

###### 1º/2º Ciência da Computação(CC)

## Orientações para a disciplina de Atividades Práticas Supervisionadas

* TEMA
* PROPOSTA DO TRABALHO
* APRESENTAÇÃO DO TRABALHO

**AtividadesPráticasSupervisionadas (APS)**

**I. TEMA:**

**“ASTÉCNICAS CRIPTOGRÁFICAS, CONCEITOS, USOS E APLICAÇÕES (Introdução a Programação Estruturada - IPE)”**

**II. PROPOSTA DO TRABALHO**

As Atividades Práticas Supervisionadas serão constituídas pelos seguintes tópicos:

1. O grupo de alunos deverá, através de fontes formais de informação, aplicar o conceito de criptografia num caso específico que envolve o envio de uma mensagem utilizando um drone com informações estritamente confidenciais através de uma chave de segurança para o servidor de dados (informações de toda a população brasileira: informações pessoais, bancárias, particulares, de redes sociais, email, localização, celular etc). De posse desta chave, poderão acessar todas as informações do cotidiano da população. O drone deve sair com a chave impressa, de uma área restrita não divulgada e se dirigir a Central de Tecnologia e Gestão da Informação para validação e acesso ao servidor.
2. O grupo deverá escolher uma técnica de criptografia e expor em sala de aula as questões relativas ao uso da mesma, tendo como cenário a rede mundial de computadores, nos seguintes aspectos:
   1. Qual a abordagem utilizada em sua concepção (estruturação, conceitos e fundamentação).
   2. Os benefícios que a mesma trouxe em relação a outras técnicas anteriores.
   3. Principais aplicações e sistemas que a utilizam ou utilizaram-na e a motivação para tal escolha.
   4. Discussão comparativa entre esta técnica e outras conhecidas / utilizadas, expondo de forma analítica as especificidades de cada uma e sua utilização mais adequada.
   5. Eventuais vulnerabilidades e falhas detectadas neste tipo de técnica.
   6. Quais as melhorias futuras foram ou têm sido proposta se eventuais consequências.
3. O grupo deverá fazer uma dissertação sobre todos os elementos citados acima, assim como o efeito desse trabalho na sua formação e discutir a interdisciplinaridade envolvida no mesmo.
4. O grupo deverá elaborar um programa, que baseado nos conceitos descritos de 1 a 3, possa efetuara criptografia / descriptografia de qualquer mensagem, cifrada ou não, baseada na técnica escolhida pelo aluno.
5. A apresentação do trabalho deverá expor em tempo real o processo de criptografia. O programa deverá contemplar a possibilidade de cifragem de frases completas até o limite de 128 caracteres, e também a sua respectiva descriptografia. A frase e eventual chave serão fornecidas pelo professor responsável.
6. O nível de refinamento, funcionalidade, tratamento de erros e funções extra neste sistema, assim como o nível de complexidade da técnica criptográfica escolhida, terá impacto direto na nota final deste trabalho.
7. A nota atribuída ao trabalho entregue configura a nota das APS. A avaliação será feita de forma individual.

**III. APRESENTAÇÃO DO TRABALHO**

1. O grupo deverá ser composto de até 5 alunos, que serão escolhidos aleatoriamente pelo professor, simulando ambiente de trabalho, onde compartilhamos informações e conhecimento com pessoas de várias áreas ou áreas afins. A formação de um grupo comum número diferente de 5 dependerá de aprovação do (a) Coordenador (a) Auxiliar do curso no campus.
2. Todas as etapas do trabalho deverão ser escritas em fonte ARIAL12, espaçamento 1,5, margem direita 2,5cm e margem esquerda 2,5cm. (digite “BIBLIOTECA CENTRAL GUIA DE NORMALIZAÇÃO PARA APRESENTAÇÃO DE TRABALHOS ACADÊMICOS DA UNIVERSIDADE PAULISTA”) O trabalho deverá ter formato A4, encadernado (espiral) com capa transparente.
3. Limites de páginas

Objetivo do trabalho:1 página e no máximo 2 páginas

Introdução: 2 páginas e no máximo 4 páginas

Criptografia (conceitos gerais):3 páginas e no máximo 5 páginas.

Técnicas criptográficas mais utilizadas: mínimo de 4 páginas e máximo de 8 páginas.

Dissertação: mínimo de 5 páginas e máximo de 15 páginas.

Projeto (estrutura) do programa: mínimo de 3 páginas e máximo de 8 páginas.

Relatório com as linhas de código: máximo de 10 páginas.

1. O trabalho deverá ser entregue junto com a ficha padrão de “Atividades Práticas Supervisionadas” ilustrando cronologicamente cada um dos itens, segundo a orientação do professor supervisor desta atividade.
2. Estrutura do trabalho:
   1. Capa:identificando o curso,o tema,a relação de alunos do grupo(nome/RA)
   2. Índice
   3. Objetivo do trabalho
   4. Introdução
   5. Criptografia (conceitos gerais)
   6. Técnicas criptográficas mais utilizadas e conhecidas
   7. Dissertação (\*\*\*Sua técnica criptográfica escolhida\*\*\*)
      1. Estruturação, conceitos e fundamentação
      2. Benefícios em relação às técnicas anteriores.
      3. Aplicações que fazem / fizeram uso da técnica.
      4. Discussão comparativa entre esta técnica e outras conhecidas / utilizadas
      5. Vulnerabilidades e falhas.
      6. Melhorias propostas e/ou implementadas.
   8. Projeto (estrutura) do programa
   9. Relatório com as linhas de código do programa
   10. Apresentação do programa em funcionamento em um computador, apresentando todas as funcionalidades pedidas e extras.
   11. Bibliografia
   12. Ficha de Atividades Práticas Supervisionadas

**IV.MODELO DE FICHA DE ATIVIDADES PRÁTICAS SUPERVISIONADAS**

