Assinatura eletrônica baseada em certificação digital – Parte II

Para garantir, em relação aos arquivos eletrônicos (particularmente, os documentos eletrônicos), autenticidade (identificação do autor), integridade (verificação de ausência de modificações no conteúdo) e até privacidade (ocultação do conteúdo), a assinatura digital, modalidade de assinatura eletrônica, utiliza modernas técnicas de criptografia.

Numa visão simples, a criptografia envolve procedimentos milenares de codificação de textos e mensagens. Assim, um texto criptografado somente será de conhecimento do remetente e do destinatário. Um terceiro que tenha contato com o texto criptografado não terá ciência do conteúdo real. Em regra, esse terceiro constata uma série de números, letras e símbolos aleatórios e sem sentido.

Na criptografia, as operações necessárias para transformar o texto legível em texto cifrado adotam a nomenclatura de *algoritmo* (a palavra possui um sentido amplo: conjunto de passos, etapas ou providências necessários para realizar uma determinada tarefa). Outro termo freqüentemente utilizado nesse campo é *chave*. Trata-se do parâmetro específico para realizar a transformação do texto legível em texto codificado.

Existem dois tipos básicos de criptografia, considerando os algoritmos e chaves utilizados nos procedimentos de codificação e decodificação.

A modalidade mais tradicional de criptografia, utilizada durante séculos, é chamada de *simétrica*. A característica básica da criptografia simétrica reside na utilização de uma só chave para cifrar e decifrar o texto ou mensagem.

Vejamos um exemplo simples de criptografia simétrica. A palavra DIREITO quando criptografada com a “cifra de César”

aparece como GMUHMXR. A “cifra de César” consiste na substituição de cada letra do texto pela terceira à sua frente no alfabeto.

A criptografia simétrica envolve uma significativa fragilidade ou insegurança. Com efeito, a chave (única) que codifica e decodifica os textos ou mensagens deve ser conhecida pelo remetente e pelo destinatário. Assim, surge o delicado problema de como distribuir de forma segura a chave (única) a ser utilizada.

A superação da fragilidade ou insegurança da criptografia simétrica (de chave única) surgiu com o desenvolvimento da criptografia *assimétrica*. Nessa modalidade de criptografia utilizam-se duas chaves distintas e relacionadas entre si (um par de chaves).

Brasília, 18 de fevereiro de 2007.

Aldemario Araujo Castro
Mestre em Direito
Professor de Informática Jurídica e Direito da Informática da Universidade Católica de Brasília
Coordenador da Especialização (a distância) em Direito do Estado da Universidade Católica de Brasília
Procurador da Fazenda Nacional
Membro do Conselho Consultivo da Associação Paulista de Estudos Tributários – APET
Co-autor do livro Manual de Informática Jurídica e Direito da Informática

Site: http://www.aldemario.adv.br