Correio electrónico

O que são as chaves pública e privada para uso no correio eletrónico?

Se não for feito o contrário, as mensagens de correio eletrónico circulam pela Internet sem qualquer proteção, podendo ser lidas por qualquer pessoa que tenha acesso a uma das máquinas por onde passam. Para garantir a privacidade das mensagens, utiliza-se uma chave para encriptar a mensagem que só o destinatário pode decifrar. Para isso, o destinatário tem de publicar a sua chave pública (por exemplo, no seu site) para que os outros a possam usar. Mas também tem de guardar a sua chave privada, que é a única que lhe permite decifrar as mensagens encriptadas com a chave pública correspondente. Para assinar digitalmente uma mensagem, o remetente encripta-a com a sua chave privada, que só ele deve conhecer. Depois, o destinatário pode decifrar a mensagem com a chave pública do remetente, garantindo assim que a mensagem foi efetivamente enviada por ele. Para assinar e encriptar uma mensagem, o remetente encripta-a com a sua chave privada e depois com a chave pública do destinatário. Depois, o destinatário decifra a mensagem com a sua chave privada e com a chave pública do remetente, garantindo assim que a mensagem foi enviada por ele e que só o destinatário a pode ler. Para mais informações sobre estas operações, consulte a documentação do seu programa de correio eletrónico. Recomendamos o seu uso!

ID de solução Único: #1389
Autor: SERU - João Martins
Atualização mais recente: 2011-12-05 11:09

(c) 2022 Universidade do Porto. Reitoria. UPdigital. AI - Assistência Informática <helpdesk.reit@sp.up.pt> | 2022-01-28 04:34
URL: https://faqs.up.pt/faq/content/2/299/pt/o-que-são-as-chaves-pública-e-privada-para-uso-no-correio-eletrónico.html