# Certificação Digital

## Segurança da Informação

Charles Tim Batista Garrocho

Instituto Federal de São Paulo – IFSP
Campus Campos do Jordão

garrocho.ifspcjo.edu.br/SEGA6

charles.garrocho@ifsp.edu.br

Curso Superior de TADS

# Certificado Digital

Os computadores e a Internet são largamente utilizados para o processamento de dados e para a troca de mensagens e documentos entre **cidadãos, governo e empresas**.

No entanto, estas transações eletrônicas necessitam da adoção de **mecanismos de segurança** capazes de garantir autenticidade, confidencialidade e integridade às informações eletrônicas.

A **certificação digital** é a tecnologia que provê estes mecanismos. No cerne da certificação digital está o certificado digital, um documento eletrônico que contém o nome, e um número público exclusivo denominado chave pública.

A **chave pública** serve para validar uma **assinatura** realizada em documentos eletrônicos.

INSTITUTO FEDERAL

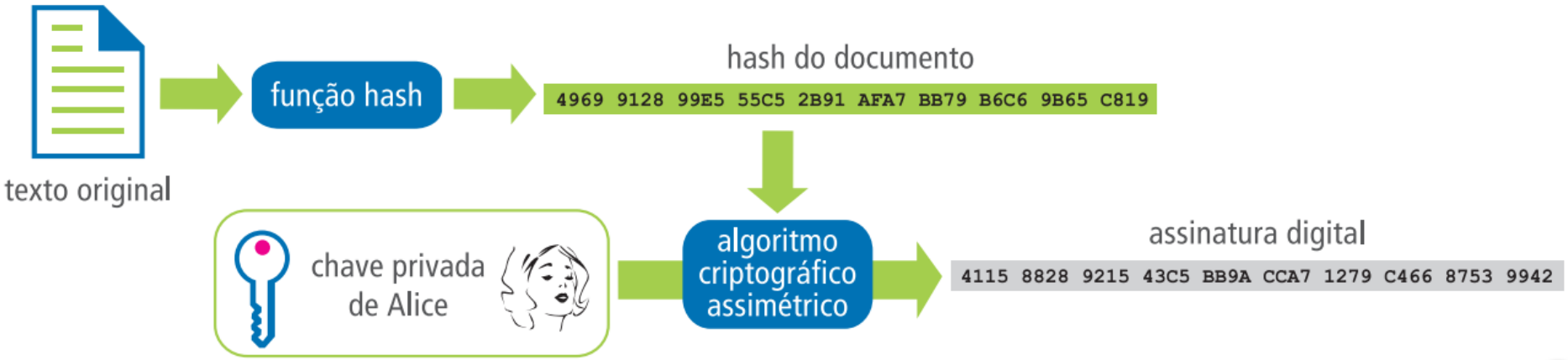
# Certificado Digital

A utilização de certificado digital proporciona:

- **Privacidade**: Garantia de que as informações trocadas nas transações eletrônicas não serão lidas por terceiros.
- **Integridade**: Garantia de que as informações trocadas nas transações eletrônicas não foram alteradas desde que foram assinadas.
- **Autenticidade**: Garantia de identidade da origem e destino da transação.
- **Assinatura Digital**: Assinatura eletrônica baseada em métodos criptográficos que é gerada a partir de um conjunto de regras e que atribui ao documento a possibilidade de confirmar, com segurança, sua integridade e a identificação do autor do documento eletrônico.
- **Não Repúdio**: É a garantia de que somente o titular do Certificado Digital poderia ter realizado determinada transação, impedindo que os integrantes de uma transação venham a contestar ou negar uma transação após sua realização.

# Assinatura Digital

O mesmo método de autenticação dos algoritmos de criptografia de chave pública operando em conjunto com uma função resumo, também conhecido como função de hash, é chamada de **assinatura digital**.




Este pode ser comparado a uma **impressão digital**, pois cada documento possui um valor único de resumo e até mesmo uma pequena alteração no documento, como a inserção de um espaço em branco, resulta em um resumo completamente diferente.

# Assinatura Digital

Para **comprovar** uma assinatura digital é necessário inicialmente realizar algumas operações.

**Calcular** o resumo criptográfico do documento e decifrar a assinatura com a chave pública do signatário.

Se forem iguais, a assinatura está correta, o que significa que foi gerada pela chave privada corresponde à chave pública utilizada na verificação e que o documento está **íntegro**.

Caso sejam diferentes, a assinatura está incorreta, o que significa que pode ter havido **alterações** no documento ou na assinatura pública.

# Assinatura Digital