UNIP
UNIVERSIDADE PAULISTA

1º/2º Ciência da Computação (CC)

Orientações para a disciplina de

Atividades Práticas Supervisionadas

2019

- TEMA
- PROPOSTA DO TRABALHO
- APRESENTAÇÃO DO TRABALHO

Atividades Práticas Supervisionadas (APS)

I. TEMA:

“AS TÉCNICAS CRIPTOGRÁFICAS, CONCEITOS, USOS E APLICAÇÕES”

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 à 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 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:

    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.
g. A implementação deve ser na linguagem de programação Pyhton, mas é vedado o uso do pacote bcrypt, ou qualquer outra função pronta para o processo de criptografia.

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 nos itens de 1 a 3, possa efetuar a 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 extras implementadas 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.

III. APRESENTAÇÃO DO TRABALHO

1. O grupo deverá ser composto de 5 alunos. A formação de um grupo com um número diferente de 5 dependerá de aprovação do(a) Coordenador(a) Auxiliar do curso no campus.

   Todas as etapas do trabalho deverão ser escritas em fonte ARIAL 12, espaçamento 1,5, margem direita 2,5 cm e margem esquerda 2,5 cm. O trabalho deverá ter formato A4, encadernado (espiral) com capa transparente.

2. 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.

3. 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.

4. Estrutura do trabalho:

Capa: identificando o curso, o tema, a relação de alunos do grupo (nome/RA)

Índice

1. Introdução

1.1. Contexto

1.2. Problema (enunciado neste manual)

1.3. Objetivo(s)

1.4. Motivação

1.5. Organização do Relatório

2. Referencial Teórico

4.1.1. Criptografia (conceitos gerais)

4.1.2. Técnicas criptográficas pesquisadas (vulnerabilidades e falhas)

4.1.3. Técnica criptográfica escolhida.

Justifique o porquê da escolha. Uma dica é dissertar sobre os benefícios em relação às demais técnicas.

4.1.4. Discussão comparativa entre a técnica escolhida e outras pesquisadas.

4.2. Trabalhos relacionados

4.2.1. Aplicações que fazem/fizeram uso da técnica.

Nesta Seção, apresente uma pesquisa de ferramentas ou produtos de software que oferece o serviço de criptografia. Um exemplo: Criptografia ponto a ponto aplicada no WhatsApp.

4.3. Projeto <nome_do_projeto_definido_pelo_grupo>

4.3.1. A técnica escolhida no contexto da aplicação (meio ambiente).

4.3.2. Fluxograma e/ou Pseudocódigo do algoritmo de criptografia.

Nesta Seção, explique o seu algoritmo.

4.3.3. Melhoria(s) proposta(s) e/ou implementada(s) [se houver(em)].

4.4. Experimentos e Análise dos Resultados

Nesta Seção, mostre a Interface Gráfica do Usuário e os mecanismos de interações entre o usuário e o sistema.

Os resultados são as saídas do processo de criptografia e descriptografia, para cada entrada.

4.5. Considerações Finais

As considerações finais devem respondem às seguintes questões:

O problema apresentado na Introdução foi resolvido?

O(s) objetivo(s) do trabalho foi(ram) alcançado(s)?

Os resultados obtidos indicam que a solução é viável?

4.6. Referências bibliográficas

4.7. Anexo 1. Estrutura do Programa do Projeto <nome_ definido_pelo_grupo>

Relatório com as linhas de código do programa (fonte courier-new, tamanho 10, espaçamento simples entre linhas, não precisa de margens de parágrafos, alinhamento à esquerda.

4.8. Ficha de Atividades Práticas Supervisionadas

IV. MODELO DE FICHA DE ATIVIDADES PRÁTICAS SUPERVISIONADAS

FICHA DAS ATIVIDADES PRÁTICAS SUPERVISIONADAS - APS

NOME:_____ **TURMA:** _____ **RA:**_____

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

CÓDIGO DA ATIVIDADE:_____ **SEMESTRE:**_____ **ANO GRADE:**_____

DATA DA ATIVIDADE	DESCRIÇÃO DA ATIVIDADE	TOTAL DE HORAS	ASSINATURA DO ALUNO	HORAS ATRIBUÍDAS (1)	ASSINATURA DO PROFESSOR

(1) Horas atribuídas de acordo com o regulamento das Atividades Práticas Supervisionadas do curso.

TOTAL DE HORAS ATRIBUÍDAS:_____

AVALIAÇÃO:_____

Aprovado ou Reprovado

NOTA:_____

DATA:_____/_____/_____

_____

CARIMBO E ASSINATURA DO COORDENADOR DO CURSO