**Universidade PAULISTA**

CIÊNCIAS DA COMPUTAÇÃO

**Atividade Prática Supervisionada**

CRIPTOGRAFIA

**CAMILA DOKI RA:**D44943-5

**GABRIELA CARVALHO RA:**D244ID-4

**STEPHANY VELOSO RA:** N198HC-0

**JOÃO GUSTAVO RA:**

Barueri

2017

**CAMILA DOKI RA:**D44943-5

**GABRIELA CARVALHO RA:**D244ID-4

**STEPHANY VELOSO RA:** N198H-C0

**JOÃO GUSTAVO RA:**D1858F-8

**Atividade Prática Supervisionada**

CRIPTOGRAFIA

Trabalho apresentado ao Curso de Ciências da Computação da UNIP - Universidade Paulista.

Prof. Edilson

Barueri

2017

Índice

[Objetivo Do Trabalho 3](#_Toc497672538)

[Tema escolhido 3](#_Toc497672539)

[Introdução 3](#_Toc497672540)

[Criptografia 6](#_Toc497672541)

[Conceitos Gerais 6](#_Toc497672542)

[Técnicas De Criptografia Mais Utilizadas 6](#_Toc497672543)

[Dissertação 6](#_Toc497672544)

[Projeto do Programa 6](#_Toc497672545)

[Relatório com as linhas de código do programa 6](#_Toc497672546)

[Bibliografia 6](#_Toc497672547)

# **Objetivo 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.

# **Tema escolhido**

Desenvolvimento de software de criptografia e descriptografia tomando como referencia Cifra de Hill.

# **Introdução**

# **Criptografia**

## Conceitos Gerais

A criptografia serve basicamente para transformar uma informação/frase/dado em ilegível, com a utilização de uma chave “secreta”, e somente o portador dessa chave consegue ler a informação criptografada.

Criptografia vem de um ramo da matemática logo é utilizada a matemática e seus conceitos para tornamos a frase ilegível.

## 

## Técnicas De Criptografia Mais Utilizadas

# **Dissertação**

# **Projeto Do Programa**

# **Relatório Com As Linhas De Código Do Programa**

# **Bibliografia**