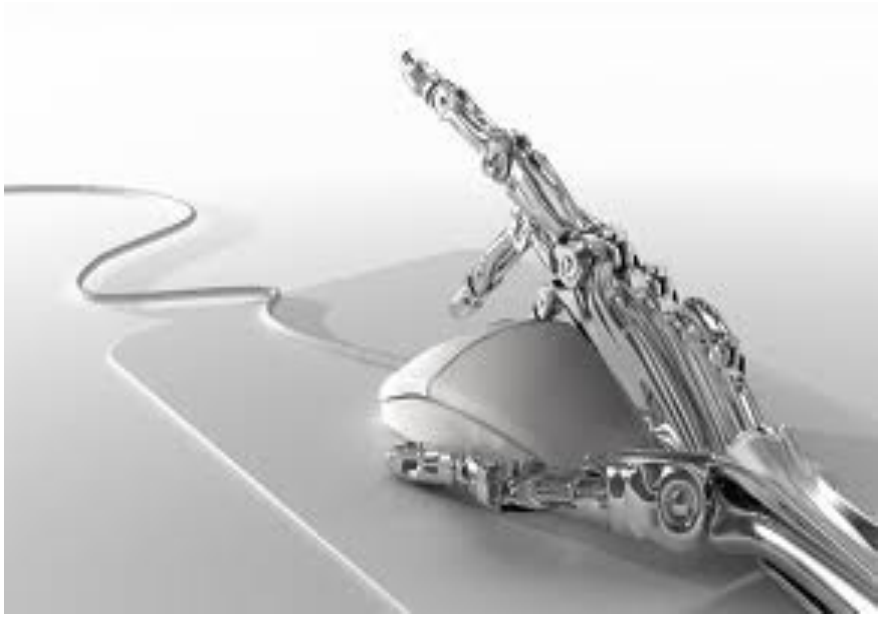
Criptografia assimétrica e certificação digital



Alunas: Bianca Souza

Bruna serra

Introdução

Desenvolvimento

Conclusão

Bibliografia

Introdução

Este trabalho apresenta os principais conceitos envolvendo criptografia assimétrica e certificação digital, fundamentais para a compreensão e implementação do comércio eletrônico seguro na Internet.

Desenvolvimento

O que é criptografia?

A palavra criptografia tem origem grega e significa a arte de escrever em códigos, de forma a esconder a informação na forma de um texto incompreensível. A informação codificada é chamada de texto cifrado. O processo de codificação ou ocultação é chamado de cifragem, e o processo inverso, ou seja, obter a informação original a partir do texto cifrado, chama-se decifragem.

Tipos de criptografia

Existem dois tipos de criptografia, a simétrica e a assimétrica. A criptografia simétrica é usada Os algoritmos de chave simétrica também chamados de sistemas de chave simetrica, criptografia de chave única, ou criptografia de chave secreta) são uma classe de algoritmos para a criptografia, que usam chaves criptográficas relacionadas para as operações de cifragem e decifragem. A operação de chave simétrica é mais simples, pois pode existir uma única chave entre as operações. A chave, na prática, representa um segredo, partilhado entre duas ou mais partes, que podem ser usadas para manter um canal confidencial de informação. Usa-se uma única chave, partilhada por ambos os interlocutores, na premissa de que esta é conhecida apenas por eles.[1]

Outros termos para criptografia de chave simétrica são: criptografia de chave secreta, de chave única, de chave compartilhada, de uma chave e de chave privada. O uso do último termo pode às vezes se confundir com o componente chave privada da criptografia de chave pública. A criptografia de chave simétrica é para ser separada de criptografia de chave assimétrica

> Assimétrica, . Este tipo de criptografia usa um par de chaves diferentes em que, não sendo possível obter uma chave a partir da outra, as duas estão relacionadas matematicamente, conseguindo uma decifrar o que foi cifrado pela outra. Com esta característica é possível que uma das chaves seja publicada, a chave pública.
>
> Esta forma de criptografia tem como vantagens o facto da chave privada se manter protegida e ser só do conhecimento do seu titular. Como desvantagens tem o facto do seu desempenho ser mais lento em consequência de utilizar um processo algorítmico mais complexo.

Funcionamento da criptografia assimétrica

A criptografia de chave pública ou criptografia assimétrica é um método de criptografia que utiliza um par de chaves: uma chave pública e uma chave privada. A chave pública é distribuída livremente para todos os correspondentes via e-maill ou outras formas, enquanto a chave privada deve ser conhecida apenas pelo seu dono.

Num algoritmo de criptografia assimétrica, uma mensagem cifrada com a chave pública pode somente ser decifrada pela sua chave privada correspondente.

Os algoritmos de chave pública podem ser utilizados para a autenticidade e confidencialidade:

Confidencialidade: A chave pública é usada para cifrar mensagens, com isso apenas o dono da *chave privada* pode decifrá-la.

Altenticidade: A chave privada é usada para cifrar mensagens, com isso garante-se que apenas o dono da chave privada poderia ter cifrado a mensagem que foi decifrada com a 'chave pública', e que a mensagem não foi forjada.

Certificação digital

Os computadores e a Internet são largamente utilizados para o processamento de dados

e para a troca de mensagens e documentos entre cidadãos, governo e empresas. No entanto, estas transações eletrônicas necessitam da adoção de mecanismos de segurança

capazes de garantir autenticidade, confidencialidade e integridade às informa-

ções eletrônicas. A certificação digital é a tecnologia que provê estes mecanismos.

No cerne da certificação digital está o certificado digital, um documento eletrônico que

contém o nome, um número público exclusivo denominado chave pública e muitos outros

dados que mostram quem somos para as pessoas e para os sistemas de informação. A chave pública serve para validar uma assinatura realizada em documentos eletrônicos.

A certificação digital tem trazido inúmeros benefícios para os cidadãos e para as

instituições que a adotam. Com a certificação digital é possível utilizar a Internet como

meio de comunicação alternativo para a disponibilização de diversos serviços com uma

maior agilidade, facilidade de acesso e substancial redução de custos. A tecnologia da certificação digital foi desenvolvida graças aos avanços da criptografia nos últimos 30 anos.

Conclusão

A criptografia assimétrica é uma ferramenta poderosa na segurança de um sistema distribuído. A sua utilização justifica-se claramente para a obtenção de confidencialidade, integridade e autorização. A confidencialidade é garantida através da criptografia forte, dependendo do algoritmo e da chave utilizada; a integridade passa pela utilização de assinaturas digitais; finalmente, uma autoridade de certificação (externa) permite estabelecer uma relação unívoca entre as A utilização generalizada na Internet de protocolos envolvendo criptografia assimétrica promove e justifica o seu desenvolvimento.

Bibliografia

WWW.pjvenda.net

WWW.training.com.br

WWW.iti.gov.br