Escola Politécnica da Universidade de São Paulo
Departamento de Engenharia de Telecomunicações e Controle

EP3 de PTC2550 - Redes de Comunicação de Dados e Transporte Multimídia - 1o semestre 2017

Nesse problema, você explorará o algoritmo de encriptação de chave pública de Diffie-Hellman (DH), que permite que duas entidades concordem com uma chave simétrica compartilhada. O algoritmo DH faz uso de um número primo grande p e outro número grande g menor do que p. Tanto p quanto g são tornados públicos (de modo que um intruso os saberia). No DH, Alice e Bob escolhem cada um, de modo independente, suas chaves secretas S_A e S_B, respectivamente. Alice então computa sua chave pública, T_A, elevando g a S_A e então tomando mod p. De forma similar, Bob computa sua própria chave pública T_B elevando g a S_B e tomando mod p. Alice e Bob então trocam suas chaves públicas pela Internet. Alice calcula a chave secreta compartilhada S elevando T_B a S_A e então tomando mod p. De forma similar, Bob calcula a chave compartilhada S' elevando T_A a S_B e então tomando mod p.

a) Prove que, em geral, Alice e Bob obtém a mesma chave simétrica, ou seja, prove que $S' = S$.

b) Com $p = 11$ e $g = 2$, suponha que Alice e Bob escolham chaves privadas $S_A = 5$ e $S_B = 12$, respectivamente. Calcule as chaves públicas de Alice e Bob, T_A e T_B, respectivamente. Mostre todos os passos.

c) Continuando o item anterior, agora calcule S, a chave simétrica compartilhada.

d) Forneça um diagrama de tempos que mostre como o esquema DH pode ser atacado, no esquema *man-in-the-middle*. O diagrama de tempos deve ter 3 linhas verticais, uma para Alice, uma para Bob e outra para a intrusa, Trudy. Detalhe todo o raciocínio de Trudy.