Centro Universitário da Zona Oeste – UEZO
Disciplina de Segurança da Informação

# Atividade Prática Pontuada

## Introdução

Esta atividade será pontuada de acordo com o combinado com o professor. Sua forma de entrega será EXCLUSIVAMENTE através do e-mail trabgnupg@gmail.com. Durante o decorrer do prazo para entrega, cabe ao aluno procurar resolvê-la e buscar o suporte do professor para resolução de suas eventuais dificuldades. Há um vídeo em meu canal no Youtube explicando alguns detalhes.
Questões relevantes: o trabalho é INDIVIDUAL e depende do uso de um software livre e gratuito, o GnuPG, que pode ser obtido em http://www.gpg4win.org para Windows ou http://www.gnupg.org para outros SO. Naturalmente, é IMPOSSÍVEL haver duas execuções iguais para um trabalho individual, logo, o plágio de um único tópico invalida todos os trabalhos envolvidos.

## Atividade

**Passos a cumprir**: Instalar o GnuPG. Criar o seu par de chaves. Disponibilizar a chave pública no chaveiro público https://memoria.rnp.br/keyserver.php. Criar um arquivo texto contendo seus dados pessoais (nome, curso, turma e matrícula), bem como o URL do chaveiro público utilizado. Obter a minha chave pública (trabgnupg@gmail.com) em https://memoria.rnp.br/keyserver.php. Criptografar e Assinar o arquivo com as respostas das perguntas abaixo. Enviar para o email trabgnupg@gmail.com o arquivo criptografado e assinado bem como um arquivo texto com a sua chave pública.

## Atividades pontuadas

1. Ao criar o seu par de chaves:
    a. Que chaves são criadas?
    b. Qual é a relação entre elas?
    c. Quais são os cuidados a tomar com cada uma delas?
    d. Cite três algoritmos deste tipo.
2. Ao criptografar e assinar o arquivo texto:
    a. Qual TIPO de chave foi utilizada para criptografar seu texto?
    b. Cite três algoritmos do tipo usado nesta tarefa.
    c. Como ela é trocada entre você e eu?
    d. Qual TIPO de chave foi usada para assinar o arquivo?
    e. Como se processa essa autenticação, passo-a-passo?
    f. Como eu verifico se o seu arquivo não foi adulterado por terceiros?
3. Explique o processo de recebimento da mensagem:
    a. O que é feito primeiro pelo recebedor, a verificação da assinatura ou a decriptografia do arquivo? Por que?
    b. Qual é o TIPO de chave usada para decriptografar o arquivo?
    c. Como se pode conferir maior confiança à autenticidade da chave pública ?

Eventuais dúvidas devem ser trazidas ao professor com a devida antecedência.

Prof. Dr. Eng. Fred Sauer
fsauer@gmail.com