O que são chaves?

Chaves são arquivos gerados por determinados programas para garantir a autenticidade e a confiabilidade de um certo usuário ao mandar mensagens ou acessar máquinas específicas. As características de autenticidade e confiabilidade são asseguradas por algoritmos simétricos ou assimétricos de criptografia.

Criptografia simétrica é o método de validação da interação de um usuário por meio de uma mesma chave, tanto para cifrar quanto para decifrar suas mensagens. Também conhecida como criptografia por chave privada.

Criptografia assimétrica consiste no uso de um par de chaves, pública e privada, bem relacionadas. Nesse método, as mensagens criptografadas com uma das chaves somente podem ser decriptografadas com a chave correspondente. Também chamada de criptografia por chave pública.

Chaves DSA fazem uso do segundo tipo de criptografia mencionado e são utilizadas por programas como o ssh. Sua intenção é prover uma conexão mais segura entre origem e destino.

A segurança está principalmente nos conceitos de autenticidade e confiabilidade. A autenticidade se faz presente quando as mensagens são cifradas pela chave privada e decifradas pela chave pública.

Agora, quando o inverso acontece, tem-se a confiabilidade; pois apenas o verdadeiro dono da chave decifradora (dessa vez, a chave privada) é quem pode confirmar a veracidade da operação requerida (acesso em máquina, transferência de arquivos, etc).

Por que usar chaves?

Em algumas máquinas Linux, o acesso só é garantido quando esse método é posto em prática. Quando esse tipo de recurso não é disponibilizado pelo usuário, a melhor escolha é impedir sua entrada no sistema, pois a máquina que requisita a conexão pode não ser segura o suficiente.

Se ainda assim o usuário quiser entrar nessa máquina ou tem a certeza de que a procedência da conexão é confiável, ele então deverá gerar as chaves e disponibilizá-las no alvo desejado. Seguindo os passos presentes nos textos abaixo esse usuário terá a permissividade de navegar por entre os diretórios da máquina desejada assim como o faz na máquina da qual acessa.