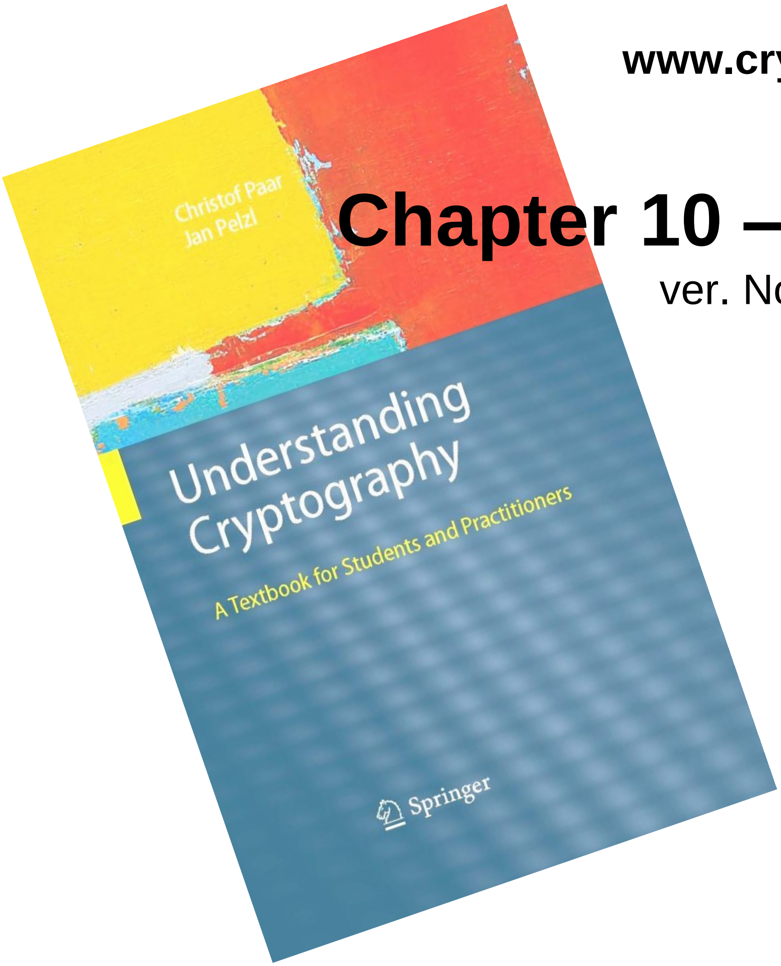
Understanding Cryptography – A Textbook for Students and Practitioners

by Christof Paar and Jan Pelzl



www.crypto-textbook.com

Chapter 10 – Digital Signatures

ver. November 13, 2024

These slides were originally prepared by Georg Becker, Christof Paar and Jan Pelzl. Later, they were modified by Tomas Fabsic for purposes of teaching I-ZKRY at FEI STU.

Homework

- Read Sections 10.1.-10.2.

Some legal stuff (sorry): Terms of Use

- The slides can used free of charge. All copyrights for the slides remain with Christof Paar and Jan Pelzl.
- The title of the accompanying book “Understanding Cryptography” by Springer and the author’s names must remain on each slide.
- If the slides are modified, appropriate credits to the book authors and the book title must remain within the slides.
- It is not permitted to reproduce parts or all of the slides in printed form whatsoever without written consent by the authors.

Content of this Chapter

- Security services
- The principle of digital signatures
- The RSA digital signature scheme
- DSA and ECDSA

Content of this Chapter

- **Security services**
- The principle of digital signatures
- The RSA digital signature scheme
- DSA and ECDSA

Core Security Services

The objectives of a security systems are called *security services*.

1. **Confidentiality *(dôvernosť)****:* Information is kept secret from all but authorized parties.
2. **Message Integrity *(integrita správ)*:** Ensures that a message has not been modified in transit.
3. **Message Authentication *(autentizácia správ):*** Ensures that the sender of a message is authentic. An alternative term is data origin authentication.
4. **Non-repudiation *(nepopierateľnosť)****:* Ensures that the sender of a message can not deny the creation of the message.

Non-repudiation: Motivation

- Bob orders a pink car from the car salesmen Alice over the internet.
- After seeing the pink car, Bob states that he has never ordered it.
- How can Alice prove towards a judge that Bob has ordered a pink car? (And that she did not fabricate the order herself)
- It would help if when ordering the car, Bob would have to “digitally sign“ his order in a manner **only** Bob can do.
- We can achieve this with public-key cryptography!

Content of this Chapter

- Security services
- **The principle of digital signatures**
- The RSA digital signature scheme
- DSA and ECDSA

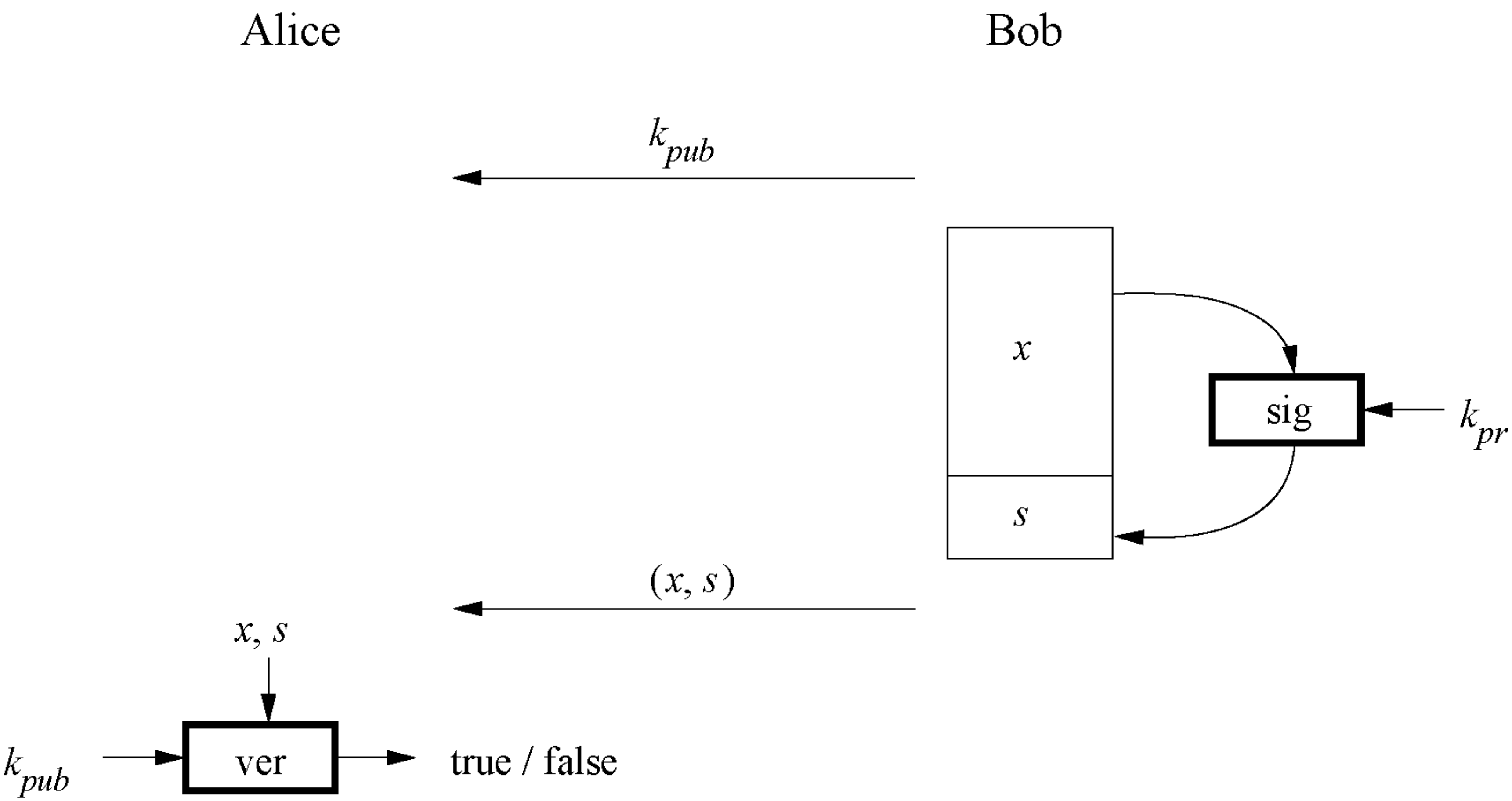
Main idea

- Bob has a private key and a public key.
- The private key is needed to generate Bob's signature.
- With Bob's public key, anyone can verify the validity of the signature.
- The signature must change for every document.

$\Rightarrow$ The signature is realized as a function with the message x and the private key as input.

$\Rightarrow$ The public key and the message x are the inputs to the verification function.

Basic Principle of Digital Signatures



Digital Signature and Security Services

1. **Confidentiality *(dôvernosť)*:** **is not provided by digital signatures**
2. **Message Integrity *(integrita správ)*:** **is provided by digital signatures**
3. **Message Authentication *(autentizácia správ):*** **is provided by digital signatures**
4. **Non-repudiation *(nepopierateľnosť)*:** **is provided by digital signatures**

Content of this Chapter

- Security services
- The principle of digital signatures
- **The RSA digital signature scheme**
- DSA and ECDSA

Main idea of the RSA signature scheme

To generate the private and public key:

- Use the same key generation as RSA encryption.

To generate the signature:

- "encrypt" the message *x* with the private key

$$s = sig_{K_{priv}}(x) = x^d \bmod n$$

- Append *s* to message *x*

To verify the signature:

- "decrypt" the signature with the public key

$$x' = ver_{K_{pub}}(s) = s^e \bmod n$$

- If $x=x'$, the signature is valid

The RSA Signature Protocol

Alice		Bob
	$\xleftarrow{K_{pub}}$	$K_{pr} = d$ $K_{pub} = (n, e)$
		Compute signature: $s = sig_{k_{pr}}(x) \equiv x^d \bmod n$
	$\xleftarrow{(x,s)}$	

Verify signature:

$x' \equiv s^e \bmod n$

If $x' \equiv x \bmod n \rightarrow$ valid signature

If $x' \not\equiv x \bmod n \rightarrow$ invalid signature

Security and Performance of the RSA Signature Scheme

Security:

The same constrains as RSA encryption: n needs to be at least 2048 bits.

⇒ The signature, consisting of s, needs to be at least 2048 bits long.

Performance:

The signing process is an exponentiation with the private key and the verification process an exponentiation with the public key e.

⇒ Signature verification is very efficient as a small number can be chosen for the public key.

Existential Forgery Attack against RSA Digital Signature

Alice	Oscar	Bob
		$K_{pr} = d$ $K_{pub} = (n, e)$
← (n,e)	← (n,e)	
	1. Choose signature: $s \in Z_n$ 2. Compute message: $x \equiv s^e \bmod n$	
← (x,s)		

Verification:
$s^e \equiv x' \bmod n$

since $s^e = (x^d)^e \equiv x \bmod n$
→ Signature is valid

Existential Forgery and Padding

- An attacker can generate valid message-signature pairs (*x*,*s*)
- But an attack can only choose the signature *s* and NOT the message *x*

⇒ Attacker cannot generate messages like „Transfer $1000 into Oscar's account"

Formatting the message *x* according to a *padding scheme* can be used to make sure that an attacker cannot generate valid (*x*,*s*) pairs.

(A messages *x* generated by an attacker during an Existential Forgery Attack will not coincide with the padding scheme. For more details see Chapter 10 in *Understanding Cryptography.)*

Content of this Chapter

- Security services
- The principle of digital signatures
- The RSA digital signature scheme
- **DSA and ECDSA**

Digital Signature Algorithm (DSA)

- Federal US Government standard for digital signatures (DSS)
- Proposed by the National Institute of Standards and Technology (NIST)
- DSA is based on the Elgamal signature scheme
- Signature is only 448 bits long when the modulus is 2048 bits
- Signature verification is slower compared to RSA

For more details see Section 10.4 in *Understanding Cryptography.*

Elliptic Curve Digital Signature Algorithm (ECDSA)

- Based on Elliptic Curve Cryptography (ECC)
- Bit lengths in the range of 256-512 bits can be chosen to provide security equivalent to 3072-15360 bit RSA
- One signature consists of two points, hence the signature is twice the used bit length (i.e., 512-1024 bits)
- The shorter bit length of ECDSA often result in shorter processing time

For more details see Section 10.5 in *Understanding Cryptography*

Lessons Learned

- Digital signatures provide message integrity, message authentication and non-repudiation.
- RSA and the Elliptic Curve Digital Signature Standard (ECDSA) are currently the most widely used digital signature algorithms. Other popular digital signature algorithm is DSA (aka DSS).
- Compared to RSA, ECDSA has the advantage of much shorter signatures.
- RSA verification can be done with short public keys e. Hence, in practice, RSA verification is usually faster than signing.
- In order to prevent certain attacks, RSA should be used with padding.
- The modulus of RSA and DSA signature schemes should be at least 2048 bits long. For true long-term security, a modulus of length 3072 bits should be chosen. In contrast, ECDSA achieves the same or higher security levels with bit lengths in the range 256-512 bits.