Este artigo tem o objetivo de explicar os principais conceitos necessários para o entendimento do processo de assinatura digital. Está organizado da seguinte forma: na seção 1 apresentamos o algoritmo base para criptografia da assinatura digital; na seção 2 falamos sobre certificado digital; na seção 3 descrevemos o que é a assinatura digital e seu processo; na seção 4 explicamos a validação desse documento.

**1. RSA**

Este tipo de algoritmo é chamado de criptografia assimétrica ou de chave pública, pois existem duas chaves que são usadas. A primeira chave é a chave pública, utilizada para criptografar ou “cifrar” os dados que vão ser enviados. A segunda chave é utilizada para descriptografar os dados, é chamada de chave privada, apenas ela consegue retornar o texto original do texto cifrado. Esta estrutura composta por duas chaves difere da criptografia simétrica, onde apenas uma chave é utilizada para criptografar e descriptografar o texto.

A construção de chaves é feita através da multiplicação de dois números primos relativamente grandes que gera um número que será elevado a um expoente que é um número público, e após isso ele é novamente elevado a outro expoente que é um número privado. Assim teremos um número público e um número privado. O processo de descriptografia será revertido através de fatoração, que é o inverso da multiplicação.

O método do RSA constrói uma tabela atribuindo a cada letra um número. Após isso, escolhemos os números primos. Após a atribuição de números para as letras, agora temos que calcular a função “totiente” que diz a quantidade de co-primos de um número que são menores que ele mesmo. Feito isso, o próximo passo é calcular a chave pública que é onde escolhe-se um número "e" em que 1 < e < função totiente. Com a chave pública em mãos podemos agora cifrar a mensagem aplicando, para cada letra, a fórmula “c = m ^ e mod n”, onde "e" é a chave pública e "m" é o valor numérico da letra.

Sem compartilhamento de chave: a criptografia RSA depende do uso de chave pública do receptor, para que você não precise compartilhar nenhuma chave secreta para receber mensagens de outras pessoas.

Prova de autenticidade: uma vez que os pares de chaves estão relacionados entre si, um receptor não pode interceptar a mensagem, pois não terá a chave privada correta para descriptografar as informações.

Os dados não podem ser modificados: os dados serão à prova de adulteração em trânsito, pois interferir nos dados altera o uso das chaves. E a chave privada não será capaz de descriptografar as informações, alertando o receptor sobre a manipulação.

**2. CERTIFICADO DIGITAL**

O Certificado Digital é a identidade eletrônica de pessoas ou empresas, é como uma carteira de identificação virtual. Os dados contidos dentro são as informações do nome da pessoa ou entidade a quem foi emitido o certificado digital e respectivo endereço, sua chave pública e respectiva validade, número de série, nome da AC que emitiu seu certificado, assinatura digital da AC.

Existem dois tipos de certificado digital. O A1 certificado digital é aquele que deve ser armazenado diretamente em um computador e mesmo que no certificado digital A1 preço não seja muito diferente do A3, o que muda é a validade que é de apenas 1 ano, podendo ser utilizado em emissões de notas fiscais automáticas e em outros processos que exijam identificação e precisem ser realizados com agilidade. O A3 certificado digital é armazenado de maneira física, em um cartão ou pendrive, tem validade de até 3 anos, pode ser transportado para qualquer lugar e é de altíssima segurança, já que não pode ser copiado.

Quando você receber o certificado de outra entidade, você pode precisar utilizar uma cadeia de certificados para obter o certificado CA raiz. A cadeia de confiança de certificação digital é a hierarquia existente entre os componentes da ICP-Brasil. Estes componentes são a AC Raiz (Autoridade Certificadora Raiz), as ACs (Autoridades Certificadoras) de primeiro nível e segundo nível, as ARs (Autoridades de Registros), e, finalmente, o usuário final.

A cadeia de certificados é uma lista de certificados utilizada para autenticar uma entidade. A cadeia, ou caminho, começa com o certificado daquela entidade, e cada certificado na cadeia é assinado pela entidade identificada pelo próximo certificado na cadeia. A cadeia termina com um certificado de CA raiz. O certificado de autoridade de certificação raiz é sempre assinado pela própria autoridade de certificação (CA). As assinaturas de todos os certificados na cadeia devem ser verificadas até que o certificado de CA raiz seja alcançado.

**3. ASSINATURA DIGITAL**

Esta é uma forma de assinatura que tem o mesmo valor jurídico que uma assinatura apunho. Ela utiliza uma técnica de criptografia para conferir segurança e integridade aos documentos eletrônicos.

Para assinar digitalmente um documento, é necessário, antes de tudo, possuir um certificado digital. O certificado, na prática, consiste em um arquivo contendo os dados referentes à pessoa ou empresa, protegidos por criptografia altamente complexa e com prazo de validade pré determinado.

Os elementos que protegem as informações do arquivo são duas chaves de criptografia, uma pública e outra privada. Elas são geradas aleatoriamente por funções matemáticas. Elas são únicas, e uma só funciona em conjunto com a outra, como um encaixe. A chave privada é guardada sob a posse do usuário, enquanto a pública é compartilhada com quem o usuário desejar no formato de certificado digital.

Ao fazer o upload do documento eletrônico no assinador digital, o software vai ler o documento e associá-lo às chaves criptográficas do certificado digital. Ele emprega a função hash, para produzir uma representação reduzida e única do conteúdo a ser assinado.

Uma função de hash é um algoritmo matemático que transforma qualquer bloco de dados em uma série de caracteres de comprimento fixo. Independentemente do comprimento dos dados de entrada, o mesmo tipo de hash de saída será sempre um valor hash do mesmo comprimento. Também são usadas ​​para garantir a integridade da mensagem, é possível garantir que um arquivo não seja adulterado através de uma examinação dos hash criados antes e depois da transmissão de dados. Se os dois hash são idênticos, então a transmissão é autêntica, significando que não houve adulteração.

É sobre esse identificador que se aplica um segundo procedimento, usando a chave privada do usuário para produzir a assinatura digital. Por fim, é gerado um pacote assinado contendo o documento, a assinatura e o certificado do assinante. Este pacote será utilizado para verificar o processo.

**4. VALIDAÇÃO**

A validade da assinatura é determinada verificando a autenticidade do status do certificado de ID digital da assinatura e a integridade do documento. É possível comparar o resumo criptográfico da documentação original com o do documento que foi cifrado pelo assinante.

Nesse caso, o validador de assinatura vai usar a chave pública do certificado digital do assinante do documento, à qual estão atreladas suas informações a fim de reverter o processo de criptografia. Nos casos em que ambos os resumos criptográficos são iguais, isso quer dizer que há integridade na assinatura digital. No entanto, caso contrário, há uma assinatura inválida.