Alunos: **Antonio Carlos, Glaycow Silveira Silva e Souza, Lucas Ribeiro**

1. Por que a utilização de funções hash criptográficas garante integridade da mensagem?

Por que o hash é aplicado sobre os dados de entrada da mensagem, assim o conteúdo não será alterado durante o caminho da entrega, e ainda garante que essa mensagem foi feita por uma pessoa já autenticada e autorizada. O processo precisa ser mais avançado. O emissor deve gerar 2 informações, conhecidas como chave privada e chave pública. A chave privada, como o nome induz, é de conhecimento apenas do emissor da mensagem, enquanto a chave pública pode ser divulgada. As chaves possuem uma relação matemática muito forte, de tal forma que o receptor da mensagem pode conferir que a mesma foi de fato emitida pela pessoa esperada usando apenas a chave pública dessa forma a mensagem tem sua integridade garantida (CARNEIRO, 2017).

1. Quais são os requisitos para uma função hash criptográfica?

As funções HASH é utilizada para produzir uma “Impressão digital” de um arquivo, mensagem ou outro bloco de dados, Para ser útil para a autenticação de mensagens, uma função HASH H deve conter os seguintes requisitos (STALLINGS; BROWN, 2014).

* 1. H pode ser aplicado a um bloco de dados de qualquer tamanho.
  2. H produz uma saída de comprimento fixo.
  3. H(x) é relativamente fácil de computar para qualquer x dados, tornando práticas implementações em hardware e em software.
  4. para qualquer código dado j, é inviável em termos computacionais achar x tal que H(x) = h. Uma função de hash com essa propriedade é denominada via ou resistente à pré-imagem.
  5. Para qualquer bloco dado x, é inviável em termo computacionais achar y ≠ x tal que H(y) = H(x). Uma função de hash com essa propriedade é denominada resistente à segunda pré-imagem, às vezes vezes denominada resiste a colisão fraca.
  6. è inviável, em tremo computacionais, achar qualquer par (x,y) tal que H(x) = H(y). Uma função de hash com essa propriedade é denominada resistente a colisão, as vezes, resistente a colisão forte.

1. O que significa uma colisão no contexto das funções hash criptográficas?

Quando os dois dados de entrada produzem a mesma cadeia de hash fina, A probabilidade disso acontecer depende de qual a função está sendo utilizado (GUZEL, 2017).

1. Em que consiste a “força” (nível de segurança) de uma função hash criptográfica?

A “força” de uma função HASH (nível de segurança) é dada pela dificuldade de se criar colisões intencionais, evitando que haja sequência iguais para dados diferentes. (FONSECA; VAZ, 2017)

**Referencias**

CARNEIRO, Luis Sergio F. . CRIPTOGRAFIA, HASH, ASSINATURA DIGITAL: QUAL A DIFERENÇA?. Disponível em: <http://www.matera.com/br/2015/02/27/criptografia-hash-assinatura-digital-qual-diferenca/>. Acesso em: 03 nov. 2017.

STALLINGS, William; BROWN, Lawrie. Segurança de Computadores. Sem Localidade: Elsevier, 2014. 744 p.

GUZEL, Burak . Compreendendo as Funções Hash e Mantendo as Senhas Seguras. Disponível em: <https://code.tutsplus.com/pt/tutorials/understanding-hash-functions-and-keeping-passwords-safe--net-17577>. Acesso em: 03 nov. 2017.

FONSECA, Thiago Castelló; VAZ, Verônica Taquette. Assinatura Digital. Disponível em: <https://www.gta.ufrj.br/grad/07\_1/ass-dig/TiposdeCriptografia.html#Topic5>. Acesso em: 04 nov. 2017.