**UNIVERSIDADE POSITIVO**

**CRIPTOGRAFIA E SEGURANÇA – Prof Escobar**

**ATIVIDADES SOBRE CRIPTOGRAFIA**

**Realização em equipe com entrega individual.**

**As atividades serão apresentadas**

**Cronograma e pontuação**

|  |  |  |
| --- | --- | --- |
| **Atividade** | **Data de apresentação** | **Pontos** |
| 1 | 10/04/2024 | 0,25 |
| 2 | 17/04/2024 | 0,25 |
| 3 | 17/04/2024 | 0,1 |

1. Observe o seguinte cenário:
   1. O sistema de gerenciamento de documentos da UniLE permite que tais documentos sejam copiados. No entanto, as cópias devem ser autenticadas. Esse mesmo sistema mantem informações em diferentes formatos : Doc, PDF e JPEG.
   2. Desenvolva uma aplicação capaz de autenticar um conteúdo. Essa aplicação deve garantir que uma cópia de um conteúdo qualquer não foi alterada.
2. Um dos desafios da criptografia é garantir o segredo de uma mensagem (dado qualquer) e que essa mensagem seja lida apenas por quem tem permissão para isso.

De certa forma, o Base64 permite isso, mas apresenta algumas fragilidades.

A técnicas de Hash, no entanto, não são recomendadas quando a decodificação é um requisito.

Dessa forma, podem-se considerar algoritmos que utilizem chaves para decodificação.

Então, pesquise e organize:

1. O que são chaves simétricas em criptografia?
2. Exemplos de algoritmos de criptografia que utilizem chaves simétricas?
3. O que são chaves assimétricas em criptografia?
4. Exemplos de algoritmos de criptografia que utilizem chaves assimétricas?
5. Considere um problema de comunicação segura:
   1. Deseja-se enviar uma mensagem criptografada no remetente
   2. Essa mensagem deve ser decodificada no destinatário
   3. Solucione a situação com uma aplicação que permita enviar uma mensagem criptografada e decodifica-la no destino utilizando chaves simétricas
   4. Solucione a situação com uma aplicação que permita enviar uma mensagem criptografada e decodifica-la no destino utilizando chaves assimétricas
   5. Compare os pontos fortes e fracos de cada implementação e julgue qual delas é mais eficiente (no sentido de econômica) e mais eficaz (no sentido de segura).