Digital signatures

Asymmetric (Block) Ciphers

Use key pairs

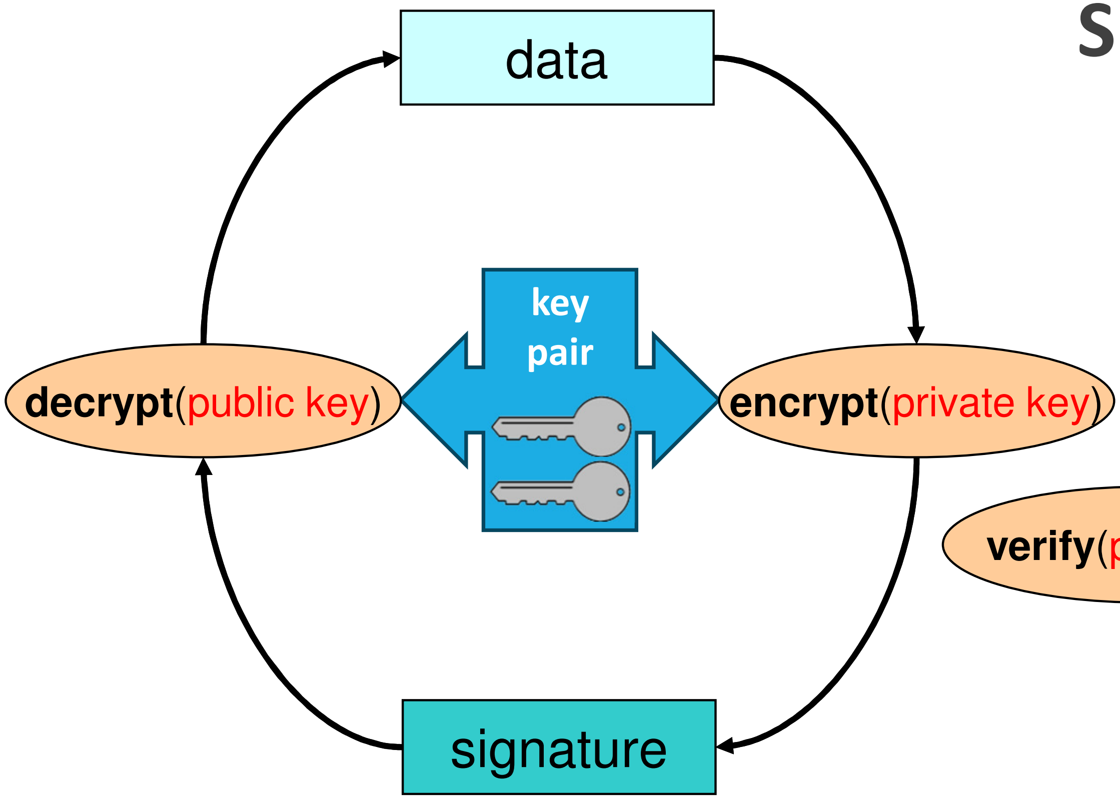
- One private key (personal, not transmittable)
- One public key, available to all

Allow

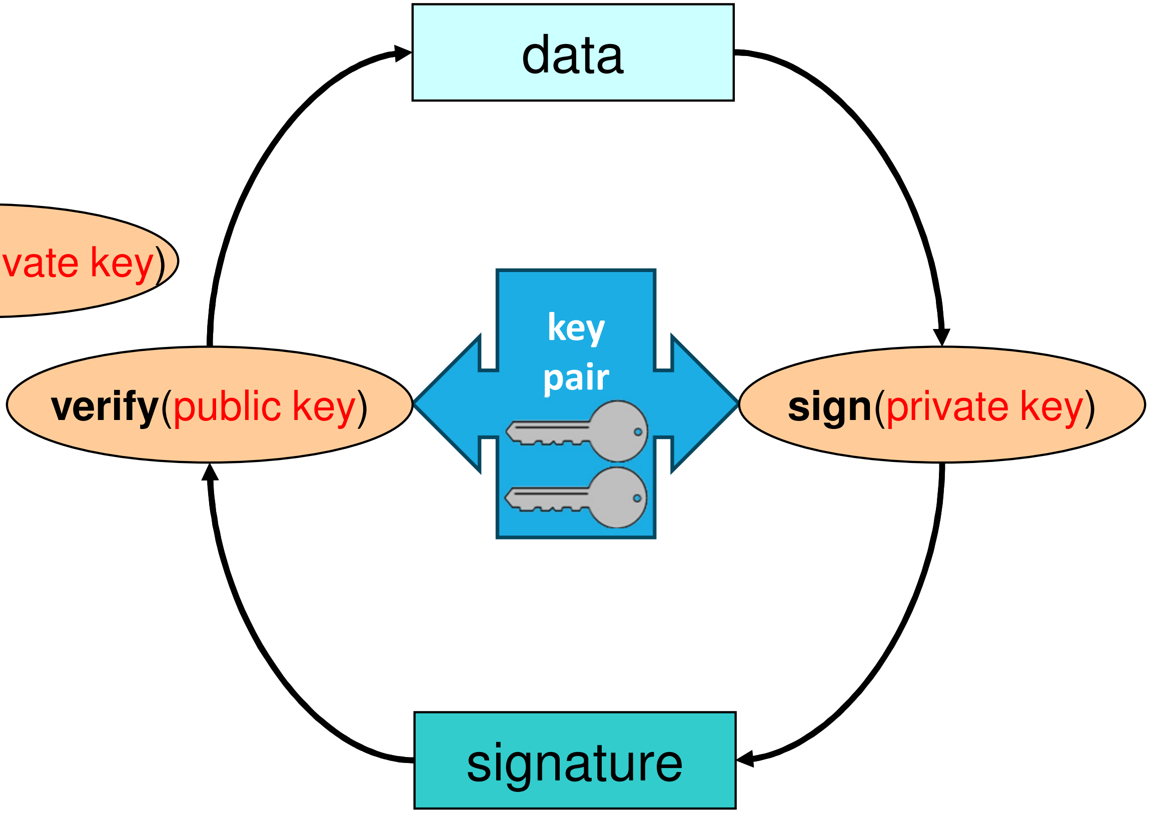
- Confidentiality without any previous exchange of secrets
- Authentication
  - Of contents (data integrity)
  - Of origin (source authentication, or digital signature)

Digital signatures

Encrypt / decrypt (RSA)



Sign / verify (ElGamal, EC)



Digital signatures

Authenticate the contents of a document

- Ensure its integrity (it was not changed)

Authenticate its author

- Ensure the identity of the creator/originator

Prevent repudiation of signatures

- Non-repudiation
- Genuine authors cannot deny authorship
  - Only the identified author could have generated a given signature

Digital Signatures

Approaches

- Asymmetric encryption/decryption or signature/verification
- Digest functions (only for performance)

Signing: $A_x(\text{doc}) = \text{info} + E(K_x^{-1}, \text{digest}(\text{doc} + \text{info}))$

$A_x(\text{doc}) = \text{info} + S(K_x^{-1}, \text{digest}(\text{doc} + \text{info}))$

$\text{info} = \text{signing context, signer identity, } K_x$

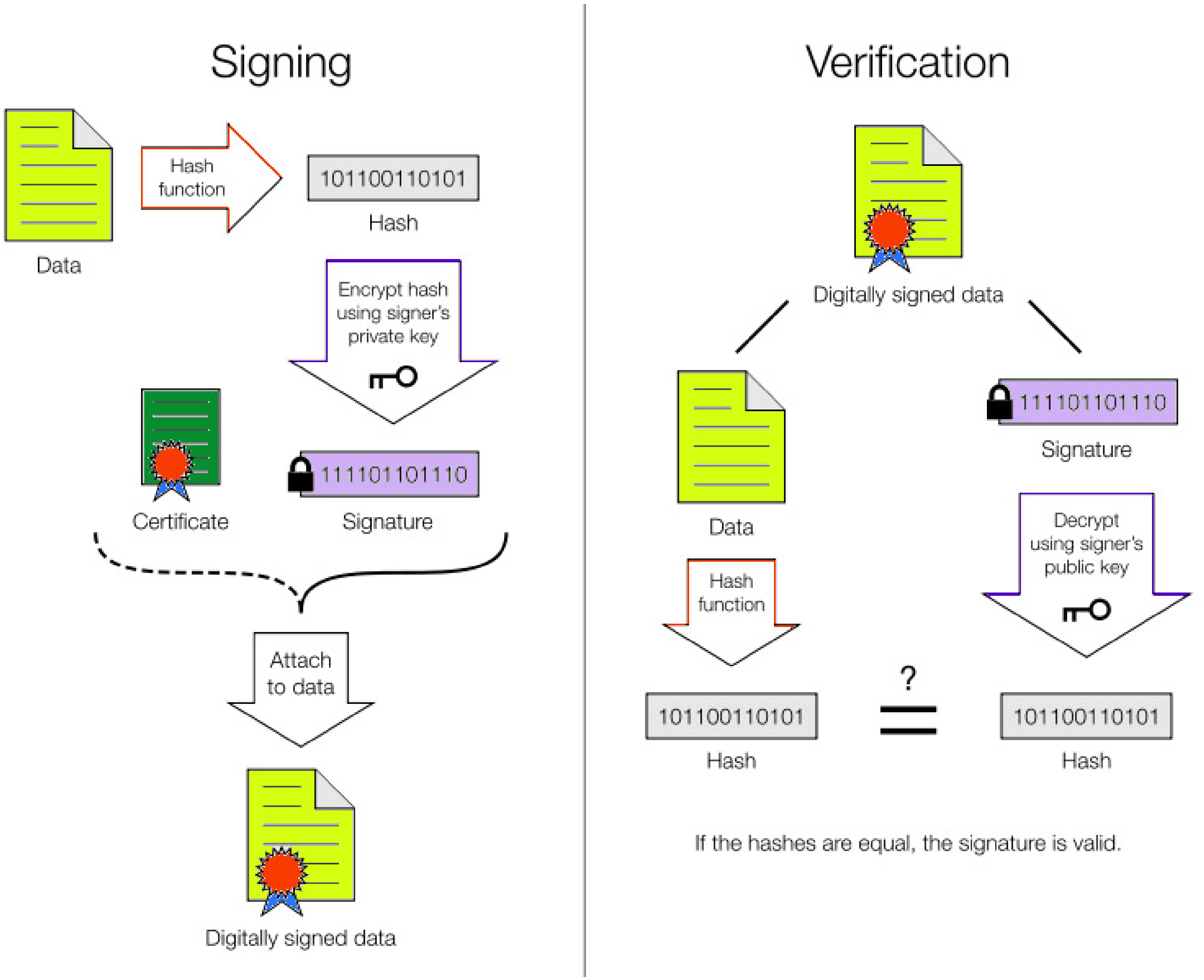
Verification:

$D(K_x, A_x(\text{doc})) \equiv \text{digest}(\text{doc} + \text{info})$

$V(K_x, A_x(\text{doc}), \text{doc}, \text{info}) \rightarrow \text{True / False}$

wikipedia, http://en.wikipedia.org/wiki/Digital_signature

Encryption / decryption signatures



Digital signature on a mail:
Multipart content, signature w/ certificate

```
From - Fri Oct 02 15:37:14 2009
[…]
Date: Fri, 02 Oct 2009 15:35:55 +0100
From: =?ISO-8859-1?Q?Andr=E9_Z=FAquete?= <andre.zuquete@ua.pt>
Reply-To: andre.zuquete@ua.pt
Organization: IEETA / UA
MIME-Version: 1.0
To: =?ISO-8859-1?Q?Andr=E9_Z=FAquete?= <andre.zuquete@ua.pt>
Subject: Teste
Content-Type: multipart/signed; protocol="application/x-pkcs7-signature"; micalg=sha1; boundary="------------ms050405070101010502050101"

This is a cryptographically signed message in MIME format.

--------------ms050405070101010502050101
Content-Type: multipart/mixed;
 boundary="------------060802050708070409030504"

This is a multi-part message in MIME format.
--------------060802050708070409030504
Content-Type: text/plain; charset=ISO-8859-1
Content-Transfer-Encoding: quoted-printable

Corpo do mail

--------------060802050708070409030504–
--------------ms050405070101010502050101
Content-Type: application/x-pkcs7-signature; name="smime.p7s"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="smime.p7s"
Content-Description: S/MIME Cryptographic Signature

MIAGCSqGSIb3DQEHAqCAMIACAQExCzAJBgUrDgMCGgUAMIAGCSqGSIb3DQEHAQAAoIIamTCC
BUkwggSyoAMCAQICBAcnIaEwDQYJKoZIhvcNAQEFBQAwdTELMAkGA1UEBhMCVVMxGDAWBgNV
[…]
KoZIhvcNAQEBBQAEgYCofks852BV77NVuww53vSxO1XtI2JhC1CDlu+tcTPoMD1wq5dc5v40
Tgsaw0N8dqgVLk8aC/CdGMbRBu+J1LKrcVZa+khnjjtB66HhDRLrjmEGDNttrEjbqvpd2QO2
vxB3iPTlU+vCGXo47e6GyRydqTpbq0r49Zqmx+IJ6Z7iigAAAAAAAA==
--------------ms050405070101010502050101--
```