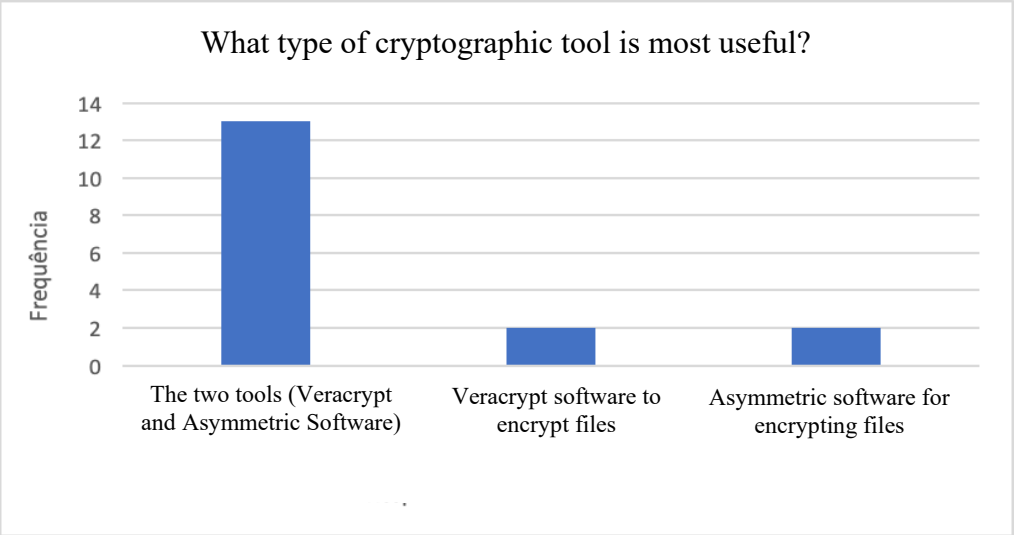
Figure 5 - Student Opinions on Understanding Disk File Encryption and Secure Email Sending



Source: Devised by the authors

The importance of both cryptographic tools used in laboratory practical classes is shown in Figure 6, reinforcing that the majority (13 students) consider both tools important. Thus, it appears that students understood the different purposes of the types of modern cryptography taught. The results also indicate that only two students consider that the most important thing in cryptography is to encrypt files on disk with the VeraCrypt tool. In contrast, and in the same proportion, two other students consider that the most important thing in cryptography is to send secure email with some asymmetric software.

Figure 6 – Students' opinions on the importance of the cryptographic tools taught



Source: Research results (2019)

The answers obtained showed that the understanding of these scientific-technological foundations of security, in information processes on the subject of cryptography, should be motivating and contextualized in terms of theoretical concepts and practical applications.

Final considerations

In this article, the concepts of information security, cryptography and its use for high school students were presented. Specifically, emphasis was placed on cryptography as it is an important foundation for today's society. The encryption tools presented to the students, together with their usage guides, allow them to work with data and message encryption, ensuring the confidentiality of information.

As cryptography is present in different equipment, whether they are fixed or mobile electronic computing devices, the involvement of students in carrying out the activities was

notorious, as well as the concentration required for its understanding. The two pedagogical practices carried out, seminar and practical classes, were well received, despite the different degrees of involvement and participation of students. The seminars explored the historical part, so that the student can understand that cryptology arises out of necessity and develops as technology advances. The practical classes allowed to apply the subjects already worked in the theoretical aspect, with software widely used in the labor market.

Through the general analysis of the questions in the questionnaires, it can be concluded that the pedagogical practices used were effective for the construction of students' knowledge about cryptography, everyone could learn at least one cryptographic technique taught. It is noteworthy, however, that some students find it difficult to use encryption tools, probably due to the complexity of the subject and the reduced time for teaching cryptography.

ACKNOWLEDGMENTS: The authors are grateful to: Federal Institute of Education, Science and Technology of Goiás (IF Goiano); and to the Federal Institute of Education, Science and Technology of São Paulo (IFSP), for the support they provided during the research that made this research possible.

REFERENCES

ABNT – ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27001**: Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação - Requisitos. Rio de Janeiro, RJ: ABNT, 2013.

ALVARENGA, L. G. **Criptografia clássica e moderna**. Clube de Autores, 2017.

BASTA, A.; BASTA, N.; BROWN, M. **Segurança de computadores e teste de invasão**. São Paulo, SP: Cengage Learning, 2014.

BELLARE, M.; ROGAWAEY, P. **Introduction to modern cryptography**. Davis, United States of America: University of California at Davis, 2005. Available: https://web.cs.ucdavis.edu/~rogaway/classes/227/spring05/book/main.pdf. Access: 06 Feb. 2019.

CERT – CENTRO DE ESTUDOS E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL. **Cartilha de Segurança para Internet versão 4.0**. São Paulo, SP: Comitê Gestor da Internet no Brasil, 2012. Available: https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf. Access: Access: 04 Apr. 2019.

FINNEY, H. *et al*. OpenPGP Message Format. **RFC 4880**. 2007. Available: https://datatracker.ietf.org/doc/html/rfc4880. Access: 23 May 2019.

GESSINGER, R. M. Atividade em grupo. *In*: GRILLO, M. C. *et al*. **A Gestão da Aula Universitária na PUCRS**. Porto Alegre, RS: EdiPUCRS, 2008. p. 109-118.

GIANOTTO, D. E. P.; DINIZ, R. E. S. Formação inicial de professores de biologia: a metodologia colaborativa mediada pelo computador e a aprendizagem para a docência. **Revista Ciência & Educação**, v. 16, n. 3, p. 631–648, 2010. Available: http://www.scielo.br/j/ciedu/a/m8BHLB9MbCb5zYhxKsVvcsk/abstract/?lang=pt. Access: 06 June 2019.

LAUDON, K.; LAUDON, J. **Sistemas de informações gerenciais**. São Paulo, SP: Pearson Prentice Hall, 2014.

MASSETO, M. T. **Competências pedagógicas do professor universitário**. São Paulo, SP: Summus Editora, 2012.

OLEJAR, D.; STANEK, M. Some aspects of cryptology teaching. *In*: **IFIP WG 11.8 1st World Conference on Information Security Education WISE1**. 1999. p. 1-9. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.21.4050&rep=rep1&type=pdf. Access: 06 Aug. 2019.

OPENPGP. **OpenPGP**. 2018. Available: https://www.openpgp.org. Access: 20 May 2019.

SILVA, V. *et al*. Mineração de dados utilizando análise de redes social para identificar tendências de participação em aulas presenciais. *In*: BRAZILIAN SYMPOSIUM ON COMPUTERS IN EDUCATION, 28., 2017, Recife. **Anais** […]. Recife, PE, 2017. p. 1467-1476. Available: https://br-ie.org/pub/index.php/sbie/article/view/7677. Access: 30 Sep. 2020.

SONG, X.; DENG, H. Taking flexible and diverse approaches to get undergraduate students interested in cryptography course. *In*: **First International Workshop on Education Technology and Computer Science**. 2009. v. 2, p. 490-494. Available: https://ieeexplore.ieee.org/document/4959085. Access: 09 Apr. 2019.

STALLINGS, W. **Criptografia e segurança de redes**: princípios e práticas. 6. ed. São Paulo, SP: Pearson Education do Brasil, 2015. 578 p.

VERACRYPT. **Veracrypt**: versão 1.18 de 2018. Available: https://www.veracrypt.fr/en/Home.html. Access: 20 May 2019.

How to reference this article

MARIN, R. P. M.; SOUZA, J. G. S.; MARIN, L. H. G. Teaching basic concepts of cryptography in professional high school. **Revista on line de Política e Gestão Educacional**, Araraquara, v. 25, n. 2, p. 1277-1290, May/Aug. 2021. e-ISSN:1519-9029. DOI: https://doi.org/10.22633/rpge.v25i2.14469

Submitted: 17/11/2020
Required revisions: 14/05/2021
Approved: 31/05/2021
Published: 01/08/2021