Curitiba, 02, outubro de 2024.

**Disciplina**: Segurança da Informação

**Professor:** Jhonatan Geremias

**Estudante:**

**Trabalho Segurança da Informação**

**Análise de desempenho Criptográfico**

# **Descrição da Atividade:**

Esta atividade consiste em analisar o desempenho dos algoritmos de criptografia simétrico e criptografia de chave pública. Demostrar o impacto do tamanho das chaves utilizadas no algoritmo.

**Entrega:**

Esta atividade deverá ser entregue até o dia **09/10/2024** no Canvas. O estudante deverá entregar um arquivo “.pdf” contendo o relatório conforme o item de especificação.

**Especificação:**

Desenvolva um programa que utiliza a criptografia de chave pública e simétrica conforme requisitos abaixo:

1. O programa deve cifrar o texto: “RSA eh um algoritmo que leva o nome de 3 professores do MIT: Rivest, Shamir e Adleman”.
2. O programa deve calcular o tempo de execução do experimento, incluindo a geração de chaves.
3. O programa deve cifrar o texto utilizando as seguintes técnicas:
   1. Utilizando o algoritmo RSA com chave pública e privada de 1024 bits.
   2. Utilizando o algoritmo RSA com chave pública e privada de 2048 bits.
   3. Utilizando o algoritmo RSA com chave pública e privada de 4096 bits.
   4. Utilizando o algoritmo RSA com chave pública e privada de 8192 bits.
   5. Utilizando o algoritmo AES com chave de 128 bits.
   6. Utilizando o algoritmo AES com chave de 256 bits.
4. Cada uma das técnicas deve ser executada pelo menos três vezes. É recomendado que o processo não seja automatizado, para que o resultado não utilize cache.
5. Realizar um printscreen obtendo o valor de cada experimento.
6. Apresentar os valores em uma planilha para adicionar no relatório, calcular o tempo médio obtido de cada técnica.

Desenvolva um relatório descrevendo o experimento executado. O relatório deve descrever o resultado das execuções, realizando uma análise do tempo de resposta das diversas técnicas. O relatório deve ser entregue no formato PDF.

**Observação:** O programa pode ser desenvolvido na linguagem de programação Java ou Python.