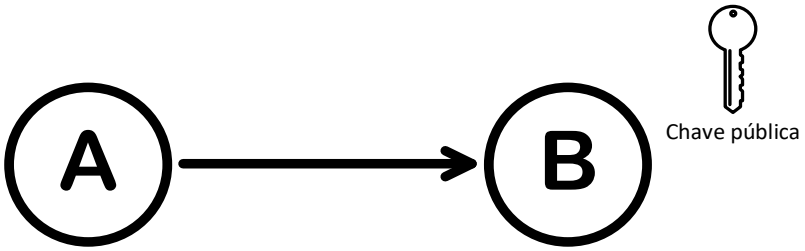
Assinatura digital

FURB
UNIVERSIDADE DE BLUMENAU

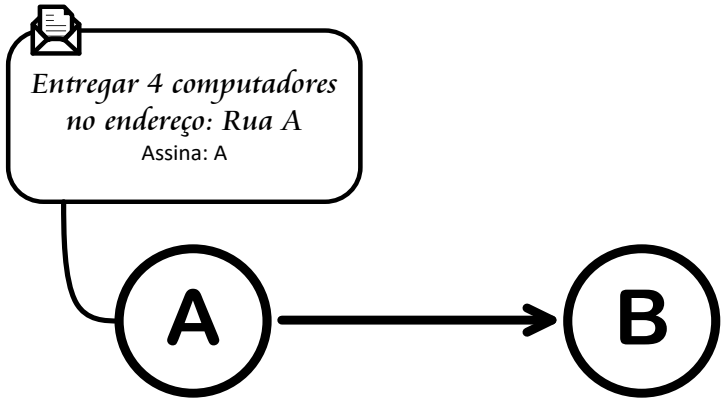
Definição

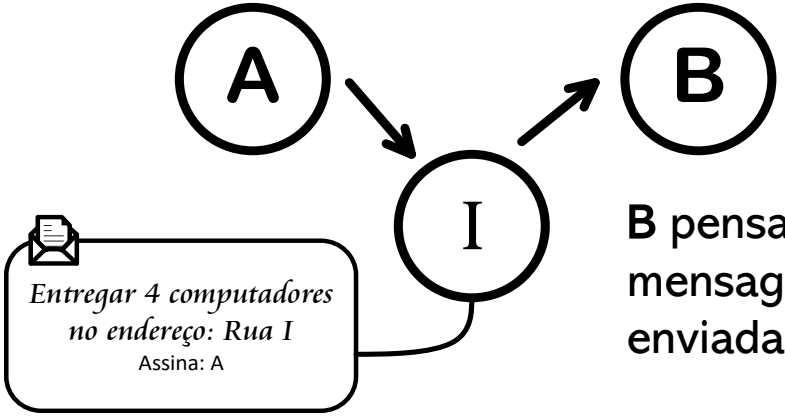
- A criptografia de chave pública ajuda a resolver o problema de distribuição de chaves.
- Na criptografia de chave assimétrica, o emissor utiliza a chave pública do destinatário para cifrar os dados



- E se o emissor utilizasse sua chave privada para cifrar os dados?
  - Qual seria o benefício?

Definição





B pensa que a mensagem foi enviada de **A**

Assinatura digital

- Se o emissor cifrar a mensagem com sua chave privada, somente a sua chave pública poderá decifrá-la
- O destinatário, ao receber a mensagem, utiliza a chave pública do remetente para decifrar a mensagem:
  - Se o conteúdo for legível, é seguro afirmar que a mensagem foi cifrada com a chave privada de quem afirma ser remetente
    - Assume-se que a chave privada é única e que ela manteve-se privada
  - Se o conteúdo não for legível, pode-se afirmar que a mensagem não foi cifrada com a chave privada de quem afirma ser remetente
- A criptografia de chave assimétrica também pode ser utilizada para autenticação e não-repúdio.

Assinatura digital

- A utilização da chave privada para criptografar dados é conhecida como **técnica de assinatura digital**
- Como é possível afirmar que a mensagem foi realmente originada de determinado emissor, o texto cifrado é chamado de **assinatura digital**

Assinatura digital

- A criptografia de chave assimétrica é lenta e cifrar completamente o texto simples não é eficiente.
- Ao invés de cifrar todo o texto simples com a chave privada, o melhor método é cifrar um *resumo de mensagem*
  - Portanto, **assinar uma mensagem** consiste em gerar um resumo da mensagem e cifrá-lo com a chave privada. O resultado é **assinatura digital**

Assinatura digital

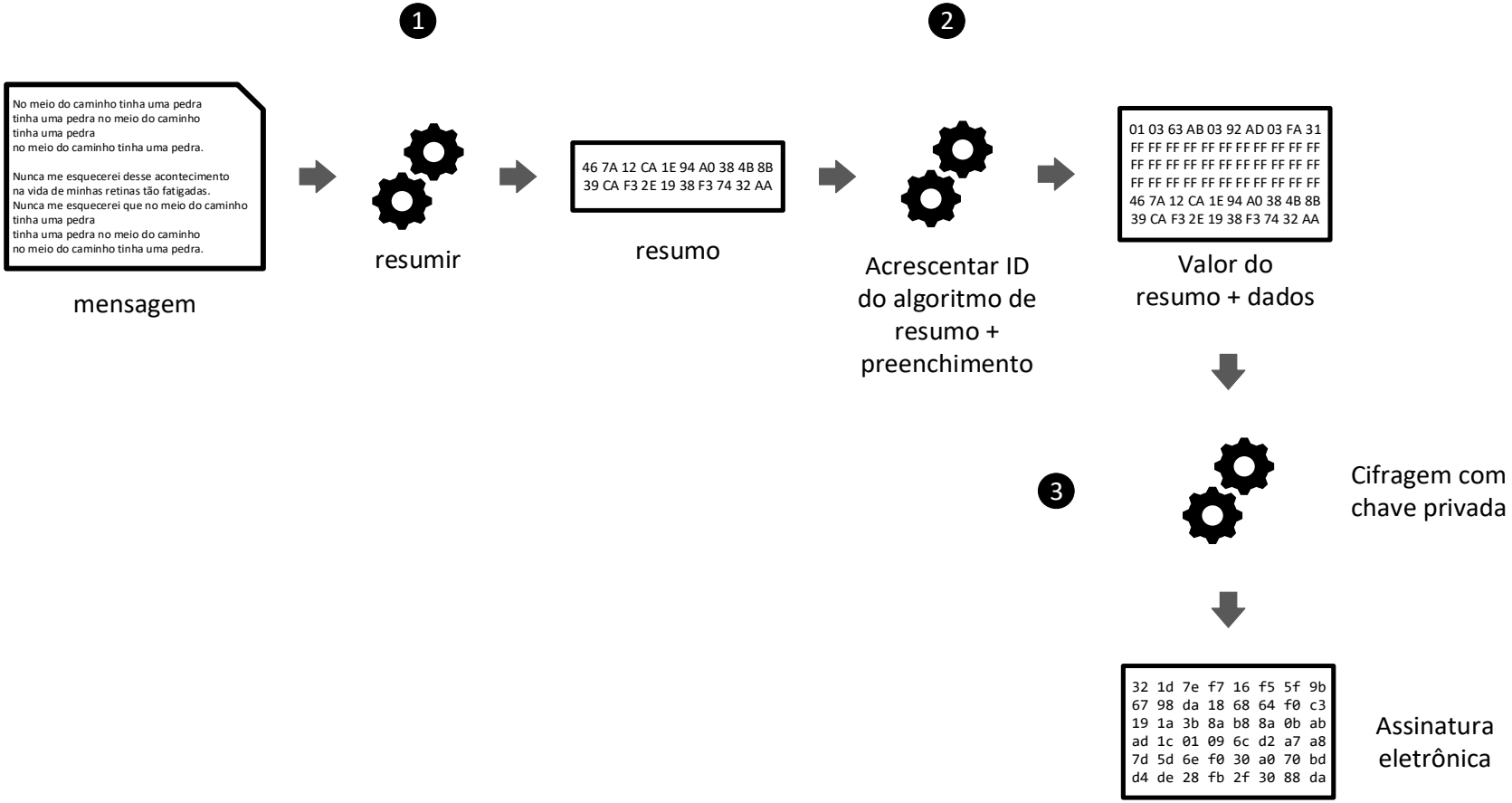
- A aplicação desta técnica não garante confidencialidade dos dados, porém:
  - Permite garantir o remente (autenticação)
  - Garante o não-repúdio
  - Permite garantir integridade dos dados

- A assinatura digital depende de duas suposições fundamentais:
  - A chave privada esteja segura
    - somente o proprietário tem acesso à ela
  - A chave é única
    - ninguém conseguiu provar que esta suposição é verdadeira

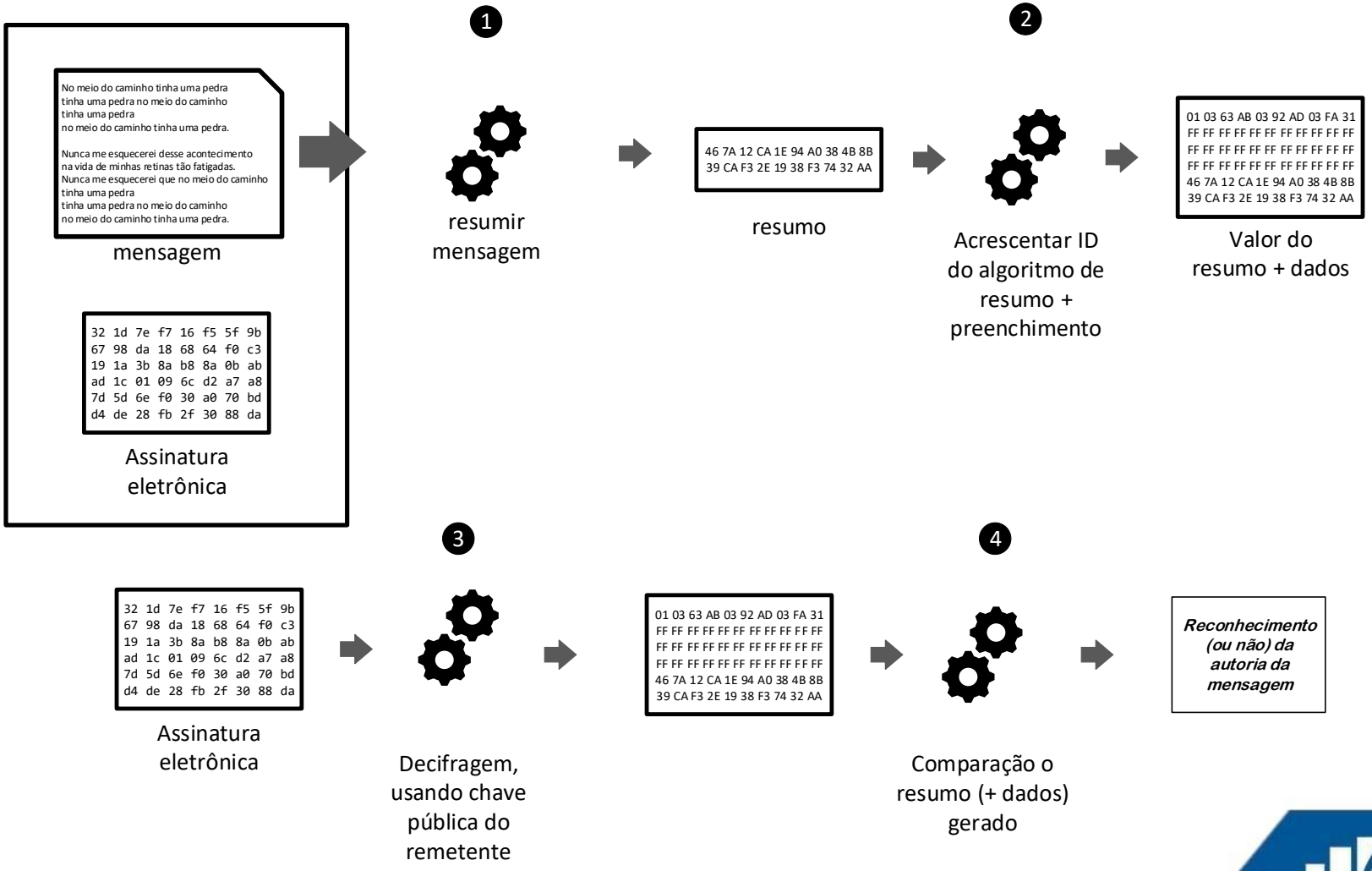
Assinatura digital

- Cada mensagem enviada possui sua própria assinatura digital
  - Não há uma única assinatura associada a uma pessoa ou a um par de chaves
  - Torna a falsificação de uma assinatura muito mais difícil
- Na prática, além do resumo da mensagem, também é acrescentado ao texto simples (isto é, ao resumo) um identificador do algoritmo de resumo utilizado.
- Além disso, bytes de preenchimento são utilizados para compor uma mensagem com tamanho igual ao da chave
- Isto é, o que é cifrado é um conjunto de dados constituído de: resumo + identificador do algoritmo + preenchimento

Geração de assinatura eletrônica



Validação de assinatura eletrônica



Assinatura digital

OID	Name	Description
1.3.14.3.2.2	md4WitRSA	Security Rivest, Shamir and Adleman (RSA) algorithm applied to a hash created by using the Message Digest 4 (MD4) algorithm
1.3.14.3.2.3	md5WithRSA	Security Rivest, Shamir and Adleman (RSA) algorithm applied to a hash created by using the Message Digest 5 (MD5) algorithm
1.3.14.3.2.4	md4WithRSAEncryption	Security "RSA2" algorithm applied to a hash created by using the Message Digest 4 (MD4) algorithm
1.3.14.3.2.6	desECB	Security Data Encryption Standard (DES) algorithm coupled with a electronic codebook mode of operation
1.3.14.3.2.8	desOFB	Data Encryption Standard (DES) algorithm coupled with a cipher-block chaining mode of operation
1.3.14.3.2.9	desCFB	Data Encryption Standard (DES) algorithm coupled with a output feedback mode of operation
1.3.14.3.2.10	desMAC	56-bit Data Encryption Standard (DES) algorithm coupled with a 64-bit Message Authentication Code (MAC) that hashes both the ...
1.3.14.3.2.11	11	Rivest, Shamir and Adleman (RSA) signature algorithm
1.3.14.3.2.12	dsa	Digital Signature Algorithm (DSA)
1.3.14.3.2.13	dsaWithSHA	Security Digital Signature Algorithm (DSA) that uses the Secure Hash Algorithm (SHA) to hash the message contents
1.3.14.3.2.14	mdc2WithRSASignature	Rivest, Shamir and Adleman (RSA) algorithm that uses the Modification Detection Code 2 (MDC2) or Meyer-Schilling hash function
1.3.14.3.2.15	shaWithRSASignature	Rivest, Shamir and Adleman (RSA) algorithm coupled with the Secure Hash Algorithm (SHA) (Oddball using ISO/IEC 9796-2 padding...
1.3.14.3.2.16	dhWithCommonModulus	Diffie-Hellman (DH) key exchange algorithm with common modulus algorithm
1.3.14.3.2.17	desEDE	Voice encryption using Data Encryption Standard (DES) (168-bit) algorithm coupled with the Encrypt-Decrypt-Encrypt (EDE) mult...
1.3.14.3.2.18	sha	Secure Hash Algorithm (SHA)
1.3.14.3.2.19	mdc-2	Modification Detection Code 2 (MDC2) or Meyer-Schilling hash function
1.3.14.3.2.20	dsaCommon	Digital Signature Algorithm (DSA)
1.3.14.3.2.21	dsaCommonWithSHA	Digital Signature Algorithm (DSA) coupled with the Secure Hash Algorithm (SHA)
1.3.14.3.2.22	rsa-key-transport	Rivest, Shamir and Adleman (RSA) key transport attribute
1.3.14.3.2.23	keyed-hash-seal	Keyed hash seal algorithm
1.3.14.3.2.24	md2WithRSASignature	Rivest, Shamir and Adleman (RSA) algorithm coupled with the Message Digest 2 (MD2) hashing algorithm (oddball using ISO/IEC 9...
1.3.14.3.2.25	md5WithRSASignature	Rivest, Shamir and Adleman (RSA) algorithm coupled with the Message Digest 5 (MD5) hashing algorithm (Oddball using ISO/IEC 9...
1.3.14.3.2.26	hashAlgorithmIdentifier	Secure Hash Algorithm, revision 1 (SHA-1)
1.3.14.3.2.27	dsaWithSHA1	Digital Signature Algorithm (DSA) that uses the Secure Hash Algorithm 1 (SHA1) producing a 320-bit signature
1.3.14.3.2.28	dsaWithCommonSHA1	Digital Signature Algorithm (DSA) that uses the Secure Hash Algorithm 1 (SHA1) with Common Parameters producing a 320-bit sig...
1.3.14.3.2.29	sha-1WithRSAEncryption	Rivest, Shamir and Adleman (RSA) algorithm that uses the Secure Hash Algorithm 1 (SHA1) (obsolete)

Identificador de algoritmo

Assinatura com o algoritmo RSA

- Além do algoritmo RSA, existem outros algoritmos para assinar mensagens:
  - DSA (*Digital Signature Algorithm*)
  - ECDSA (*Elliptic Curve Digital Signature Algorithm*)

- O algoritmo RSA é “quase onipresente e tornou-se o padrão de fato”.

Geração de assinatura digital em Java

Signature
+ getInstance(algorithm : String) : Signature + initVerify(publicKey : PublicKey) : void + initVerify(certificate : Certificate) : void + initSign(privateKey : PrivateKey) : void + initSign(privateKey : PrivateKey, random : SecureRandom) : void + sign() : byte[] + sign(outbuf : byte[], offset : int, len : int) : int + verify(signature : byte[]) : boolean + verify(signature : byte[], offset : int, length : int) : boolean + update(b : byte) : void + update(data : byte[]) : void + update(data : byte[], off : int, len : int) : void

Algoritmos suportados:

- MD2withRSA
- MD5withRSA
- SHA1withRSA
- SHA224withRSA
- SHA256withRSA
- SHA384withRSA
- SHA512withRSA

```
PrivateKey privateKey = carregarChavePrivada(new File("etc/private.key"));
byte[] textoSimples = lerArquivoParaAssinar(new File("etc/textoSimples.txt"));

Signature signature = Signature.getInstance("SHA1WithRSA");
signature.initSign(privateKey);
signature.update(textoSimples);

byte[] assinatura = signature.sign();
```

Validação de assinatura digital

```
Signature signature = Signature.getInstance("SHA1withRSA");
signature.initVerify(chavePublica);
signature.update(mensagemRecebida);
if (signature.verify(assinaturaRecebida)) {
    System.out.println("OK");
} else {
    System.out.println("Não ok");
}
```