Criptografia SHA-256

Wagner Oliveira dos Santos[1]

[1]Escola Politécnica
Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS)
Av. Ipiranga, 6681 Partenon Porto Alegre - RS

w.santos@acad.pucrs.br

1. Função Hash

Funções Hash [DE ALVARENGA 2017] são amplamente utilizadas para diversas aplicações na área da computação, algumas delas são geração de números aleatórios, assinatura digital, código de autenticação de mensagem (MACs), e outras formas de autenticação. Seus principais componentes são o modo de operação, função de compressão e operação de confusão e dispersão.

2. Autenticidade de arquivo de vídeo

Simulou-se a validação da autenticidade de um arquivo de vídeo quebrado em N partes de tamanho fixo *1KB*. Aonde inicia-se o processo de geração do hash do último bloco do arquivo, concatenando o valor resultante ao bloco anterior, e repetindo esse processo até primeiro bloco do vídeo. Dessa forma é possível realizar a validação do vídeo por partes, não sendo necessário o arquivo por completo para garantir sua autenticidade.

3. Resultados da validação do arquivo

Nas imagens abaixo são exibidos os resultados da geração do valor hash dos vídeos utilizados.

```
→ make
python3 hash_validation.py ./data/video05.mp4
8e423302209494d266a7ab7e1a58ca8502c9bfdaa31dfba70aa8805d20c087bd
```

Figura 1. Vídeo de exemplo - video05

```
→ make
python3 hash_validation.py ./data/video03.mp4
ee24473e4a369a305c9c3d54629eff01f609b8e2f61ca9cf6f3084f13fe346d6
```

Figura 2. Vídeo de teste - video03

Referências

DE ALVARENGA, L. (2017). *Criptografia Clássica E Moderna*. Clube de Autores.