CENTRO UNIVERSITÁRIO DE VOLTA REDONDA – UniFOA
FUNDAÇÃO OSWALDO ARANHA

Campus Universitário Olezio Galotti – Avenida Paulo Erlei Alves Abrantes, 1325
Três Poços – Volta Redonda RJ – Tel: (24) 3340-8400 – www.unifoa..edu.br

Curso Tecnológico de Redes de Computadores
Disciplina: Segurança da Informação
Professor: José Maurício S. Pinheiro ***V. 2010-1***

AULA 7: Resumo Criptográfico (hash)

Existem diversos métodos para assinar digitalmente documentos, e esses métodos estão em constante evolução. Porém de maneira resumida uma assinatura típica envolve dois processos criptográficos: o hash (resumo) e a encriptação deste hash.

1. Função Resumo

A tradução literal de hash é "picar, misturar, confundir". Funções criptográficas de resumo são usadas em vários contextos, por exemplo, para computar um resumo de mensagem ao criar uma assinatura digital.

A Função Resumo (hash) é uma transformação matemática que faz o mapeamento de uma seqüência de bits de tamanho arbitrário para uma seqüência de bits de tamanho fixo menor – conhecido como resultado hash ou resumo criptográfico - de forma que seja muito difícil encontrar duas mensagens produzindo o mesmo resultado hash (resistência à colisão) e que o processo reverso também não seja realizável (dado um resultado hash, não é possível recuperar a mensagem que o gerou).

Entre outras aplicações, as funções de resumo são usadas em criptografia para:

- Garantia de integridade dos dados.
- Garantia de origem de uma mensagem.
- Cálculo de respostas que são função de uma chave secreta e de uma mensagem de desafio (em protocolos de identificação através de desafio).
- Confirmação de chave.
- Confirmação de conhecimento (habilidade de comprovar conhecimento prévio de algo sem a necessidade de expor os dados previamente).
- Derivação de chave.
- Geração de números pseudo-aleatórios.

2. Resumo Criptográfico

Em um primeiro momento é gerado um resumo criptográfico da mensagem através de algoritmos complexos (MD5, SHA-1, SHA-256, por exemplo) que reduzem qualquer mensagem sempre a um resumo de mesmo tamanho. A este resumo criptográfico se dá o nome de hash. O resumo

criptográfico, em conjunto com a criptografia assimétrica, é utilizado para garantir a integridade de um documento digital.

Após gerar o hash, ele deve ser criptografado através de um sistema de chave pública, para garantir a autenticação e a irretratabilidade. O autor da mensagem deve usar sua chave privada para assinar a mensagem e armazenar o hash criptografado junto a mensagem original.

Para verificar a autenticidade do documento, deve ser gerado um novo resumo a partir da mensagem que está armazenada, e este novo resumo deve ser comparado com a assinatura digital. Para isso, é necessário descriptografar a assinatura obtendo o hash original. Se ele for igual ao hash recém gerado, a mensagem está íntegra. Além da assinatura existe o selo cronológico que atesta a referência de tempo à assinatura.

A idéia básica desta função é que um valor resumo serve como uma imagem representativa compacta (às vezes chamada de impressão digital ou MD - *Message Digest*) da cadeia de bits da entrada, e pode ser usada com se fosse unicamente identificável com aquela entrada. As funções de resumo criptográfico funcionam semelhantes ao dígito verificador do CPF. Por exemplo, se um número qualquer do CPF for modificado, o dígito verificador também sofrerá alteração.

As funções de resumo criptográfico são usadas para garantir a integridade de dados. Algumas das propriedades desta função são:

- Deve ser computacionalmente inviável fazer a operação inversa, ou seja, dado um resumo, deve ser inviável obter uma mensagem original;
- Duas mensagens semelhantes devem produzir um resumo completamente diferente;
- Deve ser fácil e rápido produzir o resumo.

Considerando que as mensagens possíveis são infinitas, mas o tamanho do hash é fixo, é impossível impedir que mensagens diferentes levem a um mesmo hash. Quando isto ocorre é dito que foi encontrada uma colisão de hashes e o algoritmo deve ser abandonado. As funções de hash estão em constante evolução para evitar que colisões ocorram.

A função resumo pode ser utilizada para garantir a integridade de uma mensagem. Isso pode ser feito enviando-se para Beto a mensagem e o resumo da mensagem cifrada com a chave privada de Alice. Beto decifra o resumo com a chave pública de Alice, calcula um novo resumo com base na mensagem recebida e compara os dois valores. Se forem iguais, a mensagem não foi alterada, garantindo-se dessa forma a sua integridade.

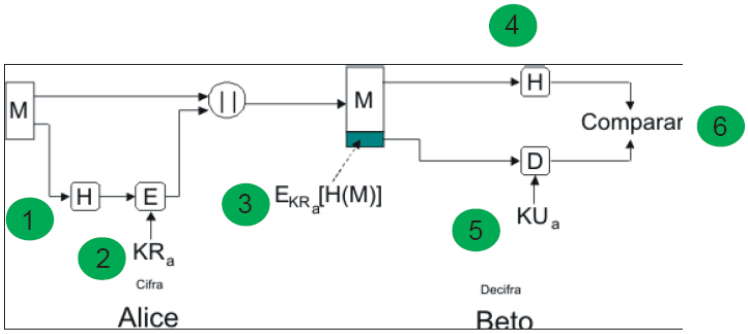

Figura 1 - Exemplo de utilização de função de resumo criptográfico

Na figura, “M” representa a mensagem. (1) Obtém-se o resumo da mensagem M. (2) Cifra o resumo com a chave privada (KRa) de Alice. (3) Mensagem original + resumo cifrado. (4) Beto obtém o *hash* do documento. (5) Beto decifra o *hash* com a chave pública de Alice. (6) Beto compara os resultados obtidos no processo 4 e 5. Se forem iguais, a mensagem está correta.

3. O algoritmo Hash

O algoritmo hash é composto por fórmulas matemáticas complexas, para poder garantir a irreversibilidade e a unicidade do MD gerado - textos diferentes não produzem o mesmo MD. A alteração de um simples bit na mensagem gera um MD completamente diferente e o valor de conferência ("check-sum") muda se um único bit for alterado, acrescentado ou retirado da mensagem. O tamanho do MD depende do algoritmo escolhido (MD1, MD2, MD5 ou SHA1, por exemplo), que é medido em bits - por exemplo, o SHA1 é o mais recente dentre estes anteriores e gera um hash de 160 bits.

A capacidade de descobrir uma mensagem que dê um hash a um dado valor possibilita a um agressor substituir uma mensagem falsa por uma mensagem real que foi assinada. Permite ainda que alguém repudie uma mensagem, alegando que assinou uma mensagem diferente, dando um hash ao mesmo valor e violando assim a propriedade de não-repúdio das assinaturas digitais.

Varias funções hash têm sido desenvolvidas com objetivo de melhorar a versão anterior a fim de obter maior segurança e evitar que os ataques sejam bem sucedidos. As mais conhecidas são:

- **MD4** - Produz um valor hash de 128 bits. Efetua uma manipulação de bits para obter o valor do hash, de forma rápida. É um padrão da Internet (RFC-1320). Porém, vários ataques foram detectados, o que fez com que o algoritmo fosse considerado frágil.
- **MD5 -** Extensão do MD4. Produz como saída um valor hash de tamanho de 128 bits. A obtenção do valor de hash é mais lenta, mas é mais segura. Está definido como um padrão da internet. (RFC-1321). É usado pelo PGP (Pretty Good Privacy).

- **SHA-1** (Secure Hash Algorithm) - Desenvolvido pelo NIST (National Institute of Standards and Technology), produz um valor hash de 160 bits. É considerado mais seguro que o MD4 e MD5 pelo seu tamanho.
- **RIPEMD-160.** É uma função hash criptográfica desenhada em um projeto chamado RIPE (Race Integrity Primitives Evaluation) e produz uma saída de 160 bits.

4. Tamanhos de chaves para assinatura digital

As recomendações que sinalizam a força de algoritmos criptográficos são baseadas nos parâmetros desses algoritmos e são caracterizadas por adotar basicamente comprimentos mínimos de chave, após esses algoritmos terem sido exaustivamente analisados. Essas estimativas de segurança são realizadas levando-se em consideração o esforço computacional necessário para se quebrar um dado algoritmo.

Não existem provas de segurança para os componentes dos sistemas de assinatura digital. Basicamente, todas as estimativas de segurança dependem de resultados de ataques considerados, atualmente, os mais eficazes. A possibilidade de uma quebra completa de um dado algoritmo (por exemplo, a descoberta de um método rápido de fatoração universal que possa ser usado contra o RSA) em tese não pode ser excluída, mas quebras desse tipo são consideradas como pouco prováveis.

Por outro lado, alguns avanços significativos em análise de algoritmos criptográficos baseados em funções hash são considerados como uma ameaça real aos sistemas de assinatura digital. Um exemplo recente são os ataques de colisão ao SHA-1, que demonstraram que essa função hash é fraca a esse tipo de ataque.