SEGURANÇA E DIREITO DIGITAL
CRIPTOGRAFIA: SHA-2

Gabriel Mitelman Tkacz
42230446@mackenzista.com.br
Universidade Presbiteriana Mackenzie, Faculdade de Computação e Informática
São Paulo, fevereiro de 2023

O SHA-2 (Secure Hash Algorithm 2) é uma função criptográfica amplamente utilizada mundialmente, desenvolvida pela Agência de Segurança Nacional (NSA) dos Estados Unidos. É uma família de funções *hash* que inclui SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224 e SHA-512/256. O SHA-2 é projetado para gerar uma saída de tamanho fixo de 224, 256, 384 ou 512 bits, dependendo da variante utilizada.

O SHA-2 é um componente crítico da segurança digital moderna e é usado para diversos fins, como por exemplo assinaturas digitais, armazenamento de senhas e verificações de integridade de dados. Um de seus principais usos é garantir a autenticidade de documentos, mensagens e dados digitais. Isso é feito gerando um valor *hash* único para cada arquivo ou mensagem, que pode então ser usado para verificar se o arquivo ou mensagem não foi adulterado durante a transmissão ou armazenamento de tais dados.

O SHA-2 é considerado um algoritmo altamente seguro devido à sua resistência a ataques, como *preimage*, colisão e ataques de aniversário. Um ataque de *preimage* é uma tentativa de encontrar uma mensagem que corresponda a um valor hash específico. Um ataque de colisão é uma tentativa de encontrar duas mensagens diferentes que produzem o mesmo valor *hash*. Um ataque de aniversário é uma tentativa de encontrar duas mensagens com o mesmo valor hash. O SHA-2 foi projetado para resistir a esses ataques, tornando-o uma ferramenta valiosa para garantir a segurança de dados nos dias atuais.

Outra vantagem do SHA-2 é sua eficiência. O algoritmo pode produzir valores hash rapidamente, tornando-o ideal para uso em aplicações em grande escala. Além disso, o SHA-2 é amplamente suportado por vários sistemas operacionais, linguagens de programação e diversos aplicativos e softwares, tornando-o fácil de integrar em sistemas existentes.

O SHA-2 é amplamente utilizado em diversas indústrias, incluindo finanças, saúde e governo. Por exemplo, o SHA-2 é usado para garantir a segurança de transações bancárias online e para proteger dados sensíveis de pacientes em sistemas de saúde. Além disso, muitos governos usam o SHA-2 para garantir a segurança de suas comunicações e proteger informações confidenciais.

Em conclusão, o SHA-2 é uma função criptográfica altamente segura e eficiente que desempenha um papel crítico na segurança digital atualmente. Sua resistência a ataques e amplo suporte o tornam uma ferramenta valiosa para garantir a integridade e autenticidade de dados. O SHA-2 provavelmente continuará sendo uma parte importante da segurança digital nos próximos anos, à medida que a necessidade de transmissão e armazenamento de dados seguros continua a crescer.

BIBLIOGRAFIA:

1. DANG, Q. Secure Hash Standard (SHS). Federal Inf. Process. Stds. (NIST FIPS). National Institute of Standards and Technology, Gaithersburg, MD. Disponível em: https://doi.org/10.6028/NIST.FIPS.180-4. Acesso em: 22 fev. 2023.
2. THALES GROUP. The Cryptography and Hash Functions Guide. Disponível em: https://www.thalesgroup.com/en/markets/digital-identity-and-security/cryptography-and-hash-functions-guide. Acesso em: 23 fev. 2023.
3. STEVENS, M.; STOEBERL, P.; APAKA, I. Announcing the first SHA1 collision. Google Online Security Blog, 23 fev. 2017. Disponível em: https://security.googleblog.com/2017/02/announcing-first-sha1-collision.html. Acesso em: 23 fev. 2023.
4. SCHNEIER, B. Cryptanalysis of SHA-1 - Schneier on Security. Disponível em: https://www.schneier.com/blog/archives/2005/02/cryptanalysis_o.html. Acesso em: 23 fev. 2023.