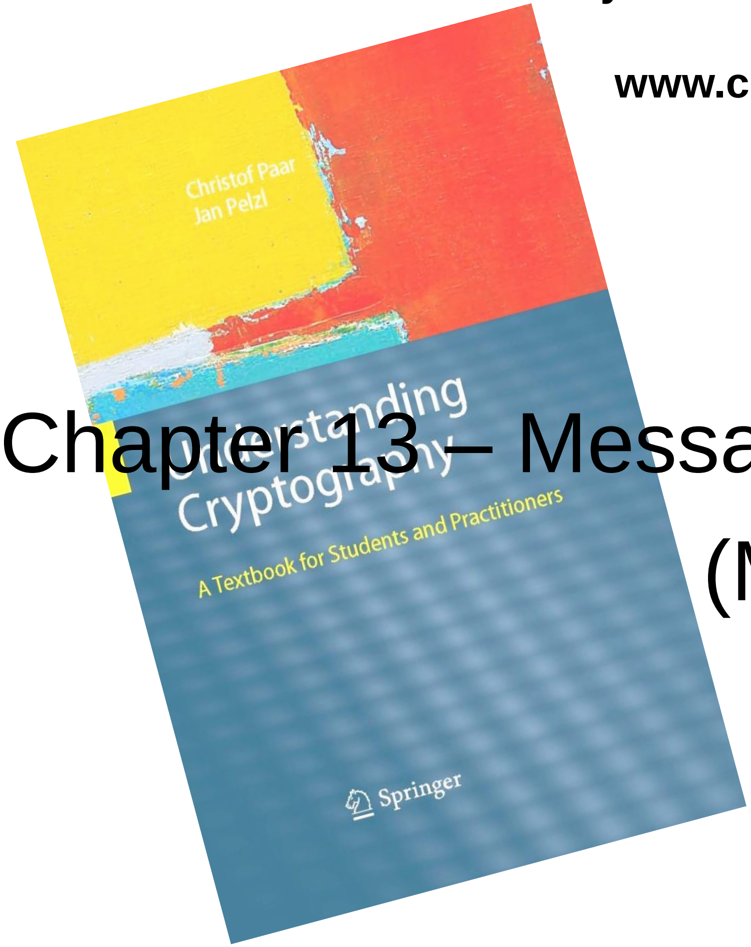
Understanding Cryptography

by Christof Paar and Jan Pelzl

www.crypto-textbook.com


Christof Paar
Jan Pelzl
Understanding Cryptography
A Textbook for Students and Practitioners
Springer

Chapter 13 – Message Authentication Codes (MACs)

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

Homework

- Read Section 13.1

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.

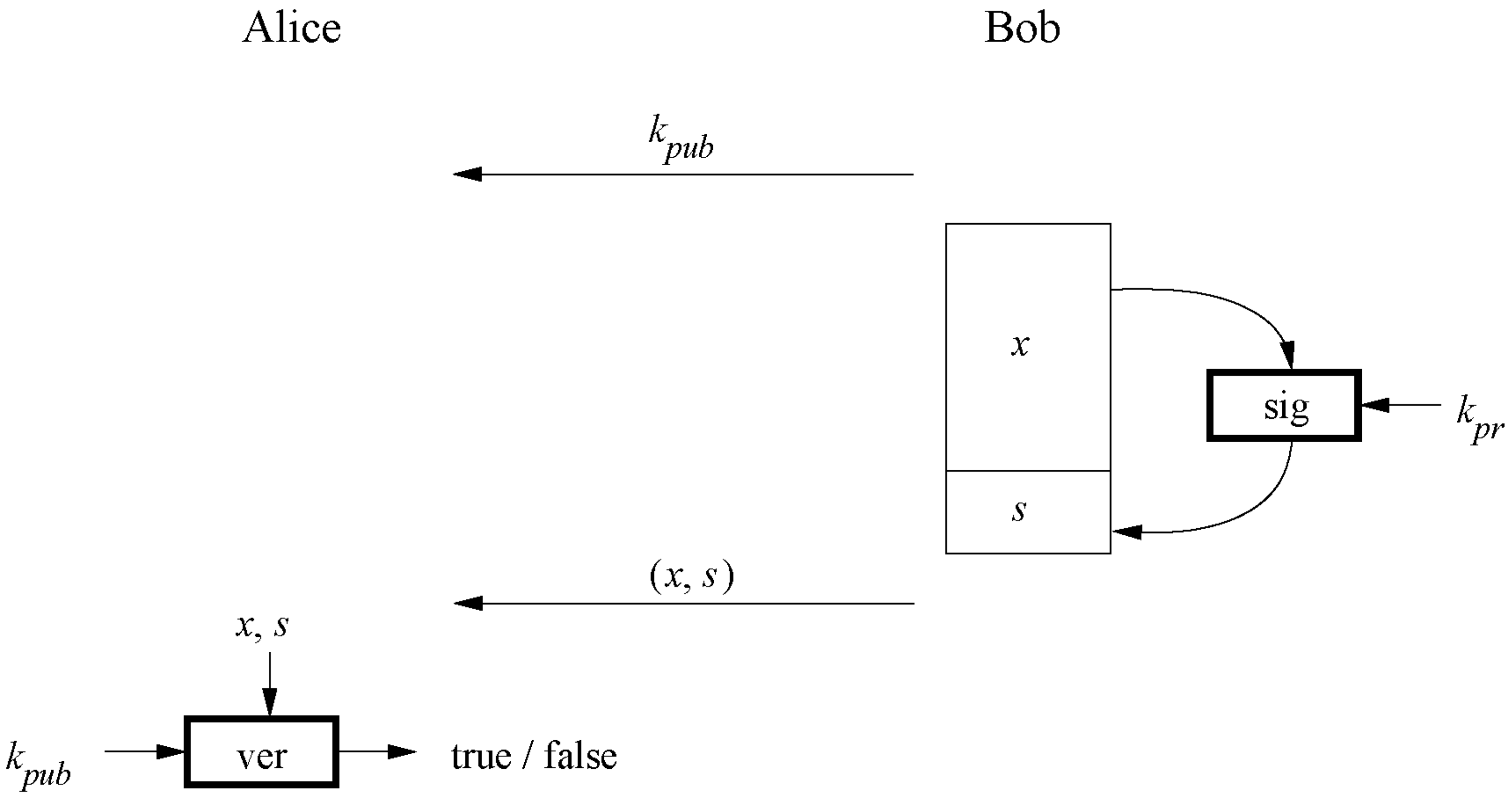
Content of this Chapter

- Reminder of digital signatures
- The principle behind MACs
- Collision attacks and MACs
- Popular MACs
- Authenticated encryption

Content of this Chapter

- **Reminder of digital signatures**
- The principle behind MACs
- Collision attacks and MACs
- Popular MACs
- Authenticated encryption

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

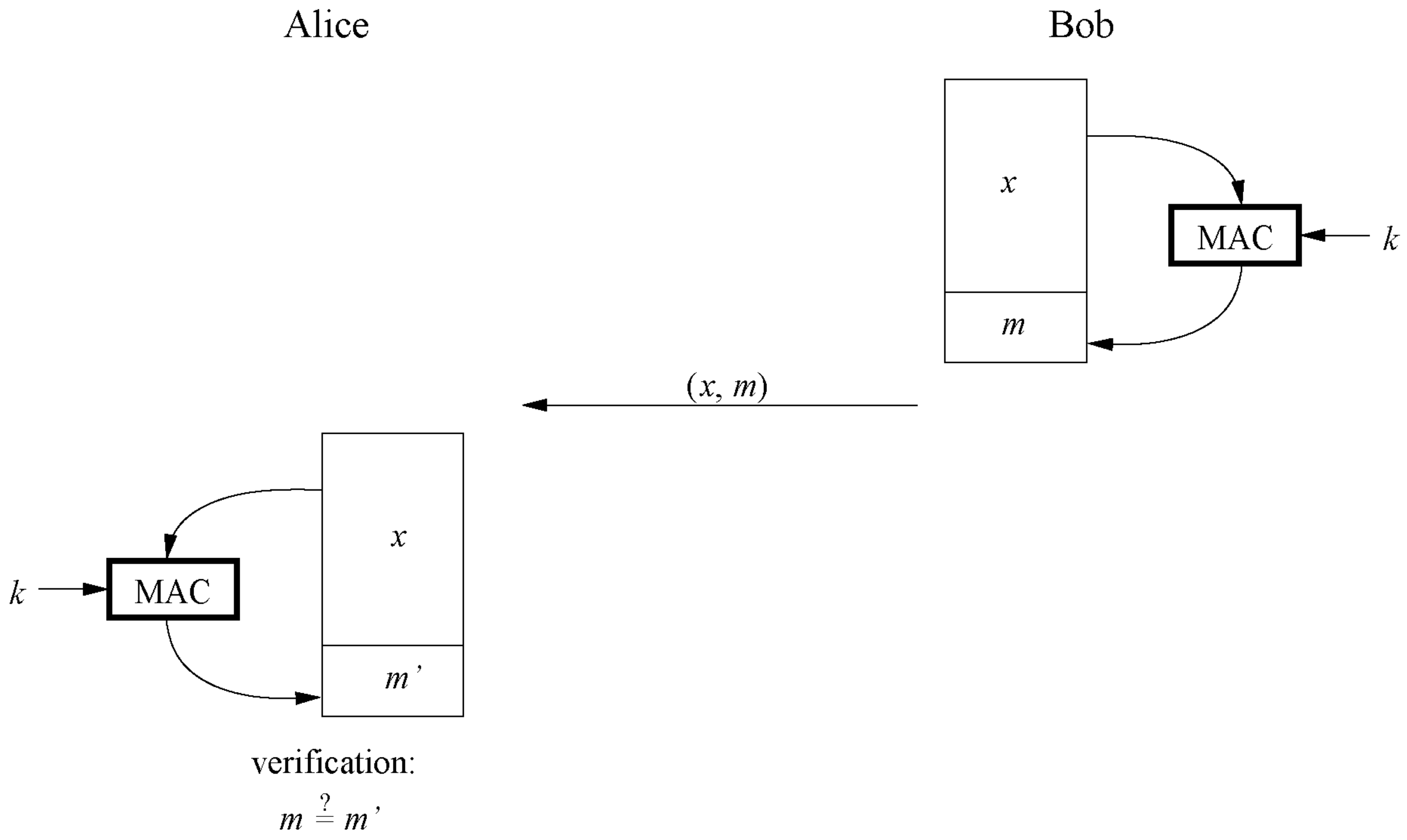
- Reminder of digital signatures
- **The principle behind MACs**
- Collision attacks and MACs
- Popular MACs
- Authenticated encryption

Motivation for MACs

- In many cases, we do not need non-repudiation, but we still need message authentication.
- We can **achieve message authentication with symmetric cryptography**
- Advantage: faster than digital signatures

Principle of MACs

- Similar to digital signatures, MACs append an authentication tag to a message
- MACs use a symmetric key *k* for generation and verification



Properties of MACs

1. **Cryptographic checksum**

   A MAC generates a cryptographically secure authentication tag for a given message.

2. **Symmetric**

   MACs are based on secret symmetric keys. The signing and verifying parties must share a secret key.

3. **Arbitrary message size**

   MACs accept messages of arbitrary length.

4. **Fixed output length**

   MACs generate fixed-size authentication tags.

Note: Properties 3. and 4. are shared with hash functions. In fact, MACs are sometimes called "*keyed hash functions*".

MACs and Security Services

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

Content of this Chapter

- Reminder of digital signatures
- The principle behind MACs
- **Collision attacks and MACs**
- Popular MACs
- Authenticated encryption

Collisions and MACs

- As in the case of hash functions, there will be collisions in MACs:

For every key k there will be pairs of messages (x,x‘) such that

$$\mathrm{MAC}_k(x) = \mathrm{MAC}_k(x‘)$$

- However, Oscar cannot search for these collisions offline (i.e. without assistance of Bob or Alice), since to find a collision the knowledge of k is needed
- Thus, to achieve the security level of 128 bits, it is sufficient to have the output length of 128 bits in MACs (in case of hash functions outputs of 256 bits are needed)

Content of this Chapter

- Reminder of digital signatures
- The principle behind MACs
- Collision attacks and MACs
- **Popular MACs**
- Authenticated encryption

- **Popular MACs**

- A very popular MAC today is **HMAC**.
- Other MACs used today are:

  CMAC

  GMAC

  CBC-MAC

but CBC-MAC has some security deficiencies.

Content of this Chapter

- Reminder of digital signatures
- The principle behind MACs
- Collision attacks and MACs
- Popular MACs
- **Authenticated encryption**

Authenticated encryption

- In many applications it is desirable to **provide confidentiality and at the same time authentication and integrity**.
- One way of achieving this is to use one of the modes of operation described in Chapter 5 for encryption together with a MAC.
- However, it often is attractive to have an encryption function that performs message encryption and MAC computation **in one pass**.
- Such cryptographic primitives are referred to as **authenticated encryption.**
- Modes of operation of symmetric ciphers which provide authenticated encryption:
  - **GCM** (aka **Galois Counter Mode**)
  - **CCM**
- The latest version of TLS suppports only these modes! (unauthenticated symmetric encryption is not supported)

Lessons Learned

- MACs provide two security services, *message integrity and message authentication,* using symmetric techniques. MACs are widely used in protocols.
- Both of these services also provided by digital signatures, but MACs are much faster as they are based on symmetric algorithms.
- MACs do not provide nonrepudiation.
- HMAC is a popular and very secure MAC, used in many practical protocols such as TLS.
- Authenticated encryption performs message encryption and MAC computation in one pass.
- Modes of operation of symmetric ciphers which provide authenticated encryption are GCM (aka Galois Counter Mode) and CCM.