ENSINANDO CONCEITOS BÁSICOS DE CRIPTOGRAFIA NO ENSINO MÉDIO PROFISSIONAL

ENSEÑANDO CONCEPTOS BÁSICOS DE CRIPTOGRAFÍA EN LA ESCUELA SECUNDARIA PROFESIONAL

TEACHING BASIC CONCEPTS OF CRYPTOGRAPHY IN PROFESSIONAL HIGH SCHOOL

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

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 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*

[1] Instituto Federal de Educação, Ciência e Tecnologia Goiano (IF GOIANO), Urutaí – GO – Brasil. Professora no curso de Informática. Doutorado em Ciência da Computação (CENTRALESUPÉLEC) – França. ORCID: https://orcid.org/0000-0002-1303-052X. E-mail: regina.marin@ifgoiano.edu.br
[2] Instituto Federal de Educação, Ciência e Tecnologia de São Paulo (IFSP), Campinas – SP – Brasil. Docente no Curso de Informática. Doutorando em Educação Escolar (UNESP). ORCID: https://orcid.org/0000-0003-4952-8618. E-mail: jackson@ifsp.edu.br
[3] Universidade de Fortaleza (UNIFOR), Fortaleza – CE – Brasil. Professor do Laboratório de Ciências de Dados e Inteligência Artificial (LCDIA). Doutorado em Engenharia (RENNES 1) – França. ORCID: https://orcid.org/0000-0002-4331-6588. E-mail: luciano.gallegos@unifor.br

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.*

***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.*

Introdução

A Internet revolucionou a nossa sociedade, permitindo acesso à informação, em grande escala, e a recursos tecnológicos que oferecem grandes oportunidades de negócios e serviços (LAUDON; LAUDON, 2014). As atividades realizadas vão desde compras e operações bancárias até serviços virtuais de informações. Neste cenário, heterogêneo e dinâmico, a segurança da informação deve permitir a salvaguarda dos usuários quanto aos serviços ofertados envolvendo dados pessoais, profissionais e financeiros. Neste aspecto, a criptografia é um dos principais mecanismos em uso nas aplicações digitais, utilizada por indivíduos e empresas para a proteção das informações, seja na comunicação ou no armazenamento de dados (CERT, 2012).

Embora a criptografia possa ser largamente explorada em disciplinas envolvendo a segurança da informação para proteção de dados, pesquisas na área da educação indicam que os alunos não se sentem motivados neste tema devido, principalmente, ao número limitado de horas de aula, dificuldades matemáticas e a falta de ferramentas para obter prática na criptografia (SONG; DENG, 2009; OLEJAR; STANEK, 1999).

Diante deste cenário, propõe-se neste artigo investigar o uso e a aprendizagem da criptografia por alunos do ensino médio profissional como meio de concretizar os saberes teóricos e práticos da disciplina de Gerenciamento e Segurança da Informação do Instituto

Federal de Educação, Ciência e Tecnologia de São Paulo (IFSP) – Campus Campinas durante o primeiro semestre de 2019. A abordagem proposta nesta pesquisa baseia-se na complementaridade das práticas pedagógicas de seminários e das aulas práticas colaborativas. Espera-se que os seminários permitam a exposição dos trabalhos desenvolvidos pelos escolares, contando com as ponderações do professor e do debate construtivo entre os próprios alunos. Segundo Masseto (2012), a prática pedagógica dos seminários é uma técnica riquíssima de aprendizagem que permite ao estudante desenvolver sua capacidade de pesquisa, de produção de conhecimento, de comunicação, de organização e fundamentação de ideias, e de elaboração de relatório de pesquisa, de forma coletiva.

Acrescenta-se aos seminários as atividades práticas para ajudar a diminuir a existência de aulas mecânicas. Para tanto, o uso adequado das tecnologias computacionais aliada à prática colaborativa pode auxiliar nos processos de ensino e aprendizagem ressaltando-se, porém, que o êxito nas tarefas mediadas depende da troca entre os participantes acerca do aprendizado, indo além da mera utilização da tecnologia para a troca de ideias, experiências e conhecimentos adquiridos (GIANOTTO; DINIZ, 2010).

Neste trabalho foi utilizada a metodologia *Survey* através de questionários autoavaliativos que visam obter informações quanto ao uso, motivação e aprendizagem da criptografia pelos alunos, organizado em quatro seções. Nas Seções subsequentes: na 2 é apresentada a fundamentação teórica, destacando-se o tema criptografia. Na Seção 3 são descritos os aspectos metodológicos para a formação de grupos de trabalho, as atividades realizadas em sala de aula, e o processo a ser seguido para a utilização da criptografia pelos alunos. A Seção 4 apresenta a análise qualitativa da aprendizagem da criptografia por alunos do ensino médio profissional. E na Seção 5 as discussões finais são pormenorizadas.

Conceitos básicos de criptografia

A criptografia é definida como um conjunto de técnicas que permitem tornar incompreensível uma mensagem originalmente escrita com clareza, de forma a permitir que apenas o destinatário a decifre e compreenda (LAUDON; LAUDON, 2014). Embora a criptografia moderna possa ser aplicada a diversas áreas do conhecimento humano, o conceito é o mesmo de sua origem: garantir a comunicação segura em um meio inseguro (BELLARE; ROGAWAEY, 2005).

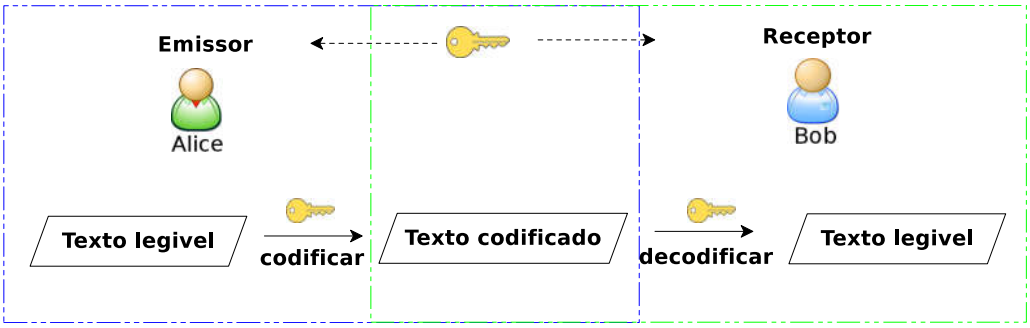
Na área das ciências da computação e da tecnologia da informação, o algoritmo criptográfico é uma função matemática aplicada à informação, para realizar a cifragem e a

decifragem dos dados. Enquanto o processo de cifrar consiste em transformar dados legíveis em ilegíveis, o processo de decifragem realiza o processo oposto. Estes processos estão baseados na utilização de chaves de acesso que interagem com os algoritmos criptográficos. As chaves de acesso possuem diferentes tamanhos e seu grau de segurança está associado com sua extensão em *bits*. Segundo a Associação Brasileira de Normas Técnicas – ABNT (2013), a criptografia pode ser utilizada para alcançar diversos objetivos de segurança da informação, principalmente:

- Confidencialidade: garantir que uma mensagem seja lida apenas pelo receptor autorizado;
- Integridade: garantir que uma mensagem não tenha sido alterada;
- Disponibilidade: garantir que a informação e os serviços estarão disponíveis para os usuários autorizados, quando necessário;
- Autenticidade: garantir que a mensagem recebida realmente originou-se de um emissor que de fato é quem alega ser podendo ser verificado e confiável.

Existem dois tipos de criptografia para segurança da informação em uso: a criptografia simétrica e a criptografia assimétrica. A criptografia simétrica, ou chave secreta, é aquele na qual o emissor e o receptor das mensagens utilizam a mesma chave para os processos de cifrar e/ou decifrar. Neste processo, uma mensagem é cifrada no emissor por meio da aplicação de um algoritmo de criptografia, tendo a chave como parâmetro. A criptografia simétrica resulta em um conjunto de dados, que se conhece como texto cifrado. O processo de decifrar, por sua vez, ocorre por intermédio da aplicação do mesmo algoritmo de criptografia pelo receptor, tendo como parâmetro a mesma chave utilizada pelo emissor na cifra, conforme é ilustrado na Figura 1. A segurança desses algoritmos é baseada inteiramente na chave utilizada, e não em detalhes técnicos dos algoritmos (BELLARE; ROGAWAEY, 2005). Alguns algoritmos importantes para a criptografia simétrica são: *Data Encryption Standard* – DES; *TripleDES*; e *Advanced Encryption Standard* – AES (BASTA; BASTA; BROWN, 2014).

Figura 1 – Criptografia simétrica

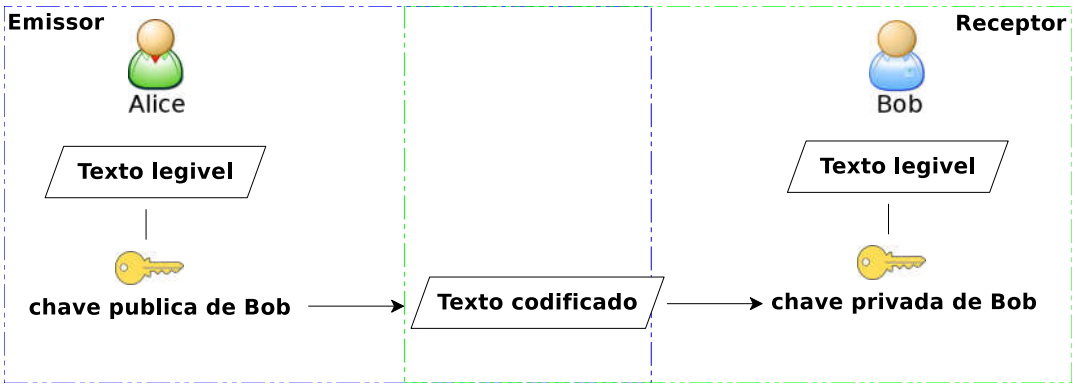


Fonte: Elaborado pelos autores (2017)

A criptografia assimétrica, diferentemente da simétrica, é uma técnica criptográfica que utiliza um par de chaves para cada interlocutor: uma chave chamada de pública e a outra chave chamada de privada. A chave pública é distribuída livremente para todos os correspondentes com os quais se quer manter comunicação. A chave privada, por sua vez, deve ser mantida confidencial e conhecida apenas pelo seu dono. A Figura 2 demonstra o funcionamento da criptografia assimétrica, em que uma mensagem cifrada com a chave pública pode somente ser decifrada pela chave privada correspondente. Do mesmo modo, uma mensagem cifrada com a chave privada pode somente ser decifrada pela sua chave pública correspondente. As principais características da criptografia assimétrica são:

- A chave pública é gerada a partir da chave privada;
- É computacionalmente impossível gerar a chave privada, a partir da chave pública;
- O gerenciamento de chaves é potencialmente mais simples do que nos sistemas baseados em chaves simétricas;
- Os algoritmos mais clássicos empregados em criptográfica de chaves assimétricas são *Rivest, Shamir e Adleman - RSA, ElGamal, Data Encryption Standard - DES* (BASTA; BASTA; BROWN, 2014);
- O tamanho de chaves criptográficas consideradas seguras contra ataques é de no mínimo 1024 *bits* e;
- Possui a vantagem de não precisar haver uma chave compartilhada para cada pessoa em um grupo, reduzindo drasticamente o número global de chaves necessárias na comunicação de grupos com mais de três indivíduos. Porém, cada usuário precisa compartilhar uma chave pública e não divulgar a sua privada.

Figura 2 – Criptografia assimétrica



Fonte: Elaborado pelos autores (2017)

O uso de um algoritmo de criptografia assimétrica permite a criação de uma assinatura digital. A assinatura digital garante a autenticidade da mensagem. A forma de assinar uma mensagem é criptografando-a com a chave privada. Assim, qualquer pessoa que possua a chave pública sabe que a mensagem foi realmente enviada pelo emissor. Os três algoritmos comuns de assinatura digital são Algoritmo de Assinatura Digital (DSA), *Rivest-Shamir-Adleman* (RSA) e *Algoritmo de Assinatura Digital Elliptic Curve* (ECDSA).

Contudo existe a possibilidade da criação de mensagens aleatórias assinadas usando somente a chave pública de um emissor. Para evitar este problema, criou-se a função *hash*. O *Hash* é uma função matemática unidirecional relativamente fácil de calcular, mas bastante difícil de reverter.

Há muitos algoritmos *hash* modernos amplamente usados atualmente. Dois dos mais populares são MD5 e SHA 256. Assim, para assinar uma mensagem, inicialmente cria-se seu *hash*, então a mensagem é enviada juntamente com um anexo, que é a saída da função *hash* criptografada com a chave privada do emissor. O receptor, ao receber a mensagem faz a *hash* e decripta a assinatura usando a chave pública do emissor. Caso o valor seja o mesmo que o obtido na *hash* da mensagem recebida, temos o emissor autenticado.

Procedimentos metodológicos

Na atualidade, é fundamental preparar os discentes para trabalharem e manipularem as tecnologias digitais. Nesse contexto, os procedimentos metodológicos utilizados no trabalho com os alunos foram baseados em duas práticas pedagógicas: seminários em sala e aulas práticas.

Os seminários objetivam desenvolver nos alunos competências para a reflexão, discussão e debate de temas muitas vezes considerados complexos, estimulando a pesquisa, a argumentação e o compartilhamento de informações entre os alunos e professores. Este tipo de prática envolve duas atividades importantes que são pesquisa e criação. Gessinger (2008) define pesquisa como a execução de relatórios escritos sobre determinado tema e criação como a elaboração de conteúdo, como maquetes, experimentos, conhecimentos etc.

As aulas práticas têm como propósito o trabalho pedagógico em grupos para a aproximação entre ensino e aprendizagem e envolve duas atividades importantes: o debate e a apresentação. Enquanto o debate consiste na discussão entre um ou mais grupos envolvendo diferentes pontos de vista, uma apresentação consiste em uma dissertação oral sobre determinado tema através de métodos como cartazes e slides (GESSINGER, 2008).

Os seminários e as aulas práticas foram conduzidos no curso técnico em informática nas modalidades concomitante/subsequente ao ensino médio do Instituto Federal de Educação, Ciência e Tecnologia de São Paulo – IFSP, Campus Campinas, na disciplina de Gerenciamento e Segurança da Informação, durante o primeiro semestre de 2019. O grupo de alunos consistia em sete mulheres e 10 homens. Em relação à faixa etária, 16 alunos estão entre 15 até 20 anos, e um aluno entre 45 até 50 anos. Ressalta-se este artigo é resultado de uma pesquisa desenvolvida no Programa de Pós-Graduação Especialização – Formação Pedagógica Para Graduados Não Licenciados do Centro Paula Souza, em São Paulo durante o ano de 2019, com a devida aprovação do IFSP, bem como de todos os participantes.

Seminário na classe

A atividade de seminário na classe teve como principal objetivo auxiliar os alunos no processo de classificação dos principais tipos de criptografia. A criptografia tradicional visou o estudo dos algoritmos de cifras de substituição (as letras são substituídas), transposição (as letras são reorganizadas) e cifra de uso único (texto claro, combinado com uma chave secreta, cria um novo caractere que é combinado com o texto claro para gerar o texto codificado). Já a classificação quanto à criptografia moderna contempla algoritmos simétricos e assimétricos utilizando as cifras de bloco e cifras de fluxos. A execução dos seminários foi conduzida conforme o seguinte cronograma de trabalho e orientações contidas no Quadro 1.

Quadro 1 – Execução dos seminários

Período	Seminários
Primeira semana (28/03/2019)	Tendo em vista que a sala de aula reúne as características propícias para o estabelecimento de tarefas em grupo (SILVA *et al.*, 2017), os alunos foram organizados em grupos pequenos quanto ao contexto histórico e o funcionamento das técnicas criptográficas. Cada grupo escolheu um tema de criptografia a ser investigado. Na sequência os grupos foram orientados a refletirem sobre a utilização prática dos tipos de criptografia, com exemplos de simples compreensão. Os diversos materiais obtidos consistiram em textos retirados de livros, revistas e páginas da Internet.
Segunda semana (04/04/2019)	"Primeiro Seminário", em que parte dos alunos apresentou e entregou relatórios sobre o contexto histórico ou clássico do desenvolvimento da criptografia. Por exemplo, os alunos que escolheram o tema 'cifra de substituição', observaram que esta foi utilizada pelos hebreus entre 500 e 600 a.C. e teve importância nas comunicações do império romano (cifra de césar, 100-44 a.C.), principalmente quando poucas pessoas na época sabiam ler (ALVARENGA, 2017).
Terceira semana (09/04/2019)	"Segundo Seminário", objetivando a apresentação e entrega de relatórios, pelos grupos sobre a criptografia moderna. Neste seminário os alunos explicitaram as bases para os cálculos da aritmética modular para o funcionamento e desenvolvimento das técnicas criptográficas, bem como entender a aplicação em transações eletrônicas

Fonte: Elaborado pelos autores (2021)

Desta forma, aplicou-se uma abordagem para aproximar o ensino da aprendizagem, ampliando o envolvimento com o conteúdo da disciplina, estimulando o desenvolvimento cognitivo e social dos alunos que, por sua vez, alcançaram de forma satisfatória os objetivos de exercício e absorção de conhecimentos, trabalhando de forma colaborativa e demonstrando interesse na execução das atividades propostas.

Aulas práticas

Atualmente, os tipos de criptografia utilizados são as simétricas e assimétricas (STALLINGS, 2015). Dessa forma, as atividades realizadas nas aulas práticas consistiram em estimular o desenvolvimento da aprendizagem sobre os *softwares* para a criptografia simétrica e assimétrica, por meio de experimentação e de práticas em laboratórios.

Os alunos foram divididos em grupos e orientados a ler os guias práticos de uso dos softwares. Assim, o êxito nas tarefas mediadas pelo *software* implica ênfase na troca entre os participantes acerca do aprendizado por meio dos recursos da informática. A execução foi conduzida conforme o seguinte cronograma de trabalho e orientações contidas no Quadro 2.

Quadro 2 – Execução das atividades práticas

Período	Atividades Práticas
Primeira Semana (23/05/2019)	Na primeira atividade prática, os grupos utilizaram o guia prático do *software* de criptografia simétrica *VeraCrypt*, com 12 páginas, descrevendo os sites de *download*, a instalação e utilização dos algoritmos criptográficos e funções de *hash* (VERACRYPT, 2018). O *VeraCrypt* surgiu da necessidade de se guardar informações de forma cifrada nos discos rígidos por longos períodos. O seu ponto forte consiste na criação e utilização de arquivos como volumes virtuais (unidades, drives ou discos) para criptografar partições inteiras de discos rígidos ou pen-drives, protegendo todos os arquivos contidos no volume virtual. Quanto ao tamanho da chave, é variável de acordo com o conjunto de algoritmos selecionados. Com a utilização do *software*, os alunos criaram um arquivo e fizeram a montagem de um volume virtual para exibição na unidade do gerenciador de arquivos. Com o término dos trabalhos, os alunos desmontaram todo o processo realizado.
Segunda Semana (06/06/2019)	Na segunda atividade prática, os grupos utilizaram o guia prático do *Open Pretty Good Privacy* - Open PGP, sendo utilizado o *software Gnu Privacy Guard* - GPG, que é gratuito e de código-fonte aberto (OPENPGP, 2018). O guia prático de sete páginas sobre o software GPG e seus similares descreve os sites para download, a instalação de *plugins* nos navegadores, geração de chaves públicas, e gerenciamento de chaves para o envio de e-mail seguro. O padrão OpenPGP é definido pela *Request for Comment*s – RFC 4880 (FINNEY *et al.,* 2007). A RFC 4880 usa criptografia assimétrica e uma chave privada de características apropriadas para prover serviço seguro de comunicação eletrônica. É importante ressaltar que alguns alunos utilizaram outros *softwares* assimétricos em virtude de conhecimento prévio do assunto. A criptografia assimétrica utiliza o conceito de chaves públicas, que são distribuídas para as pessoas com quem se deseja trocar dados ou mensagens, e a chave privada fica em sua máquina (ou preferencialmente *token* criptográfico ou *SmartCard*) e não deve ser distribuída.

Fonte: Elaborado pelos autores (2021)

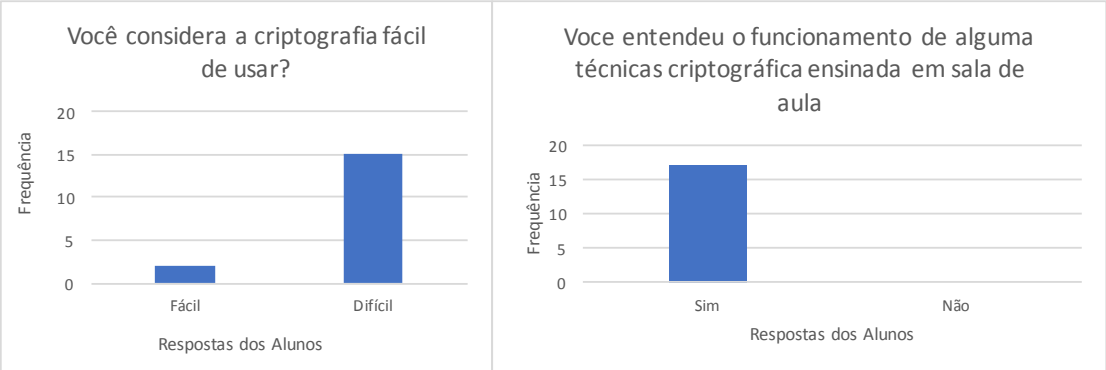
Análise dos resultados

Visando avaliar a aprendizagem das práticas pedagógicas propostas, elaborou-se dois questionários autoavaliativos para alunos no *Google Forms*. O primeiro questionário versa sobre o conhecimento teórico da criptografia estudada nos seminários. O segundo questionário versa sobre o uso dos softwares criptográficos utilizados nas aulas práticas. Os questionários foram respondidos por 17 alunos, sendo que 10 alunos afirmaram já ter algum conhecimento prévio sobre a criptografia e os outros sete alunos afirmaram não conhecer o tema. Os resultados das análises qualitativas são mostrados graficamente a seguir.

A facilidade de uso e aprendizagem do funcionamento da criptografia é apresentada nos gráficos da Figura 3. O gráfico da esquerda demonstra que a maioria dos alunos consideram a criptografia difícil (15 alunos), somente dois alunos acham de fácil uso. No

entanto, o gráfico da direita indica que todos (17 alunos) afirmam ter aprendido o funcionamento de pelo menos uma técnica criptográfica ensinada em sala de aula.

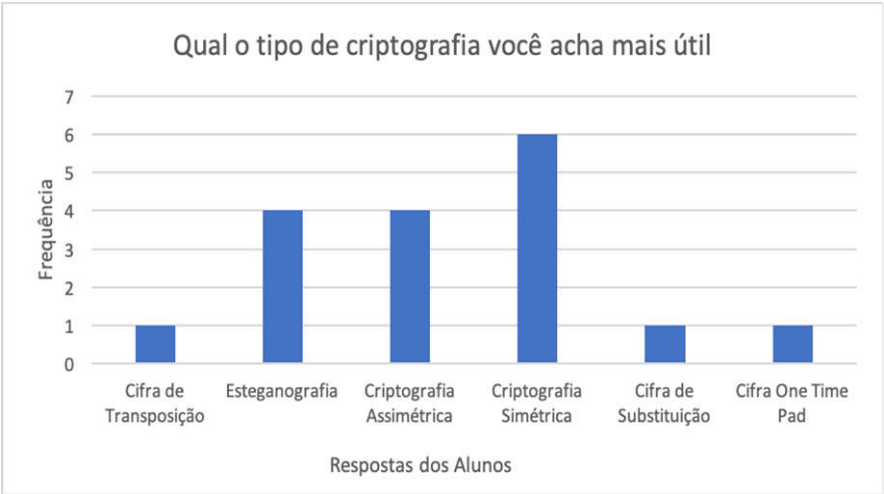
Figura 3 – Opiniões dos alunos sobre a facilidade de uso e aprendizagem da criptografia



Fonte: Resultados desta pesquisa (2019)

A utilidade do tipo de criptografia é mostrada na Figura 4. Observa-se que a criptografia simétrica é considerada a mais útil pela maioria dos alunos (seis alunos), seguida pela criptografia assimétrica (quatro alunos) e esteganografia (quatro alunos). Nota-se que os tipos de criptografia clássica foram considerados menos úteis: somente um aluno escolheu a cifra de transposição, um aluno a cifra de substituição e um aluno a cifra *de one time pad*. Os resultados sugerem que os alunos entenderam a importância da criptografia moderna intermediada por computador e suas aplicações cotidianas.

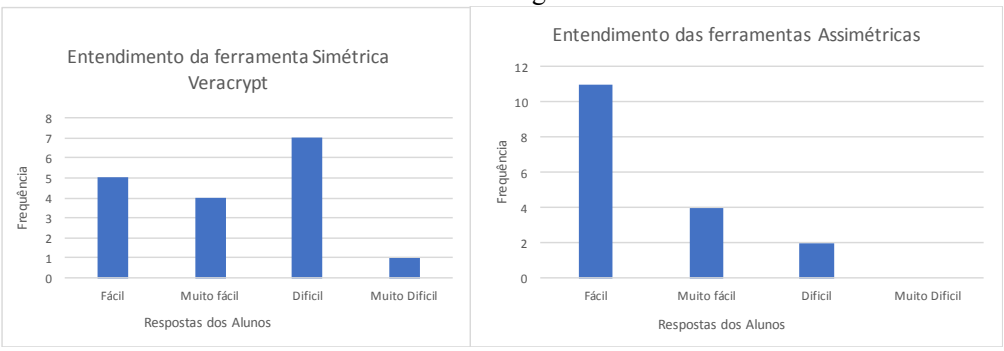
Figura 4 – Opiniões dos alunos sobre a utilidade do tipo de criptografia



Fonte: Resultados desta pesquisa (2019)

O entendimento das ferramentas criptográficas utilizadas em aula práticas laboratoriais é apresentado nos gráficos da Figura 5. O gráfico da esquerda indica que a maioria dos alunos consideram a ferramenta *VeraCrypt* difícil de usar com a finalidade de cifrar arquivos em disco. O gráfico da direita mostra que a criptografia assimétrica foi considerada de fácil uso, mesmo sendo necessário o entendimento de geração e distribuição de chaves criptográficas para enviar e-mail seguro. Este resultado em relação às ferramentas assimétricas pode ser explicado pelo fato de alguns alunos terem conhecimento prévio sobre outros *softwares* assimétricos, que foram permitidos na atividade. Desta forma, os alunos que já conheciam o assunto se aprofundaram e atualizaram os seus conceitos, bem como auxiliaram os outros alunos, que não conheciam a criptografia assimétrica, na aquisição dos novos saberes.

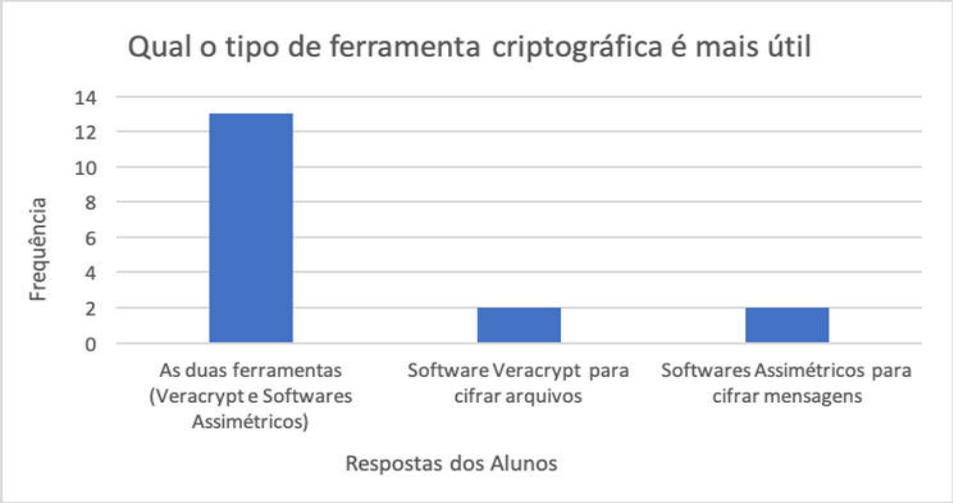
Figura 5 - Opiniões dos alunos sobre o entendimento de cifrar arquivos em disco e envio de e-mails seguro.



Fonte: Elaborado pelos autores

A importância de ambas as ferramentas criptográficas utilizadas em aula práticas laboratoriais é apresentada na Figura 6, reforçando que a maioria (13 alunos) consideram ambas as ferramentas importantes. Dessa forma, constata-se que os alunos compreenderam as finalidades distintas dos tipos de criptografia moderna ensinada. Os resultados indicam também que somente dois alunos consideram que o mais importante em criptografia é cifrar arquivos em disco com a ferramenta *VeraCrypt*. Em contraste, e na mesma proporção, outros dois alunos consideram que o mais importante em criptografia é enviar e-mail seguro com algum software assimétrico.

Figura 6 – Opiniões dos alunos sobre a importância das ferramentas criptográficas ensinadas



Fonte: Resultados desta pesquisa (2019)

As respostas obtidas evidenciaram que a compreensão destes fundamentos científico-tecnológicos de segurança, em processos de informação sobre o tema criptografia, devem ser motivadoras e contextualizadas quanto aos conceitos teóricos e as aplicações práticas.

Considerações finais

Neste artigo foram apresentados os conceitos de segurança da informação, de criptografia e seu uso, para alunos do ensino médio profissional. Especificamente, foi dada ênfase à criptografia por ser um importante alicerce para a sociedade atual. As ferramentas de criptografia apresentadas aos alunos, juntamente com seus guias de uso, permitem trabalhar com criptografia de dados e mensagens, garantindo a confidencialidade das informações.

Como a criptografia está presente em diferentes equipamentos, sejam eles aparelhos eletrônicos computacionais fixos ou móveis, foi notório o envolvimento dos alunos na realização das atividades, bem como a concentração exigida para a sua compreensão. As duas práticas pedagógicas realizadas, seminário e aulas práticas, tiveram boa receptividade, apesar dos diferentes graus de envolvimento e participação dos alunos. Os seminários exploraram a parte histórica, para que o estudante possa compreender que a criptologia surge por necessidade e se desenvolve conforme a tecnológica avança. As aulas práticas permitiram aplicar os assuntos já trabalhados no aspecto teórico, com softwares amplamente usados no mercado de trabalho.

Através da análise geral das perguntas dos questionários, pode-se concluir que as práticas pedagógicas utilizadas foram eficazes para a construção do conhecimento dos alunos sobre o tema criptografia, todos puderam aprender pelo menos uma técnica criptográfica ensinada. Ressalta-se, porém, que alguns alunos encontram dificuldades na utilização das ferramentas de criptografia, provavelmente pela complexidade do assunto e o reduzido tempo para o ensino da criptografia.

AGRADECIMENTOS: Os autores agradecem ao: Instituto Federal de Educação, Ciência e Tecnologia Goiano (IF Goiano); e ao Instituto Federal de Educação, Ciência e Tecnologia de São Paulo (IFSP), pelo apoio que prestado durante as pesquisas que viabilizaram a elaboração desta pesquisa.

REFERÊNCIAS

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. Disponível em: https://web.cs.ucdavis.edu/~rogaway/classes/227/spring05/book/main.pdf. Acesso em: 06 fev. 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. Disponível em: https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf. Acesso em: Acesso em: 04 abr. 2019.

FINNEY, H. *et al*. OpenPGP Message Format. **RFC 4880**. 2007. Disponível em: https://datatracker.ietf.org/doc/html/rfc4880. Acesso em: 23 maio 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. Disponível em:

http://www.scielo.br/j/ciedu/a/m8BHLB9MbCb5zYhxKsVvcsk/abstract/?lang=pt. Acesso em: 06 jun. 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. Disponível em: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.21.4050&rep=rep1&type=pdf. Acesso em: 06 ago. 2019.

OPENPGP. **OpenPGP**. 2018. Disponível em: https://www.openpgp.org. Acesso em: 20 maio 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. Disponível em: https://br-ie.org/pub/index.php/sbie/article/view/7677. Acesso em: 30 set. 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. Disponível em: https://ieeexplore.ieee.org/document/4959085. Acesso em: 09 abr. 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. Disponível em: https://www.veracrypt.fr/en/Home.html. Acesso em: 20 maio 2019.

Como referenciar este artigo

MARIN, R. P. M.; SOUZA, J. G. S.; MARIN, L. H. G. Ensinando conceitos básicos de criptografia no ensino médio profissional. **Revista on line de Política e Gestão Educacional**, Araraquara, v. 25, n. 2, p. 1282-1296, maio/ago. 2021. e-ISSN:1519-9029. DOI: https://doi.org/10.22633/rpge.v25i2.14469

Submetido em: 17/11/2020
Revisões requeridas em: 14/05/2021
Aprovado em: 31/05/2021
Publicado em: 01/08/2021