CSI303 - Segurança e Auditoria de Sistemas
TP001 – 30 pontos

Profª. Janniele Aparecida Soares Araujo – janniele@ufop.edu.br
https://professor.ufop.br/janniele

5 de outubro de 2021

1 Orientações

- Data de Entrega: **22 de outubro de 2021 até às 12h**.
- Escolha o seu grupo na tarefa do moodle (máximo 4 alunos).
- O código deverá ser disponibilizado no GitHub para download.
- O relatório contendo as análises e o link do GitHub deverá ser anexado na tarefa do moodle.
- O programa pode ser implementado em qualquer linguagem.
- O trabalho será apresentado por videoconferência (Google Meet) por todos os membros do grupo:
  - As apresentações ocorrerão nos dias 22 de outubro.
  - Na apresentação deverá ser mostrado o código, seu funcionamento e o relatório técnico.
  - O membro do grupo que não comparecer **receberá nota zero.**
  - Em caso de **plágio ou cópia** o grupo **receberá nota zero.**

2 Temas e Grupos

A encriptação de dados tem como objetivo prover sigilos das mensagens quando se usa um meio de comunicação inseguro. Portanto, o processo de encriptação consiste em converter um texto claro em um texto encriptado usando uma chave secreta. O processo inverso, conhecido por decriptação, transforma um texto encriptado em um texto claro usando a mesma chave usada na encriptação.

O Trabalho Prático consiste em **implementar** o algoritmo assimétrico **RSA**,seu nome é formado com iniciais dos autores: Rivest, Shamir & Adleman (1978) e **implementar** o algorimto **ElGamal**. Faça um **relatório** com testes em diferentes tamanhos de textos e chaves, avalie e compare o desempenho dos algoritmos implementados para encriptar e decriptar.