

# Trabalho Prático 6

---

CET 8493 | UFCD 9196 - Cibersegurança Ativa | Formador: Paulo Vaz

Formando: João Rodrigo Mota da Costa

## 2. Quais são os principais tipos de criptografia?

Existem vários tipos de criptografia, mas aqui estão os três principais tipos:

**Criptografia simétrica:** Também conhecida como criptografia de chave secreta, é o tipo de criptografia em que a mesma chave é usada para criptografar e descriptografar a mensagem. A chave deve ser mantida em segredo entre as partes que desejam comunicar de forma segura.

**Criptografia assimétrica:** Também conhecida como criptografia de chave pública, é o tipo de criptografia em que cada parte tem uma chave pública e uma chave privada. A chave pública é compartilhada com outras pessoas para que possam criptografar mensagens enviadas para a pessoa, mas apenas a chave privada da pessoa pode ser usada para descriptografar as mensagens criptografadas.

**Hashing:** Este tipo de criptografia é usado para proteger a integridade dos dados, em vez de mantê-los secretos. O hashing é um processo em que uma mensagem é transformada em uma sequência de caracteres, geralmente de comprimento fixo, chamada de hash. O hash é então usado para verificar se a mensagem foi alterada ou corrompida durante a transmissão. Uma das funções mais comuns de hashing é o MD5 (Message Digest 5), que produz um hash de 128 bits. No entanto, algoritmos mais seguros, como SHA-256 e SHA-512, são frequentemente usados em vez do MD5.

## 3. Qual é a importância da criptografia na segurança da informação?

A criptografia é fundamental para a segurança da informação, uma vez que permite que dados sensíveis sejam transmitidos, armazenados e processados de forma segura e confidencial. A criptografia transforma dados legíveis em um formato ilegível, que só pode ser lido por pessoas autorizadas que possuem a chave para descriptografar os dados.

A criptografia garante a privacidade da informação, protegendo-a de ser lida ou acessada por pessoas não autorizadas. Além disso, a criptografia também é importante para garantir a integridade dos dados, pois garante que a informação não tenha sido alterada ou corrompida durante a transmissão ou armazenamento.

## 5. Quais são os principais tipos de esteganografia?

Existem vários tipos de esteganografia, mas aqui estão os três principais tipos:

**Esteganografia de arquivos:** Este tipo de esteganografia envolve a ocultação de informações dentro de um arquivo, como uma imagem, áudio ou vídeo. As informações podem ser ocultas nas propriedades do arquivo, no cabeçalho ou nos bits de dados do arquivo.

**Esteganografia de rede:** Este tipo de esteganografia envolve a ocultação de informações dentro do tráfego de rede. Por exemplo, as informações podem ser ocultas em pacotes de rede, cabeçalhos de protocolo ou em espaços não utilizados em pacotes de dados.

**Esteganografia de texto:** Este tipo de esteganografia envolve a ocultação de informações dentro de texto comum, como um e-mail ou uma página da web. As informações podem ser ocultas usando técnicas como a substituição de palavras por sinônimos, a alteração da ordem das palavras ou a adição de espaços extras entre as palavras.

## 6. Qual é a importância da esteganografia na segurança da informação?

A esteganografia é importante na segurança da informação porque permite a ocultação de informações confidenciais em outras formas de dados, como arquivos de áudio, vídeo, imagens ou mesmo em texto comum, sem levantar suspeitas.

Ao contrário da criptografia, que protege dados por meio da transformação do conteúdo em um formato ilegível, a esteganografia oculta informações confidenciais dentro de dados aparentemente comuns, tornando-os menos suscetíveis de serem detectados por pessoas não autorizadas.