INSTITUTO FEDERAL DE EDUCAÇÃO CIÊNCIA E TECNOLOGIA
PARAÍBA

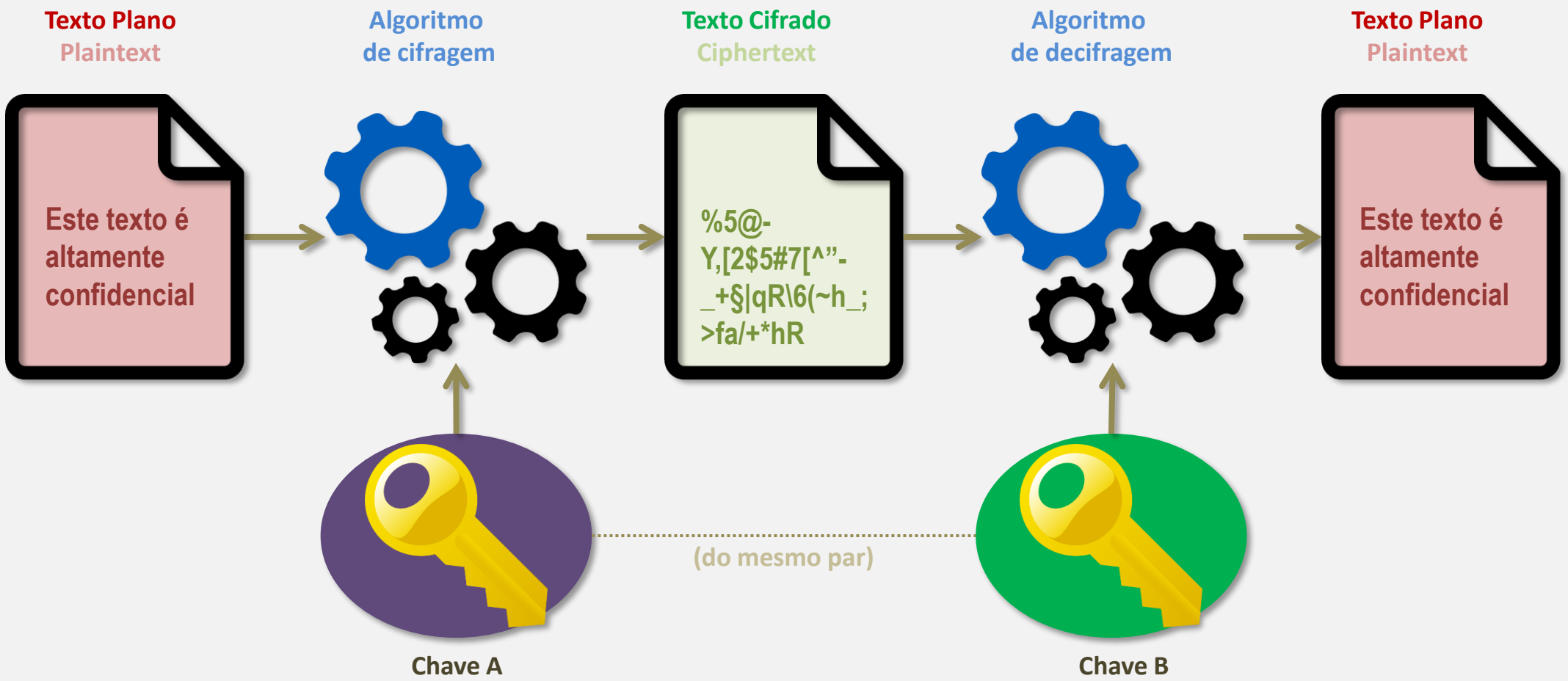
# Assinatura Digital

Dênio Mariz

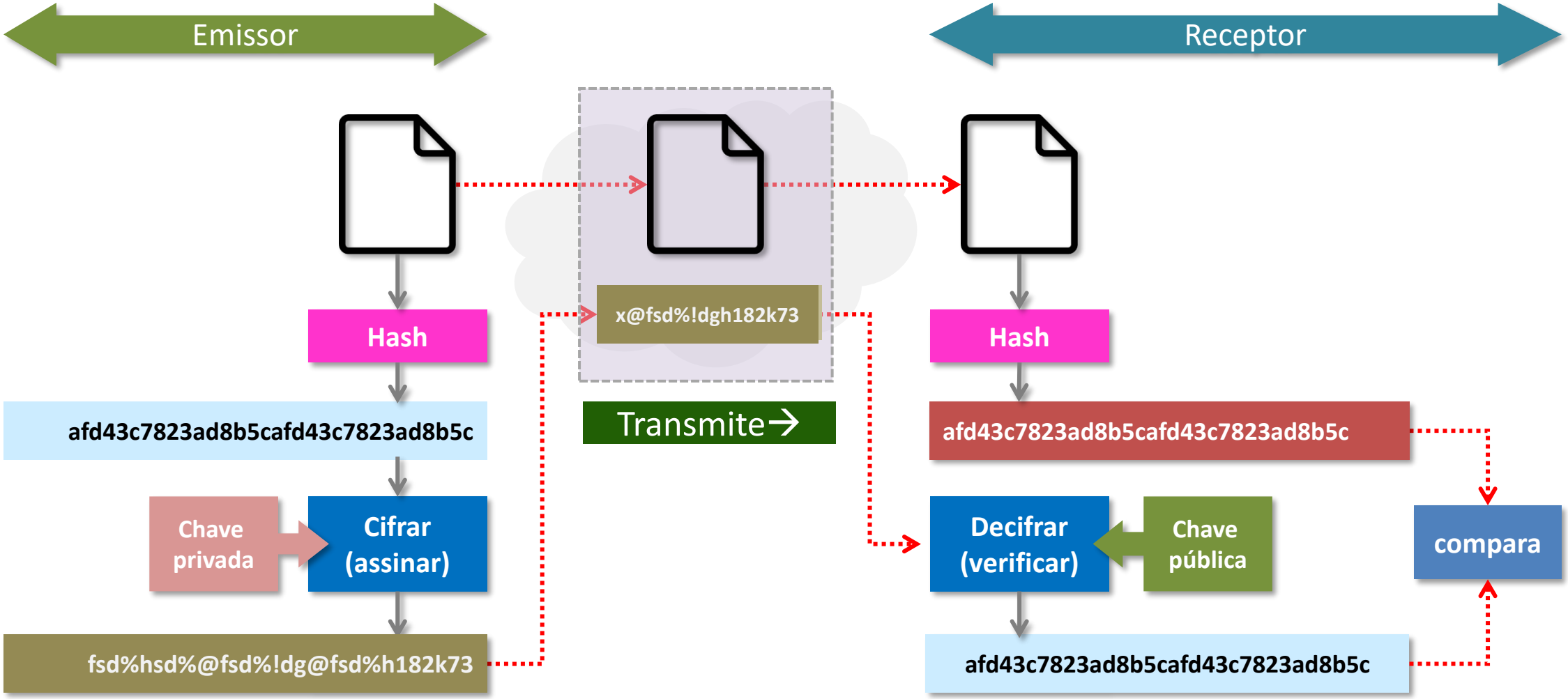
Setembro 2020

Prof. Dênio Mariz, IFPB

# Criptografia Assimétrica



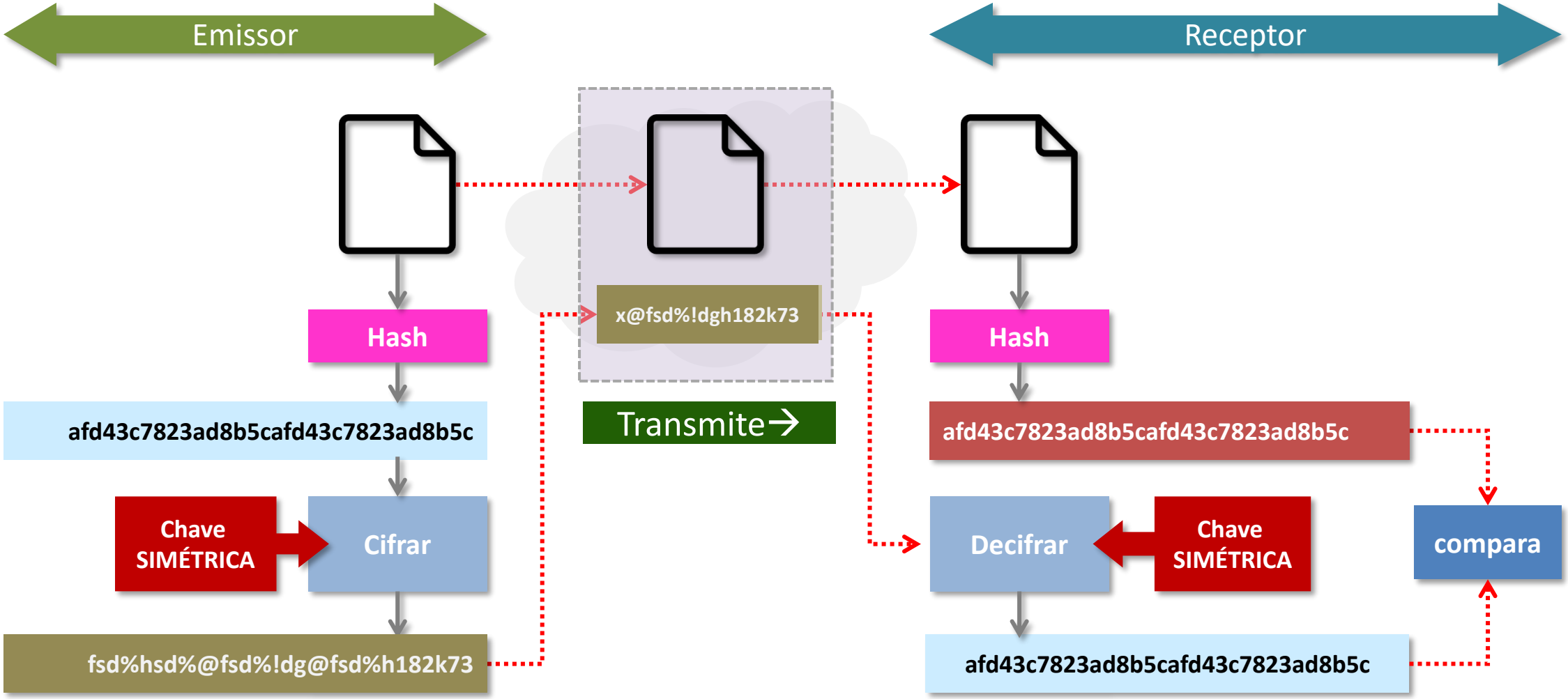
# Assinatura Digital



# HMAC – Hash-based Message Authentication Code

- Requer:
  - Chave simétrica
  - Algoritmo para assinatura
  - Algoritmo de hash
- Permite
  - Verificar integridade
  - Confirma que o autor é alguém que conhece uma chave compartilhada
- Não é uma assinatura!
  - Assinatura digital requer chaves assimétricas

# HMAC



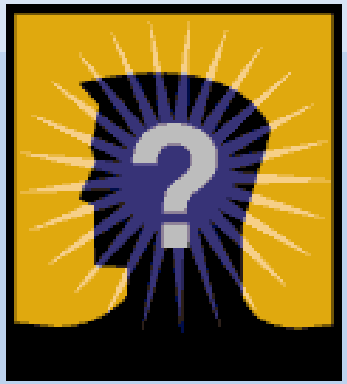



Prof. Dênio Mariz, IFPB

# HMAC Vs Assinatura

- Assinatura
  - Permite verificação de integridade
  - Requer: Par de chaves assimétricas
  - Algoritmo Assimétrico (ex: RSA)
  - Garante autenticidade da autoria
- HMAC
  - Permite verificação de integridade
  - Requer: uma chave compartilhada (simétrica)
  - Algoritmo Simétrico (ex: Rinjdael)
  - **NÃO** Garante autenticidade da autoria (garante apenas que o outro lado conhece a chave)

INSTITUTO FEDERAL DE EDUCAÇÃO CIÊNCIA E TECNOLOGIA
PARAÍBA



# Assinatura Digital

Dênio Mariz
denio@ifpb.edu.br

SafeNet Authentication Client 10.7 Setup

**Welcome to the SafeNet Authentication Client 10.7 Installation Wizard**

SafeNet Authentication Client 10.7 Setup

**Interface Language**

Select the interface language.

gemalto
security to be free

Select the Saf

Portuguese

InstallShield

SafeNet Authentication Client 10.7 Setup

**License Agreement**

Please read the following license agreement carefully.

gemalto
security to be free

SAFENET SO

SafeNet Aut

Legal notice

SafeNet soft
licensed all
UNLESS YOU
CONTROLS A

I accept th

I do not ac

InstallShield

SafeNet Authentication Client 10.7 Setup

**Destination Fol**

Click Next to
to a different

Insta
C:\F

InstallShield

SafeNet Authentication Client 10.7 Setup

The wizard is ready to begin installati

Click Install to begin the installation.

If you want to review or change any of
Click Cancel to exit the wizard.

InstallShield

SafeNet Authentication Client 10.7 Setup


**SafeNet Authentication Client 10.7 has been successfully installed.**

Click Finish to exit Setup.