Universidade Federal do
Agreste de Pernambuco
Av. Bom Pastor s/n - Boa Vista
55292-270 Garanhuns/PE
☎ +55 (87) 3764-5500
http://www.ufape.edu.br

Bacharelado em Ciência da Computação
CCMP3079 Segurança de Redes de Computadores
Prof. Sérgio Mendonça

Atividade Cap. 10
Para 5/2/2024

Nome Completo: _____

Questões retiradas do livro-texto da disciplina.
Conforme conversamos em sala de aula, as atividades devem ser realizadas para apresentação e discussão em sala, sempre nas aulas das quintas-feiras, atribuindo ao estudante uma nota de 0 ou 1 por cada atividade realizada e apresentada.

1. Os usuários A e B utilizam a técnica de troca de chaves Diffie-Hellman com um primo comum $q = 71$ e uma raiz primitiva $\alpha = 7$.
   (a) Se o usuário A tem chave privada $X_A = 5$, qual é a chave pública de A, Y_A?
   (b) Se o usuário B tem chave privada $X_B = 12$, qual é a chave pública de B, Y_B?
   (c) Qual é a chave secreta compartilhada?
2. Considere um esquema Elgamal com um primo comum $q = 71$ e uma raiz primitiva $\alpha = 7$.
   (a) Se B tem chave pública $Y_B = 3$ e A escolheu um inteiro aleatório $k = 2$, qual é o texto cifrado de $M = 30$?
   (b) Se A, então, selecionar um valor diferente de k, de modo que a codificação de $M = 30$ seja $C = (59, C_2)$, qual é o inteiro C_2?
3. Demonstre que as duas curvas elípticas da Figura 10.4 satisfazem, cada uma, às condições para um grupo sobre os números reais.
4. $(4, 7)$ é um ponto na curva elíptica $y^2 = x^3 - 5x + 5$ sobre números reais?

Livro-texto da disciplina:
STALLINGS, William. Criptografia e segurança de redes. Princípios e práticas, Ed. 6. 2014.