INE 5429 - Prova 02

prof. Ricardo Felipe Custódio

13 de junho de 2013

1. Com relação ao protocolo de acordo de chaves Diffie-Hellman
   (a) Seja $q = 97$. Determine α uma raiz primitiva de q usando o método apresentado como trabalho inividual;
   (b) Determine as chaves secretas das partes comunicantes Alice e Beto. Tais chaves devem ser maiores que a raiz primitiva.
   (c) Determine a chave de acordo entre Alice e Beto.
   (d) Explique o ataque do Homem no Meio (Man in the Middle Attack). Como esse ataque pode ser evitado?
2. Usando RSA. Escolha dois número primos p e q. O primeiro primo p deve ser maior que 70 e menor que 99. O segundo primo deve ser maior que 100.
   (a) Determine um par de chaves RSA usando esses parâmetros.
   (b) Cifre o texto $M = 21$ usando uma das chaves
   (c) Decifre o texto $C = 40$ usando a outra chave

Mostre **TODOS** os cálculos.
O valor entre parêntesis antes de cada questão é o peso da questão.
Boa Sorte