INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

REDE FEDERAL DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA

SEGURANÇA DE REDES

EXERCÍCIO

Nome: _____
Turma: _____

Objetivando consolidar os conceitos de criptografia de chaves públicas (assimétrica), considere que dois usuários (Alice e Bob) de uma mesma máquina Linux desejam trocar arquivos criptografados. Utilizando a máquina virtual fornecida pelo professor, elabore um tutorial para realizar as seguintes operações:

1. Criação das contas dos usuários.

2. Criação do par de chaves utilizando a ferramenta gpg (GNUPG).

3. Realização da troca de chaves entre os usuários.

4. Realização, entre os usuários, dsa operação com arquivos:

    a. Apenas assinados;
    b. Apenas criptografados;
    c. Criptografados e assinados.

5. Com relação aos servidores de chaves PGP:
    a. Como exportar uma chave para o keyserver;
    b. Como importar uma chave do keyserver;
    c. Faça uma lista com os principais servidores.

6. Com relação ao chaveiro de um usuário:
    a. Como listar as chaves existentes;
    b. Como exportar as chaves públicas;
    c. Como exportar as chaves privadas;
    d. Como importar chaves públicas;
    e. Como importar chaves privadas;
    f. Como editar chaves.

7. Como implementar um esquema do PGP com clientes de e-mail.