

Quiz#4

Autenticação

O e-mail do participante (**igor.ribeiro@unifesp.br**) foi registrado durante o envio deste formulário.

O que significa o termo autenticação? *

- ☐ Certificando-se de que os dados são precisos.
- ☐ Garantir que os dados sejam mantidos em sigilo, para que apenas o proprietário dos dados possa vê-los.
- ☐ Certificar-se de que alguém que usa o computador é quem diz ser por meio de senhas e outras técnicas.
- ☒ Todas as alternativas

O que é autenticação multifator?

- ☐ Requer que um usuário carregue uma chave de identificação para fazer login em um sistema.
- ☒ Requer que o usuário faça login (autentique) com mais de um tipo de identificação.
- ☐ Requer um ser humano para identificar alguém antes que eles possam usar um sistema de computação.
- ☐ Requer impressão digital ou outra identificação biométrica.

Qual das opções a seguir NÃO é uma maneira de aumentar a proteção por senha?

- ☐ Use uma senha complexa.
- ☐ Altere sua senha regularmente.
- ☒ Use a mesma senha para vários sites e sistemas de computador.
- ☐ Treine as pessoas sobre como criar uma boa senha.



Em uma troca de chave DH entre A e B, em que $g=3$, $p=353$ e a chave $K=305$. Sendo a chave pública de A = 302 e a chave privada de B=29. A chave privada de A e a chave pública de B são respectivamente:

- ☐ 29 e 67
- ☒ 67 e 149
- ☐ 53 e 149
- ☐ 149 e 29
- ☐ Nenhuma das alternativas

Dado a função Hash SHA1. O valor do digest para a mensagem "Esse eh um teste de hash.", é:

- ☒ D24D13216654FB07950471D5C5F59376555C8BF3
- ☐ D27D12116654FB07950471D5C5F79376555C8BF5
- ☐ D27D12116654FB07950471D5C5F59376555C8BF5
- ☐ D27D12114554FB07950471D6C5F59376555C8BF4
- ☐ Nenhuma das Alternativas

Sobre MAC e Funções Hash é incorreto afirmar:

- ☐ O SHA foi originalmente projetado pelo NIST & NSA em 1993
- ☒ Qualquer função hash pode ser utilizada na execução de um CMAC.
- ☐ A diferença entre MAC e CMAC é que o primeiro faz uso de funções hash unidirecionais enquanto que o segundo faz uso de cifras de bloco.
- ☒ CMAC é também conhecido como CBC-MAC.
- ☒ O resultado de uma função hash pode ser revertido por meio da reaplicação do mesmo algoritmo sobre o digest obtido.



Google Formulários



