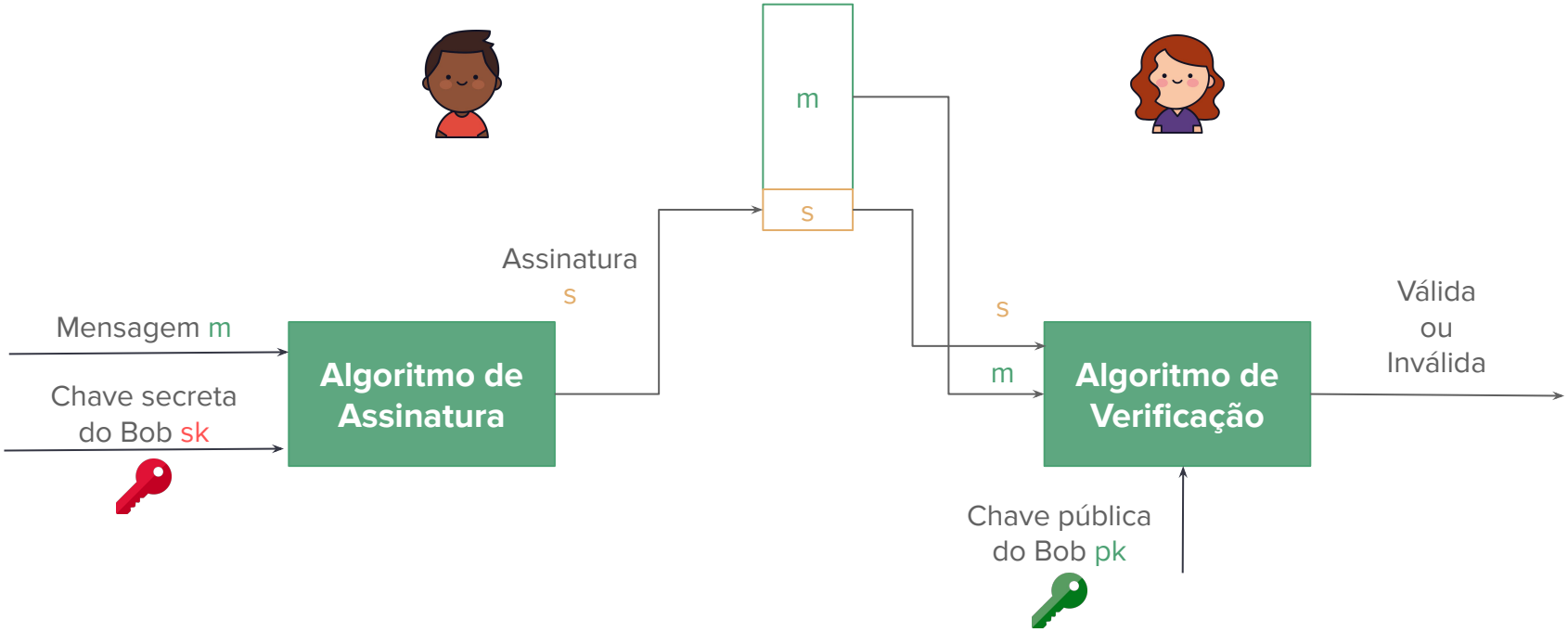
Criptografia Aplicada

Atividade prática com assinatura digital

Assinatura Digital



Algoritmos necessários

- Geração de chaves: (pk,sk) = KeyGen
- Assinatura: s = Sign(m, sk)
- Verificação: Verify(m, s, pk)
  - “válida” se s = Sign(m, sk)
  - “inválida” caso contrário

Assinatura digital e hash

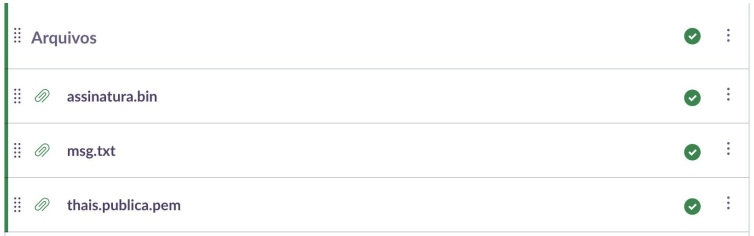
- Normalmente, esquemas de assinatura são usados juntamente com uma função de hash criptográfica
- O hash da mensagem é assinado, ao invés da mensagem

Atividade

- Vamos trabalhar com assinaturas digitais no python!
- Vamos utilizar a biblioteca PyCryptodome
- Para instalar no linux, basta rodar o comando:
  - pip install pycryptodome
  - pip install pycryptodomex (alternativa se não funcionar a anterior)
- Importação da biblioteca:
  - `from Cryptodome.Cipher import AES`
  - `from Crypto.Cipher import AES`

Atividade 1

- Crie uma função python para verificar a assinatura digital RSA disponibilizada no Canvas na semana passada



- Essa função será equivalente a rodar:

```
openssl dgst -sha256 -verify thais.publica.pem -signature assinatura.bin msg.txt
```

- Ver `RSAsig.py` para um esqueleto do código

Atividade 1 - Dicas

- Crie uma função genérica de verificação, que receba a mensagem, assinatura e chave em bytes e retorna True ou False;
  - a leitura em arquivo com f.read() retorna o conteúdo em bytes
- Se desejarem printar o conteúdo dos arquivos na tela, decodificar os bytes
  - ex: `print(mensagem.decode())`
- Para printar assinaturas, primeiro é necessário codificar em base64 e depois decodificar os bytes:
  - ex: `print(b64encode(signature).decode())`

Atividade 2

- Complemente o código com funções de **geração de chaves** e **assinatura**
- A geração de chaves deve receber o tamanho da chave
- Crie uma função de assinatura que receba a mensagem e a chave em bytes e retorne a assinatura em RSA
- Alguma função demorou mais tempo para executar?
- Tente fazer um código mais genérico, que funcione também para ECDSA

Referências

Documentação PyCryptodome:

- Assinaturas Digitais
- Funções de Hash
- Chaves RSA