UNIP
UNIVERSIDADE PAULISTA

1º/2º Ciências da Computação (CC) e Sistemas de Informação (SI)

Orientações para a disciplina de Atividades Práticas Supervisionadas 2019

- TEMA
- PROPOSTA DO TRABALHO
- APRESENTAÇÃO DO TRABALHO

Atividades Práticas Supervisionadas (APS)

TEMA:

“AS TÉCNICAS CRIPTOGRÁFICAS, CONCEITOS, USOS E APLICAÇÕES”

PROPOSTA DO TRABALHO

As Atividades Práticas Supervisionadas serão constituídas por duas partes que possuirão o mesmo peso na avaliação: uma parte de pesquisa e produção de conteúdo acadêmico, e outra prática, envolvendo o desenvolvimento de um programa em Python, sob a orientação dos professores da disciplina de IPE. Ambas as partes estão descritas nos Capítulos I e II deste manual.

I. PESQUISA E PRODUÇÃO DE CONTEÚDO ACADÊMICO

1) O trabalho consiste em três etapas:

   - Uma pesquisa em geral sobre o tema criptografia (histórico, fundamentos, conceitos, aplicações);

   - Escolha de uma técnica de criptografia específica e exposição das questões relativas ao uso da mesma, tendo como cenário a rede mundial de computadores, nos seguintes aspectos:

      a. Qual a abordagem utilizada em sua concepção (estruturação, conceitos e fundamentação).
      b. Os benefícios que a mesma trouxe em relação a outras técnicas anteriores.
      c. Principais aplicações e sistemas que a utilizam ou utilizaram-na e a motivação para tal escolha.
      d. Discussão comparativa entre esta técnica e outras conhecidas/utilizadas, expondo de forma analítica as especificidades de cada uma e sua utilização mais adequada.

e. Eventuais vulnerabilidades e falhas detectadas neste tipo de técnica.
f. Quais as melhorias futuras foram ou têm sido propostas e eventuais consequências.

- Após a realização das pesquisas, o grupo deve tecer comentários e propostas de solução para o problema apresentado abaixo (esta parte do trabalho deve ser inserida no tópico “Dissertação”; ver Capítulo III deste manual).

“O grupo de alunos deverá, através de fontes formais de informação, aplicar a utilização do conceito de criptografia num caso específico que envolve restrição de acesso a uma área contaminada ambientalmente que contenha riscos a saúde pública: um navio foi aprendido pela guarda costeira brasileira por transportar lixo tóxico da Ásia para a região norte do Brasil. O acesso à tripulação, assim como a todo conteúdo tóxico radiativo, deverá ser controlado. Somente inspetores devidamente trajados com roupas especiais poderão adentrar no navio. Por razões legislativas o navio deve permanecer a uma distancia segura: 50 quilômetros da costa e todo e qualquer contato deverá ser realizado por meio de helicópteros, para minimizar e restringir o contato. A área do entorno num raio de 10 quilômetros está isolada.”

2) 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 (mais detalhes no capítulo III deste manual).

II. PRODUÇÃO DE UM PROGRAMA DE CRIPTOGRAFIA

1) O grupo deverá elaborar um programa em Python, que baseado nos conceitos descritos nos itens 1 e 2 do capítulo anterior, possa efetuar a criptografia/descriptografia de qualquer mensagem, cifrada ou não, baseada preferencialmente na técnica escolhida pelo grupo. A apresentação do trabalho deverá expor em tempo real o processo de criptografia.

2) O programa deverá contemplar a possibilidade de cifragem de frases completas até o limite de 128 caracteres, e também a sua respectiva descriptografia. O programa deverá fazer uso de uma chave criptográfica.

3) O nível de refinamento, funcionalidade, tratamento de erros e funções extras implementadas neste sistema, assim como o nível de complexidade da técnica criptográfica escolhida, terá impacto direto na nota final deste

III. APRESENTAÇÃO DO TRABALHO

1) O grupo deverá ser composto de **5 (cinco) alunos**. A formação de um grupo com um número diferente de 5 dependerá de aprovação do(a) Coordenador(a) Auxiliar do curso no campus e/ou dos professores orientadores.

2) Todas as etapas do trabalho deverão ser escritas em fonte ARIAL 12, espaçamento 1,5, margem direita 2,5cm e margem esquerda 2,5cm. As páginas do trabalho deverão ser formato A4. O trabalho deve seguir o formato de um trabalho acadêmico (seguindo normas ABNT) e deverá contemplar os tópicos listados nos itens 3 e 5 deste capítulo.

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.

4) 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.

5) Estrutura do trabalho:

- Capa: identificando o curso, o tema, a relação de alunos do grupo (nome/RA)
- Índice
- Objetivo do trabalho
- Introdução
- Criptografia (conceitos gerais)
- Técnicas criptográficas mais utilizadas e conhecidas
- Dissertação (***Sua técnica criptográfica escolhida e estudo de caso***)
  - Estruturação, conceitos e fundamentação
  - Benefícios em relação às técnicas anteriores.
  - Aplicações que fazem/fizeram uso da técnica.
  - Discussão comparativa entre esta técnica e outras conhecidas/utilizadas
  - Vulnerabilidades e falhas.
  - Melhorias propostas e/ou implementadas.
  - Estudo de caso.
  - Interdisciplinaridade da Atividade.
- Projeto (estrutura) do programa
  - Apresentação do programa em funcionamento em um computador, apresentando todas as funcionalidades pedidas e extras.
- Relatório com as linhas de código do programa
- Bibliografia
- Ficha de Atividades Práticas Supervisionadas **(com no mínimo 75 horas – 1 ficha por integrante do grupo)**

6) As formas de apresentação e entrega do trabalho (impressa, digital, seminário perante os demais alunos, demonstração do programa em funcionamento no laboratório, etc.) ficam a critério dos professores coordenadores, assim como as datas e prazos de entrega, tanto do trabalho final quanto de partes do trabalho.

7) O trabalho escrito deve obrigatoriamente ser postado em sua versão final no site http://trabalhosacademicos.unip.br/entrega/ até a data definida no calendário escolar. A nota será atribuída pelos professores através do site, e **a não postagem implicará em reprovação automática**.

IV. AVALIAÇÃO DO TRABALHO

1) Será dado mesmo peso ao trabalho escrito e ao programa desenvolvido, ou seja, cada um corresponderá à metade da nota atribuída ao trabalho. A não entrega de uma das partes nos prazos estipulados, mesmo que esta seja postada no sistema (capítulo III, item 7, deste manual) irá implicar na atribuição de nota 0,0 (zero) a esta parte do trabalho.

2) Caso a parte escrita não esteja de acordo com os formatos indicados no capítulo 3, isto implicará em redução da nota da mesma durante a avaliação, mas não afetará a avaliação da parte prática (programa).

3) Caso a versão do trabalho entregue/apresentada aos professores responsáveis seja diferente da versão postada no sistema, isto poderá implicar em redução da nota atribuída ou até mesmo em reprovação do trabalho.

4) A identificação de plágios no trabalho de pesquisa ou no código apresentado irá implicar em redução da nota atribuída, ou até mesmo na atribuição de nota 0,0 (zero), a critérios dos professores envolvidos na correção. Por plágio entende-se o uso de qualquer material não escrito ou desenvolvido por integrantes do grupo que não seja explicitamente identificado como sendo de um autor externo.

V. MODELO DE FICHA DE ATIVIDADES PRÁTICAS SUPERVISIONADAS

FICHA DE ATIVIDADES PRÁTICAS SUPERVISIONADAS - APS

Atividades Práticas Supervisionadas (laboratórios, atividades em biblioteca, Iniciação Científica, trabalhos Individuais e em grupo, práticas de ensino e outras)

NOME:_____

RA:_____ **CURSO:**_____

CAMPUS:_____ **SEMESTRE:**_____ **TURNO:**_____

			ASSINATURA	
DATA	**ATIVIDADE**	**TOTAL DE HORAS**	**ALUNO**	**PROFESSOR**

TOTAL DE HORAS:_____