UNIP
UNIVERSIDADE PAULISTA

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

Orientações para a disciplina de

Atividades Práticas Supervisionadas

2013

- 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.

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.

2. 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.

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:

   5.1. Capa: identificando o curso, o tema, a relação de alunos do grupo (nome/RA)
   5.2. Índice
   5.3. Objetivo do trabalho
   5.4. Introdução
   5.5. Criptografia (conceitos gerais)
   5.6. Técnicas criptográficas mais utilizadas e conhecidas
   5.7. Dissertação (*** Sua técnica criptográfica escolhida***)
      5.7.1. Estruturação, conceitos e fundamentação

5.7.2. Benefícios em relação às técnicas anteriores.

5.7.3. Aplicações que fazem/fizeram uso da técnica.

5.7.4. Discussão comparativa entre esta técnica e outras conhecidas / utilizadas

5.7.5. Vulnerabilidades e falhas.

5.7.6. Melhorias propostas e/ou implementadas.

5.8. Projeto (estrutura) do programa

5.9. Relatório com as linhas de código do programa

5.10. Apresentação do programa em funcionamento em um computador, apresentando todas as funcionalidades pedidas e extras.

5.11. Bibliografia

5.12. Ficha de Atividades Práticas Supervisionadas

IV. 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:_____