A função *hash* criptográfica SHA-3

Gustavo Zambonin*
Segurança em Computação (UFSC – INE5429)

1 Definições

- Uma *função hash criptográfica*, ou função de resumo criptográfica (futuramente denotada por h), é um algoritmo matemático que mapeia uma quantidade de bytes qualquer[1] para uma palavra de tamanho fixo, ou seja, $h : \{0,1\}^* \longrightarrow \{0,1\}^n$, $n \in \mathbb{N}$.

  Para que seja resistente a diversos tipos de criptoanálise, uma função $h : X \longrightarrow Y$ deve respeitar algumas propriedades:

  i. *Resistência à pré-imagem*: Para um resumo $M' \in Y$, é computacionalmente impraticável[2] encontrar a mensagem $M \in X$ tal que $h(M) = M'$. Uma função matemática com esta propriedade é chamada de unidirecional.

  ii. *Resistência à segunda pré-imagem*: Para uma mensagem $M_0 \in X$, é computacionalmente impraticável encontrar uma segunda mensagem $M_1 \in X$ tal que $M_0 \neq M_1$ e $h(M_0) = h(M_1)$.

  iii. *Resistência à colisão*: Para duas mensagens $M_0, M_1 \in X$, é computacionalmente impraticável encontrar $M_0 \neq M_1$ e $h(M_0) = h(M_1)$.

  É importante notar que, embora as definições sejam extremamente parecidas, resistência à segunda pré-imagem e resistência à colisão são conceitos diferentes; um atacante não consegue escolher a primeira mensagem caso queira atacar a resistência à segunda pré-imagem; para a resistência à colisão, o atacante pode escolher livremente o par de mensagens.

- Algumas aplicações destas funções são enumeradas abaixo:

  – Podem ser utilizadas para verificar a integridade da mensagem, comparando resumos criptográficos calculados antes e depois da transmissão de mensagem e/ou arquivos.

  – Para evitar o armazenamento de senhas em texto claro, é possível armazenar apenas o resumo criptográfico de cada senha e compará-lo na autenticação do usuário.

  – Resumos criptográficos são comumente descritos como identificadores únicos seguros para um arquivo ou informação digital (por exemplo, *commits* em um sistema de controle de versão).

- O padrão SHA-3, descrito pelo documento FIPS 202 [1], é baseado em uma instância do algoritmo Keccak, selecionado pelo NIST (*National Institute of Standards and Technology*). Este documento também especifica a família Keccak$-p$ de permutações matemáticas.

Referências

[1] Morris J. Dworkin. SHA-3 standard: Permutation-based hash and extendable-output functions. Technical report, July 2015.

*`gustavo.zambonin@grad.ufsc.br` — todos os algoritmos utilizados podem ser encontrados também neste repositório.
[1] algumas funções desse tipo têm limites quanto ao tamanho da entrada, embora estes sejam extremamente grandes.
[2] o tempo ou recursos gastos para esta computação excedem a validade ou utilidade da informação desejada.