INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Professor: Macêdo Firmino
Disciplina: Redes de Computadores
Prática 04: Assinatura Digital com função Hash

Hash

Uma função Hash é um método criptográfico que, quando aplicado sobre uma informação, independente do tamanho que ela tenha, gera um resultado único e de tamanho fixo.

Você pode utilizar hash para:

- Verificar a integridade de um arquivo armazenado em seu computador ou em seus backups;
- verificar a integridade de um arquivo obtido da Internet (alguns sites, além do arquivo em si, também disponibilizam o hash correspondente, para que você possa verificar se o arquivo foi corretamente transmitido e gravado);
- gerar assinaturas digitais.

Para verificar a integridade de um arquivo, por exemplo, você pode calcular o hash dele e, quando julgar necessário, gerar novamente este valor. Se os dois hashes forem iguais então você pode concluir que o arquivo não foi alterado. Caso contrário, este pode ser um forte indício de que o arquivo esteja corrompido ou que foi modificado. Exemplos de métodos de hash são: SHA-1, SHA-256 e MD5.

Assinatura Digital

A assinatura digital permite comprovar a autenticidade e a integridade de uma informação, ou seja, que ela foi realmente gerada por quem diz ter feito isto e que ela não foi alterada.

A assinatura digital baseia-se no fato de que apenas o dono conhece a chave privada e que, se ela foi usada para codificar uma informação, então apenas seu dono poderia ter feito isto. A verificação da assinatura é feita com o uso da chave pública, pois se o texto foi codificado com a chave privada, somente a chave pública correspondente pode decodificá-lo.

Para contornar a baixa eficiência característica da criptografia de chaves assimétricas, a codificação é feita sobre o hash e não sobre o conteúdo em si, pois é mais rápido codificar o hash (que possui tamanho fixo e reduzido) do que a informação toda.

Uma vez computada, criptografa-se o hash gerado com uma chave privada. O resultado de todo este procedimento é chamado de assinatura digital da informação. Assinaturas digitais, como outras convencionais, podem ser forjadas. A diferença é que a assinatura digital pode ser matematicamente verificada. Dado um documento e sua assinatura digital, pode-se facilmente verificar sua integridade e autenticidade. Primeiro, executa-se a função hash, e posteriormente, decifra-se a assinatura digital com a chave pública do remetente. A assinatura digital decifrada deve produzir o mesmo hash gerado pela função hash executada anteriormente. Se estes valores são iguais é determinado que o documento não foi modificado após a assinatura do mesmo, caso contrário o documento ou a assinatura, ou ambos foram alterados.

PyCryptodome

O PyCryptodome é uma biblioteca em pyhton que trata de implementações de algoritmos de criptografia e hash. Ele foi usado na aula passada com criptografia simétrica, agora iremos utiliza-lo com criptografia assimétricas, funções hash e assinatura digital.

A seguir será apresentado um exemplo de um código que faz uso do algoritmo SHA256 do PyCryptodome para fazer o hash de uma mensagem de texto.

```
from Crypto.Hash import SHA256

text = 'seguranca de redes'
hash = SHA256.new(text).digest()
```

A seguir um exemplo, de uma assinatura do hash usando o algoritmo RSA.

```
from Crypto.PublicKey import RSA
from Crypto import Random

#Gerando as chaves
key_size = 1024
rand = Random.new().read
key = RSA.generate(key_size, rand)

#Assinando
signature = key.sign(hash, '')

#Verificando
result = public_key.verify(hash, signature)
```

Atividade

Faça uma aplicação cliente-servidor (continuação da aula de criptografia) para demonstrar a programação de socket, função Hash e assinatura digital, da seguinte maneira:

- O cliente e o servidor utilizam assinatura com chave pública RSA e Hash com SHA256;
- A chave pública do servidor foi previamente compartilhada para o cliente.
- O servidor inicializa e fica aguardando conexão.
- Um cliente envia para o servidor um texto (chamado de desafio);
- O servidor recebe o desafio, calcula o hash, assina o hash com sua chave privada e envia para o cliente.
- O cliente recebe a resposta, calcula o hash do desafio e compara com a decriptografia (verificação) da mensagem ddo servidor, com a chave pública do servidor.
- Rode o Wireshark e veja o funcionamento do seu programa na rede.