



CRIOGRAFIA PARA O BEM E PARA O MAL

Mauro Porto Guterres¹

Carla Souto²

RESUMO

Com a evolução da tecnologia, considerando-se que traz vantagens e desvantagens, tratando da proteção de nossas informações que são de vital importância e da segurança em vários ambientes, desde o pessoal ao mundial, será desenvolvida uma breve explanação sobre a criptografia, sua história e seus usos. Este trabalho não tem o objetivo de tornar o leitor um especialista no assunto mas sim de fornecer pelo menos as noções básicas de como surgiu a criptografia, sua importância cada vez maior nas nossas vidas, seus usos mais comuns e no dia a dia, explicar e exemplificar como pode ser usada tanto para proteção de nossas informações como para nos fazer reféns de criminosos. Como qualquer ferramenta, a criptografia pode ser utilizada para o bem ou o mal, o que vai definir seu uso é a intenção de quem e como vai ser empregada.

Palavras-chave: Segurança. Vantagens. Criptografia. Tecnologia. Informações.

¹Acadêmico do Curso Superior em Tecnologia em Programação para Internet – Faculdade Alcides Maya. mauro.guterres@alcidesmaya.edu.br
² Professora do Curso Técnico em Informática. Carla.souto@alcidesmaya.com.br



A primeira referência a criptografia foi encontrada no túmulo de um egípcio morto há aproximadamente 3.900 anos, chamado Khnumhotep II³. Da primeira referência encontrada até os dias atuais houve uma grande evolução. Foi utilizada em guerras ao longo da história para evitar que no caso de comunicações serem interceptadas, não pudessem ser compreendidas, protegendo assim a estratégia que estava sendo criada e compartilhada. Também foi muito utilizada em cartas de amor com o objetivo de manter em segredo as conversas dos apaixonados.

Atualmente a criptografia se popularizou e se tornou de suma importância para manter a privacidade e segurança de nossos dados pessoais, transações financeiras, redes de comunicação, já que todas as informações nos dias atuais circulam e são armazenadas por meios digitais.

3. Definição

Criptografia se define como a utilização de códigos para manter informações sigilosas. Do grego, *kryptós*⁴ quer dizer “escondido, oculto”, e *gráphein*, significa “escrita”. Trata-se de uma técnica que torna a mensagem codificada passível de interpretação apenas para o emissor e o receptor, evitando que intrusos a decodifiquem. É usada há bastante tempo, e hoje em dia, existem áreas próprias de estudo.

4. Princípios

A criptografia segue quatro princípios: confidencialidade, integridade, autenticação e não-repúdio, ou irretratibilidade.

4.1. O princípio da confidencialidade é a propriedade que garante que a informação contida na mensagem, documento ou qualquer outro meio, só será acessada pelas pessoas que tiverem a devida autorização.

³ <https://www.binance.vision/pt/security/history-of-cryptography>

⁴ <https://www.colegioweb.com.br/curiosidades/criptografia.html>



4.2. O princípio da integridade define que a informação transmitida, independente do meio utilizado, não sofreu alterações não autorizadas. Tem a garantia que a informação enviada e recebida contém o mesmo conteúdo.

4.3. O princípio da autenticação garante a identidade do emissor da informação. Assim temos certeza de quem está enviando a mensagem.

4.4. O princípio do não-repúdio ou irretratibilidade é o princípio que dá a garantia do emissor não negar que transmitiu a mensagem. Princípio esse muito importante se tratando de transações financeiras e comerciais.

5. Usos legítimos

Mas nem todos os sistemas ou algoritmos são utilizados para atingir tais objetivos. Essa técnica foi bastante aplicada e incrementada em grandes conflitos, como a Segunda Guerra Mundial ou a Guerra Fria, na tentativa de evitar vazamentos de informações.

A criptografia nos computadores não é usada no intuito somente de misturar e desembaralhar informações. Ela é uma ferramenta para garantir a privacidade entre quem envia e quem recebe a mensagem, garantindo que só as partes envolvidas e interessadas tenham acesso ao conteúdo enviado. Se as mensagens forem interceptadas por terceiros, a criptografia é a única garantia de segurança que impede acesso às informações encaminhadas. Além disso, documentos criptografados, tem sua autenticidade comprovada, já que somente quem envia e recebe tem a chave de acesso a esse documento evitando não só que o mesmo seja consultado mas também que seja alterado, garantindo a integridade da informação.

Se não fosse pelas técnicas criptográficas utilizadas, a vida seria muito diferente. Nossa vida gira em torno da criptografia. Está tão inclusa no nosso cotidiano que nem percebemos mas sem ela não poderíamos, por exemplo, executar transações bancárias. Outros exemplos mais simples são quando enviamos mensagens por aplicativos como *Whatsapp*, quando usamos redes sociais como *Facebook* ou até mesmo quando se usa um cartão de crédito para comprar um café.



6. Desvios no uso

Mas nem todos utilizam a criptografia para o bem. Pessoas mal intencionadas se utilizam do anonimato e proteção oferecidos pelos meios criptográficos para planejamento de atos criminosos.

A popularização de *smartphones* e *tablets*, contribuiu muito para o aumento da quantidade de crimes cibernéticos. Atualmente uma grande parcela da população utiliza esses equipamentos para armazenamento de dados pessoais, compras por meios eletrônicos, operações bancárias e acabam expondo dados sensíveis. Com uso de *softwares* mal intencionados (vírus, spam, sites falsos), criminosos se apropriam ou sequestram esses dados.

Um exemplo pode ser o *ransomware*, que o objetivo não é obter os dados mas sequestrá-los, cobrando um resgate para que sejam devolvidos ou correndo o risco da perda dos mesmos. Como tudo em tecnologia evolui, o *ransomware* agora se atualizou, passando a ser um *crypto-ransomware*, utilizando a criptografia não para sequestrar mas para embaralhar os dados da vítima, sendo cobrada uma quantia pela chave que serve para desembaralhar esses dados.

Mesmo criminosos comuns se beneficiam da criptografia utilizada em aplicativos como *Whatsapp* ou *Telegram* para conversas e planejamento de pequenas e grandes operações criminosas. O roubo de aproximadamente R\$ 110,2 milhões em ouro⁵ no dia 25 de julho de 2019, no Aeroporto de Guarulhos em São Paulo pode ser citado como um exemplo. Para uma operação dessa magnitude, certamente foram muitas horas de planejamento e logística, necessitando muita troca de informações que se não fossem criptografadas seriam facilmente rastreadas pelas autoridades.

Proibir ou reprimir o uso da criptografia não é solução para amenizar o cometimento de crimes cibernéticos ou que deles façam uso. Ao contrário, sem essa proteção, os dados, informações e a vida das pessoas estariam expostos a todo tipo de malfeitores que teriam acesso a tudo que precisam.

⁵ <https://g1.globo.com/sp/sao-paulo/noticia/2019/07/25/grupo-fortemente-armado-invade-terminal-de-cargas-de-cumbica-faz-refem-e-rouba-ouro-de-carro-forte.ghtml>



Sobre o assunto, o que diz Marcacini (2010. P. 114/119):

O fato de a criptografia também servir para comunicação entre criminosos é um argumento forte em contrário, mas que, na busca de um equilíbrio entre os interesses, não parece bastante para justificar restrições ao seu uso. Como vários dos direitos individuais, o direito à privacidade obtida pela criptografia pode, infelizmente, servir para acobertar operações ilegais. Mas a presunção de inocência e outros princípios que regem o processo penal também permitem, por vezes, a libertação do culpado, e ninguém em sã consciência iria sustentar o fim destes ideais de liberdade. Aparatos tecnológicos podem ser usados para o bem ou para o mal. Pessoas que andam livremente pelas ruas podem estar se preparando para cometer um crime. O ponto que não podemos desprezar é que não se deve privar a população em geral da sua liberdade, ou de algum outro conforto ou facilidade tecnológica, em nome do combate ao crime a que se dedicam alguns criminosos.

O direito à privacidade deve ser preservado mesmo que o preço pago seja alto. A tecnologia deve ser usada para contornar os problemas causados por mal intencionados que se utilizam de tecnologias legítimas para usos torpes.

7. Conclusão:

Embora possa ser utilizada para o mal, a criptografia deve ser um direito irrevogável dos usuários de tecnologia sendo que sua função de proteção de dados e informações é muito maior e mais importante do que as atividades criminosas por ela proporcionadas. Com o avanço da tecnologia, maior preparação e conhecimento dos usuários é possível minimizar os riscos do uso mal intencionado da criptografia. Infelizmente nenhum sistema de proteção é infalível mas isso não é o suficiente para que tenhamos que abrir mão da nossa privacidade nos restando gerenciar os riscos. A criptografia já tem seu lugar na história e não deixará de ser utilizada nunca, só devemos definir como será aplicada.



REFERÊNCIAS:

BORGES, Fabiane. **Criptografia: o uso maléfico de uma tecnologia criada para a proteção da privacidade dos usuários.** Disponível em: <<https://fabianiborges.jusbrasil.com.br/artigos/363173950/criptografia-o-uso-malefico-de-uma-tecnologia-criada-para-a-protecao-da-privacidade-dos-usuarios>>. Acesso em: 09 nov. 2019.

COLÉGIO WEB. **Criptografia.** 2019. Disponível em: <<https://www.colegioweb.com.br/curiosidades/criptografia.html>>. Acesso em: 09 nov. 2019.

NOGUEIRA, Michelle. **Criptografia.** 2015. Disponível em: <<https://www.estudopratico.com.br/criptografia/>>. Acesso em: 09 nov. 2019.