Introduction to Cryptography and Security Mechanisms:

Unit 10

Digital Signatures

Learning Outcomes

- Explain general requirements for a digital signature scheme
- Recognise that not all digital signatures rely on public key cryptography
- Appreciate the role that hash functions play in creating some types of digital signature scheme
- Explain two different methods of creating a digital signature scheme based on RSA
- Compare various properties of digital and hand-written signatures
- Identify some points of vulnerability in any practical digital signature scheme

Sections

1. Digital signatures
2. Digital signature schemes based on RSA
3. Digital signature schemes in practice

1. Digital signatures

Informal definition

Informally, a **digital signature** is a technique for establishing the origin of a particular message in order to settle later disputes about what message (if any) was sent.

The purpose of a digital signature is thus for an entity to bind its identity to a message.

Digital signatures

- The **signer** is an entity who creates a digital signature.
- The **verifier** is an entity who receives a signed message and attempts to check whether the digital signature is **valid** or not.

Electronic signatures

The European Community Directive on electronic signatures refers to the concept of an **electronic signature** as:

> data in electronic form attached to, or logically connected with, other electronic data and which serves as a method of authentication

What different things can you think of that might satisfy this rather vague notion of an electronic signature?

Advanced electronic signatures

The European Community Directive on electronic signatures also refers to the concept of an **advanced electronic signature** as:

an electronic signature that is:

1. uniquely linked to the signatory
2. capable of identifying the signatory
3. created using means under the sole control of the signatory
4. linked to data to which it relates in such a way that subsequent changes in the data is detectable

Security requirements

We will define a **digital signature scheme** to be a cryptographic primitive that provides:

1. Data origin authentication of the signer
2. Non-repudiation

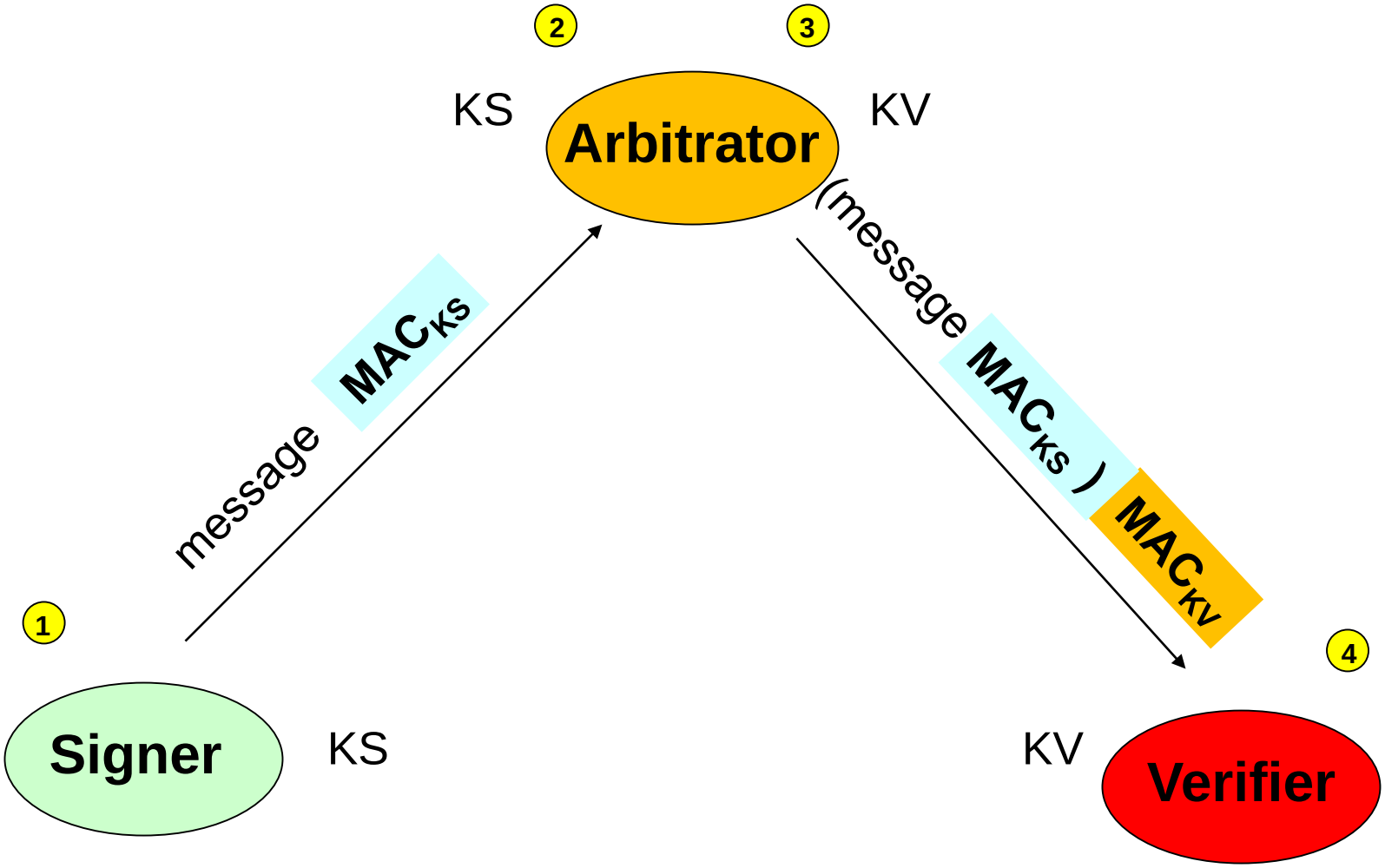
It thus needs to reply on:

- The data
- A secret parameter known only by the signer

Properties of a digital signature

- Easy for the signer to sign data
- Easy for anyone to verify a digital signature
- Hard for anyone to forge a digital signature

Arbitrated digital signatures



Arbitrated digital signatures

1. How does the verifier check the first MAC, computed using KS?
2. What is the main (practical) problem with implementing arbitrated signatures?

Complementary requirements

A **“**true**”** digital signature is one that can be sent directly from the signer to the verifier.

For the rest of this unit when we say **digital signature scheme** we mean “true” digital signature .

Digital signature requirements	Public-key encryption requirements
Only the holder of some secret data can sign a message	“Anyone” can encrypt a message
“Anyone” can verify that a signature is valid	Only the holder of some secret data can decrypt a message

A naive approach

1. Given the apparent symmetry of the requirements for public key encryption and digital signatures, propose a naïve approach to designing a digital signature scheme.
2. State two reasons why the above approach is naïve.

2. Digital signature schemes based on RSA

Three caveats

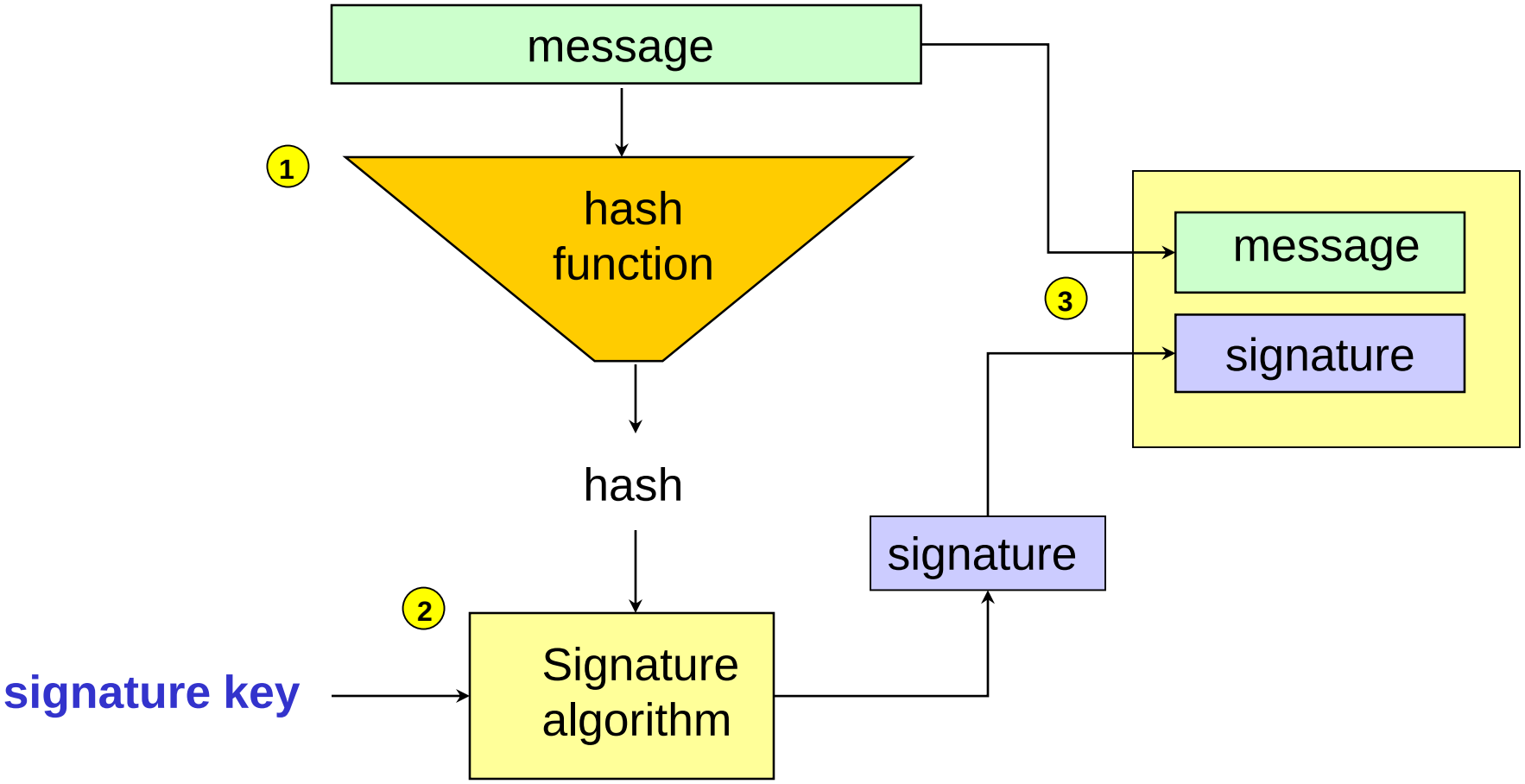
We will focus this section on describing digital signatures based on RSA. Please note:

1. There are important digital signature schemes that are not based on RSA
2. The RSA public key cryptosystem has some **special properties** that allow it to be used as a basis for both encryption and digital signature schemes
3. The processes described here are simplified – please consult relevant standards before implementing!

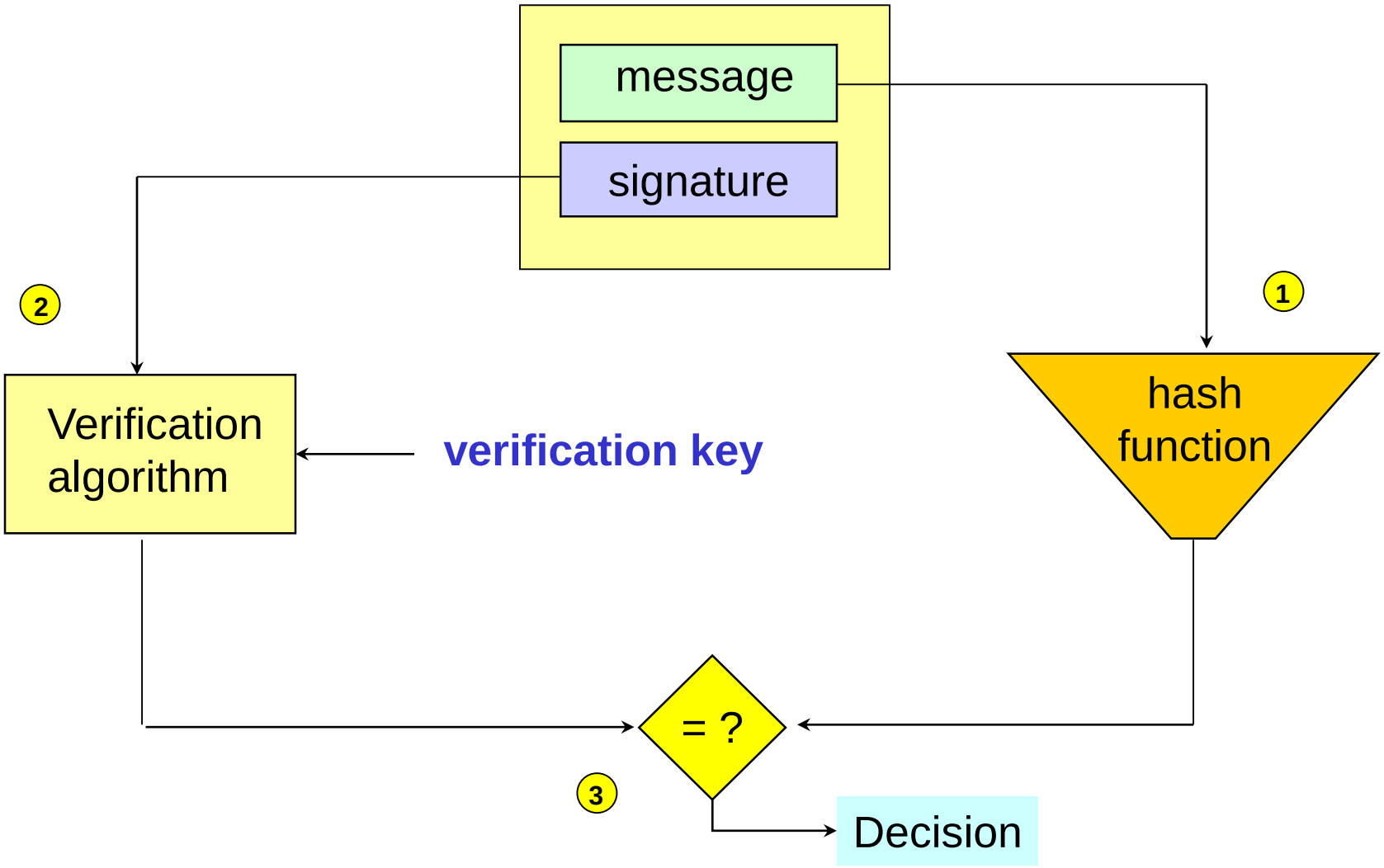
Terminology

Public-key encryption	Digital signature scheme
Public key	Verification key
Private key	Signature key

Creating an RSA signature with appendix



Verifying an RSA signature with appendix



Hashing before signing

There are at least two reasons why a message is hashed before it is signed using RSA.

What are they?

Beware of misconceptions

You cannot obtain a digital signature scheme by swapping the roles of the private and public keys of any public-key cryptosystem

You cannot obtain a public-key cryptosystem by swapping the roles of the signature and verification keys of any digital signature scheme

Key separation

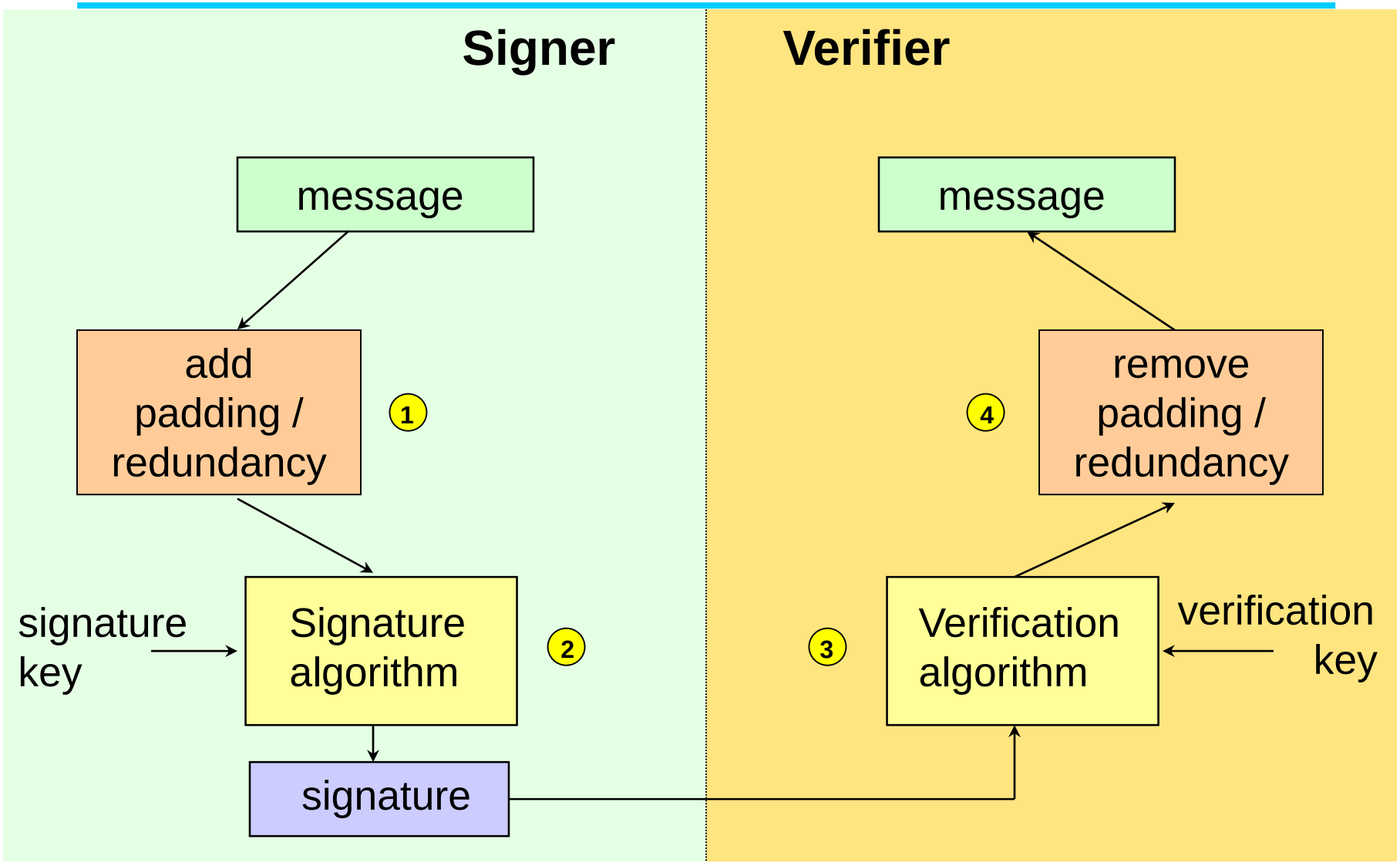
In real applications you should avoid using the same RSA key pair for both encryption and for digital signatures.

The reason is that good key management follows a principle known as **key separation**.

Properly implemented versions of RSA that are to be used for both encryption and digital signatures should issue each user with **two** key pairs:

- a public / private key pair for encryption
- a verification / signature key pair for digital signatures

RSA signatures with message recovery



Digital Signature Algorithm

The **Digital Signature Algorithm** (**DSA**) is based on ElGamal.

Standardised by the U.S. Government as the **Digital Signature Standard** FIPS 186-3.

The DSA is a digital signature with appendix.

It is a dedicated digital signature scheme – it cannot be used as a public key encryption scheme.

The elliptic-curve-based variant is known as ECDSA.

3. Digital signature schemes in practice

All too true (thanks to XKCD)

Hand-written v digital signatures

Compare hand-written and digital signatures with respect to:

1. **Security differences** (such as consistency over messages, consistency over time, uniqueness to individuals, precision of verification, ease of forgery, binding to individuals)
2. **Practical differences** (such as cost, longevity, acceptability, legal recognition)
3. **Flexibility** (such as binding to underlying data, support for multiple signatures, availability issues)

Generic attacks

- **Obtain someone else's private signature key**
  - In a digital signature scheme "you are your private key"
- **Persuade others that someone else's public verification key belongs to you**
  - You do not need to obtain that other person's signature key
- **Find a collision in the hash function**
  - Hopefully impossible!

Sign then encrypt

- Digitally sign the message
- Public-key encrypt the message and the digital signature

What are the disadvantages of this approach?

Encrypt then sign

- Public-key encrypt the message
- Digitally sign the ciphertext

What are the disadvantages of this approach?

Summary

- Digital signatures are in some senses complementary to public key encryption, offering data origin authentication and non-repudiation of digital messages.
- There are two general techniques for designing a digital signature scheme (with appendix and message recovery)
- Digital signatures have different properties and offer different guarantees to hand-written signatures.