o que diferencia uma assinatura de um hash comum?

A **diferença entre uma assinatura digital e um hash comum** está no **propósito, função e segurança** envolvida em cada um:

**🔑 Resumo direto da diferença**

| **Aspecto** | **Hash comum** | **Assinatura digital** |
| --- | --- | --- |
| **Função principal** | Geração de resumo (digest) de dados | Garantir **autenticidade**, **integridade** e **autoridade** |
| **Chaves envolvidas** | Nenhuma chave | Usa **chave privada** para assinar e **chave pública** para verificar |
| **É reversível?** | Não (é unidirecional) | Também não, mas pode ser **verificado** com a chave pública |
| **Verifica integridade?** | Sim | Sim + **autenticidade do remetente** |
| **Propriedade de não repúdio** | Não | Sim – o autor **não pode negar** ter assinado |

**⚙️ Como funciona cada um**

**✅ Hash comum (ex: SHA-256)**

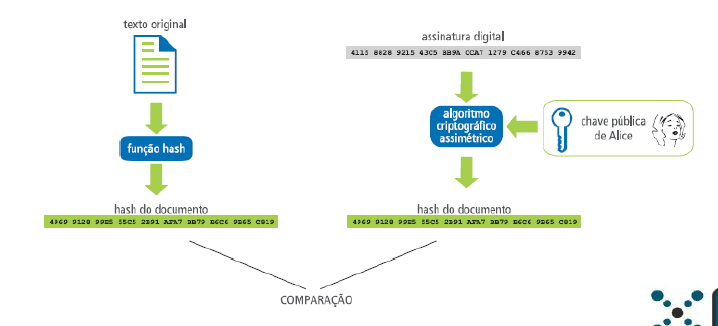
* Transforma qualquer entrada em uma **saída fixa e única**.
* Exemplo:  
  SHA256("arquivo.txt") → abc123...
* Serve para:
  + Verificar integridade
  + Comparar arquivos
  + Armazenar senhas de forma segura (junto com sal e KDF)

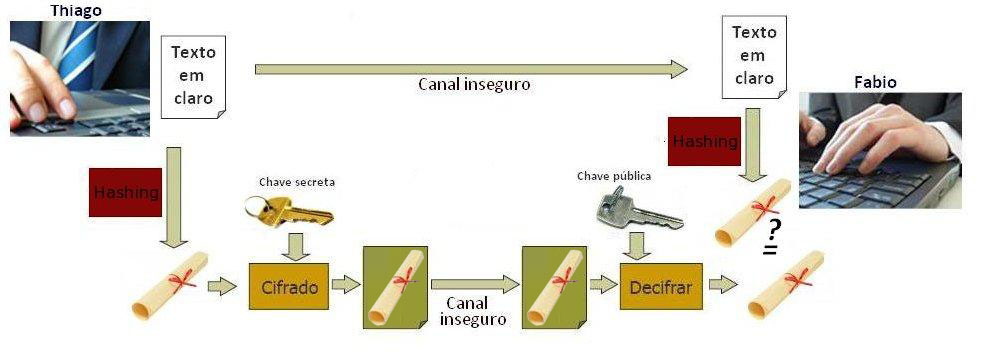
**✅ Assinatura digital**

* Envolve **criptografia assimétrica**:
  1. O remetente calcula um **hash dos dados**.
  2. Esse hash é **criptografado com a chave privada** → isso é a assinatura.
  3. O receptor:
     + Recalcula o hash do conteúdo.
     + Usa a **chave pública do remetente** para **verificar a assinatura**.
* Garante que:
  1. Os dados **não foram alterados**.
  2. Vieram de quem diz ter enviado (autenticidade).
  3. O remetente **não pode negar** (não repúdio).

**🎯 Conclusão**

* **Hash ≠ assinatura.**
* Um **hash é um resumo** (sem identidade);
* Uma **assinatura digital é um hash cifrado com chave privada**, o que **prova a origem** e **protege contra falsificação**.





**De Quem É A Chave Privada E De Quem É A Chave Pública Em Uma Assinatura Digital?**

Em uma **assinatura digital**, as chaves pertencem a **quem assina a mensagem**. Veja a correspondência exata:

**🔐 Assinatura digital: de quem é cada chave?**

| **Chave** | **Quem possui** | **Função** |
| --- | --- | --- |
| **Chave privada** | **Do remetente (quem assina)** | É usada para **criar a assinatura digital** |
| **Chave pública** | **Distribuída ao destinatário(s)** | É usada para **verificar a assinatura** |

**📦 Exemplo concreto**

Imagine que **Alice** envia uma mensagem para **Bob**:

1. **Alice tem:**
   * Sua **chave privada**, que ela guarda em segredo.
   * Sua **chave pública**, que ela distribui (ex: para Bob).
2. **Processo:**
   * Alice gera um **hash** da mensagem.
   * Alice **usa sua chave privada para assinar** esse hash → isso cria a **assinatura digital**.
   * Alice envia a **mensagem + assinatura** para Bob.
3. **Bob:**
   * Usa a **chave pública de Alice** para verificar a assinatura.
   * Se a verificação passar, ele sabe que:
     + A mensagem **veio de Alice** (autenticidade),
     + **Não foi alterada** (integridade),
     + Alice **não pode negar** (não repúdio).

**🧠 Analogia simples**

* **Assinar com a chave privada** é como **selar uma carta com um carimbo exclusivo seu**.
* **Verificar com a chave pública** é como **qualquer pessoa checar que aquele selo é de fato o seu**.