Information Security

CS3002

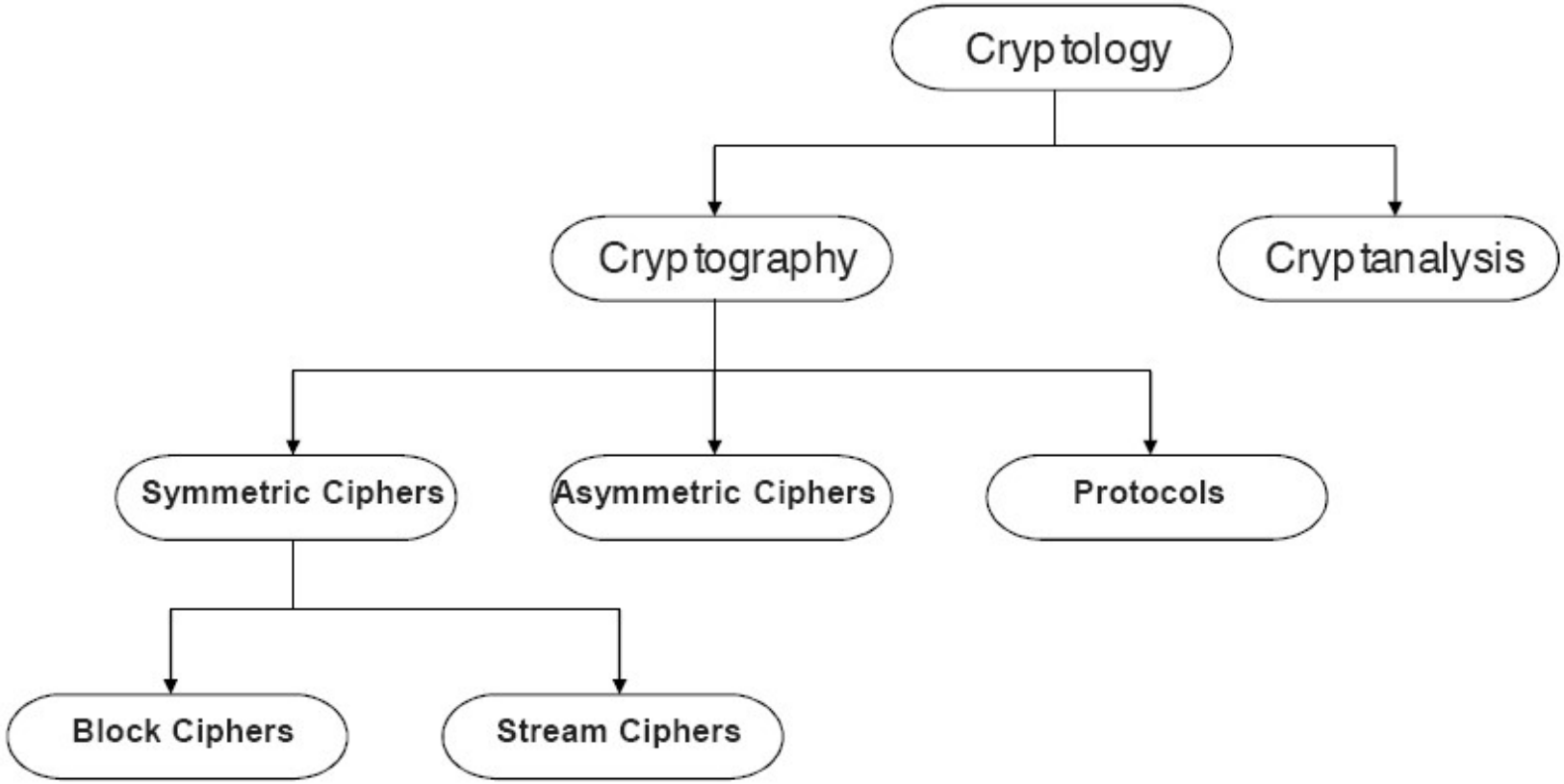
Lecture 9

21st September 2023

Dr. Rana Asif Rehman

Email: r.asif@lhr.nu.edu.pk

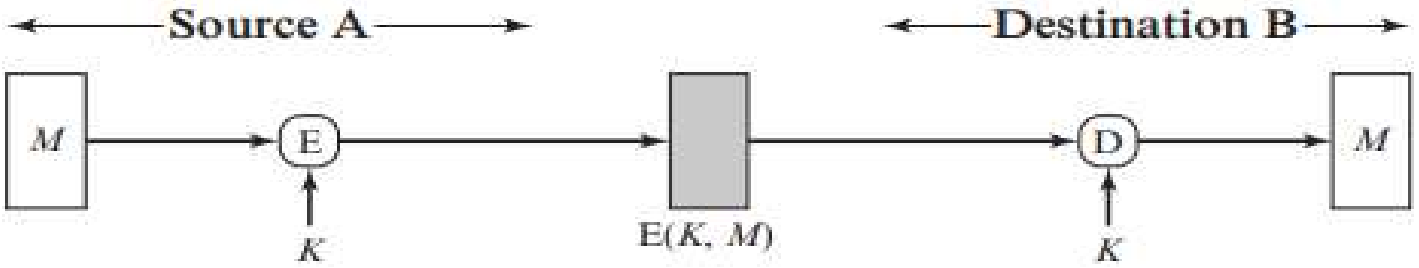
Classification of the Field of Cryptology



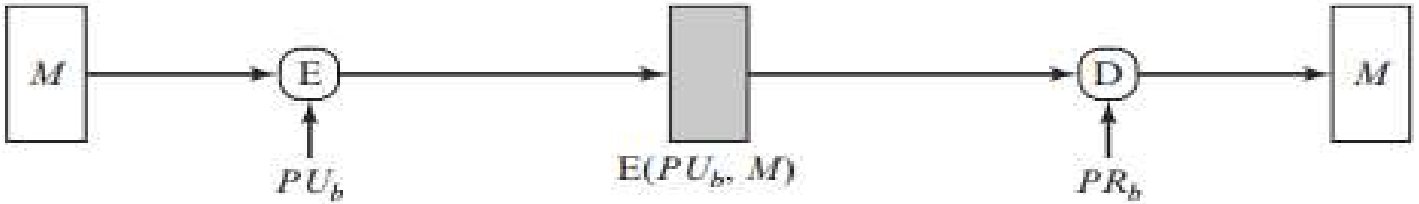
Adopted with thanks from: Chapter 1 of Understanding Cryptography by Christof Paar and Jan Pelzl

MESSAGE AUTHENTICATION CODE (MAC)

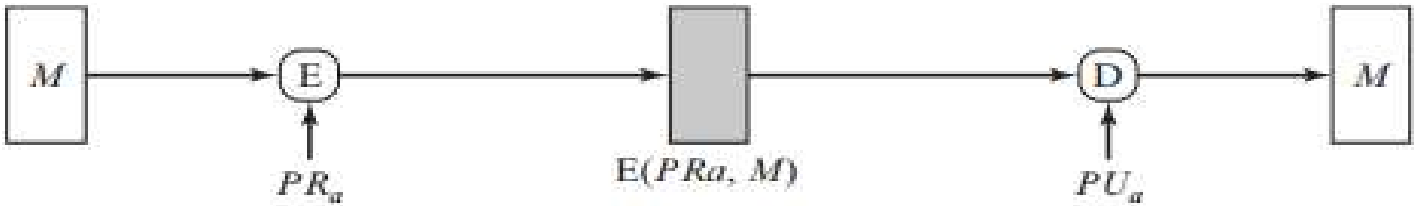
Authentication by Using of Encryption



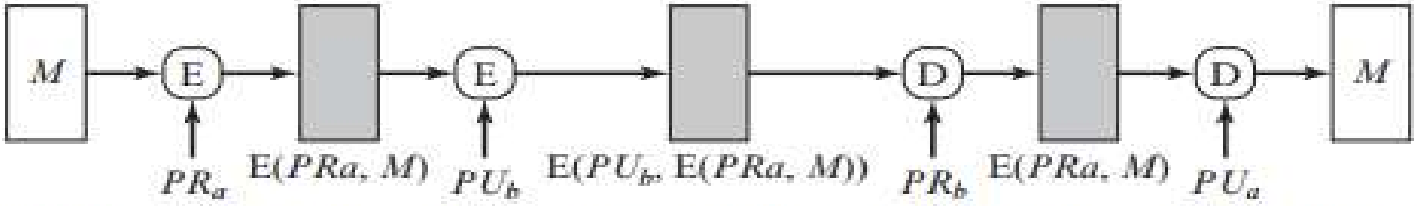
(a) Symmetric encryption: confidentiality and authentication



(b) Public-key encryption: confidentiality

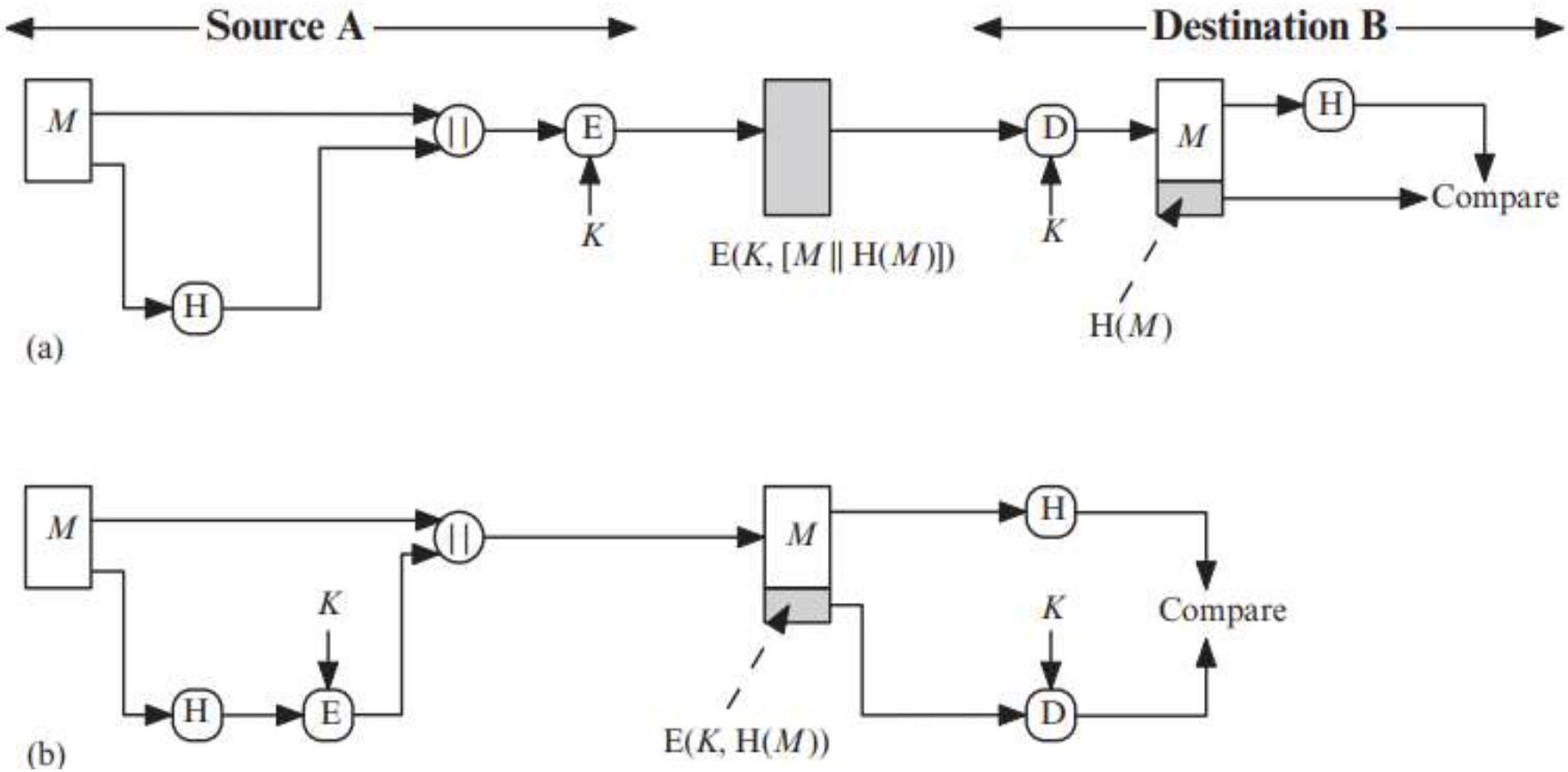


(c) Public-key encryption: authentication and signature

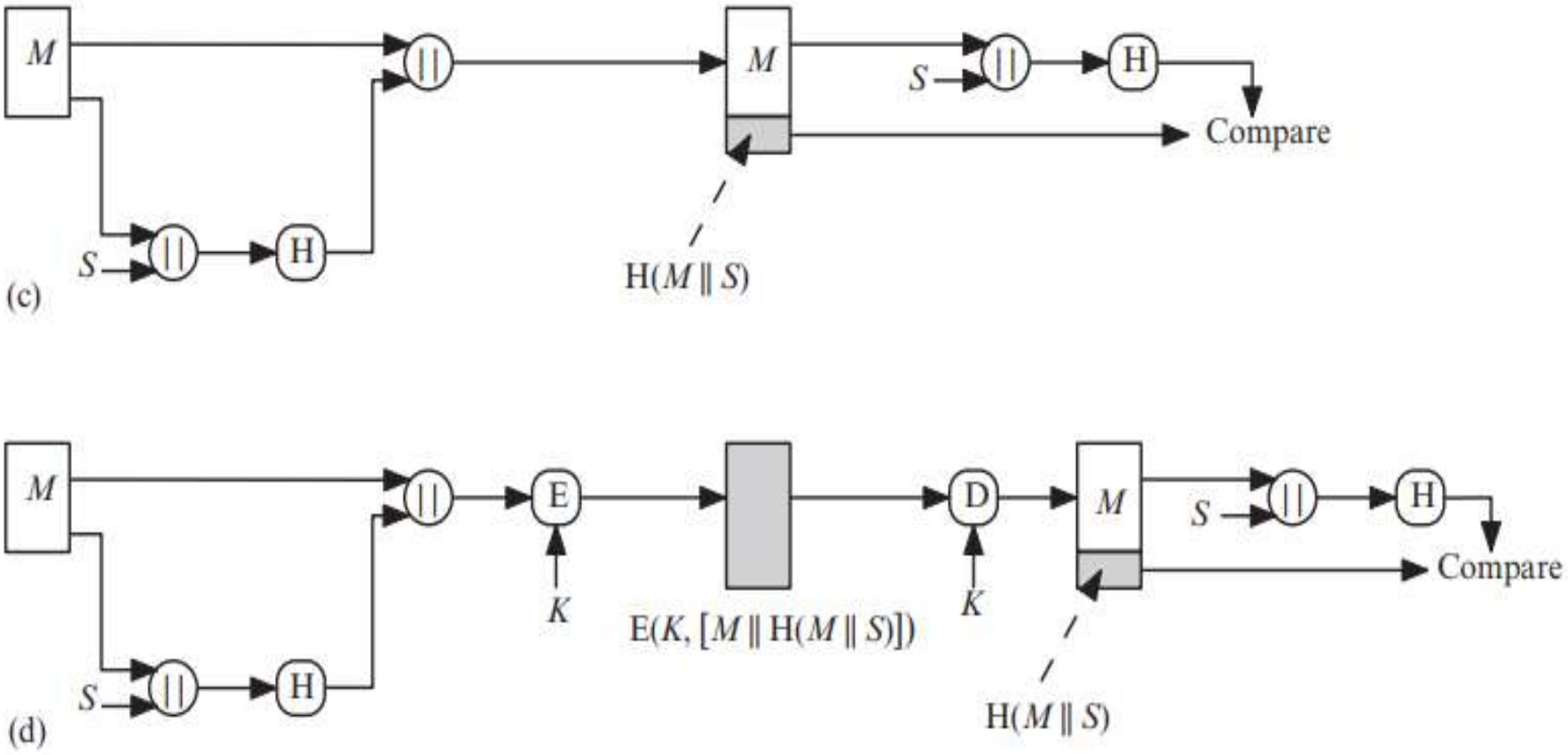


(d) Public-key encryption: confidentiality, authentication, and signature

Authentication by Using of Hash Function

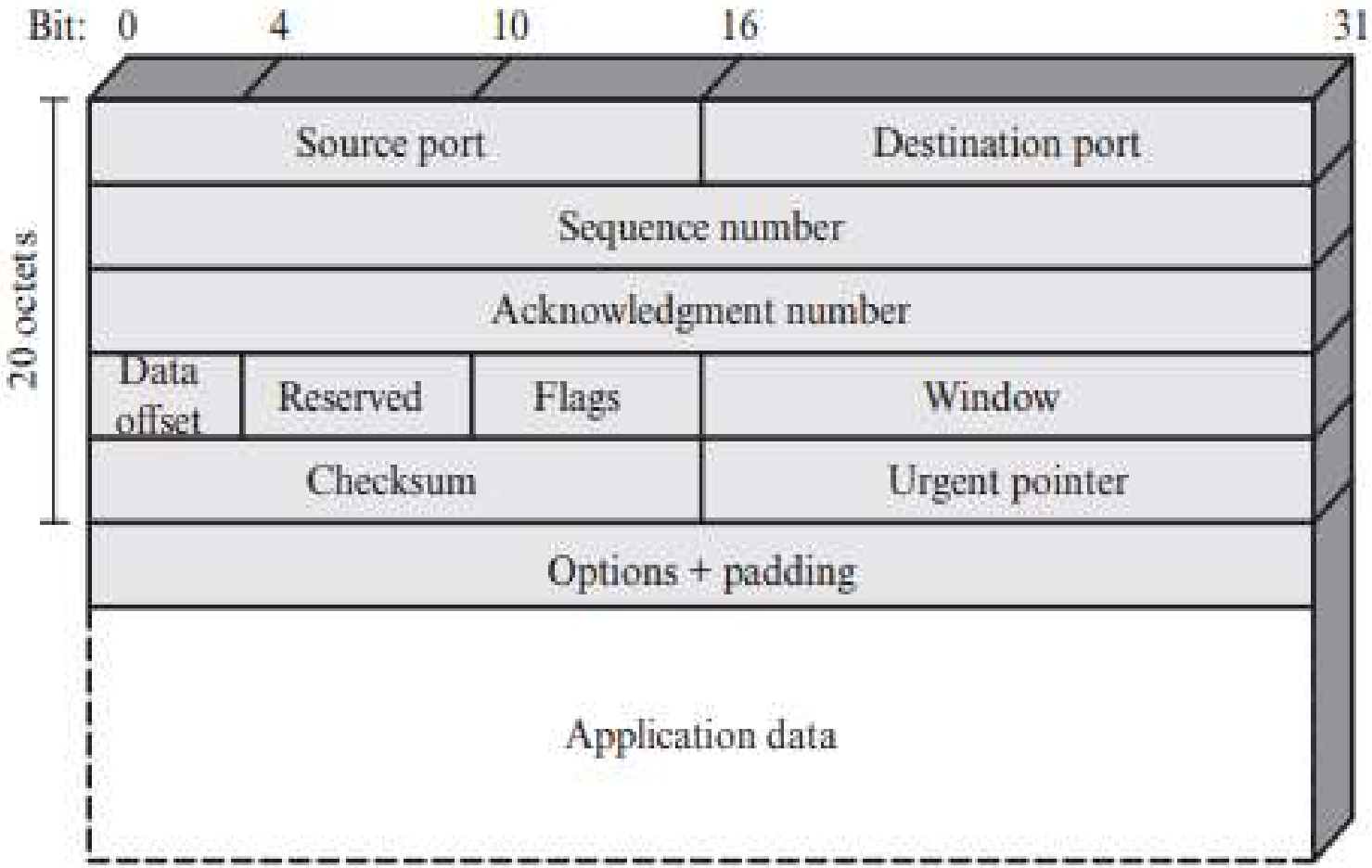


Authentication by Using of Hash Function



MESSAGE AUTHENTICATION CODE (MAC)

TCP Segment


Bit: 0
4
10
16
31
20 octets
Source port
Destination port
Sequence number
Acknowledgment number
Data offset
Reserved
Flags
Window
Checksum
Urgent pointer
Options + padding
Application data

Message Authentication Code (MAC)

- Also known as a *keyed hash function.*
- Typically used between two parties that share a secret key to authenticate information exchanged between those parties.

Takes as input a secret key and a data block and produces a hash value (MAC) which is associated with the protected message

- If the integrity of the message needs to be checked, the MAC function can be applied to the message and the result compared with the associated MAC value.
- An attacker who alters the message will be unable to alter the associated MAC value without knowledge of the secret key.

Message Authentication Code (MAC)

- Generated by an algorithm that creates a small fixed-sized block.
  - Depending on both message and some key.
  - Like encryption though need not be reversible.
- Appended to message as a **signature.**
- Receiver performs same computation on message and checks it matches the MAC.
- Provides assurance that message is unaltered and comes from sender.

MAC Properties

- A MAC is a cryptographic checksum

  `MAC = C(K,M)`

  – Condenses a variable-length message M.

  – Using a secret key K.

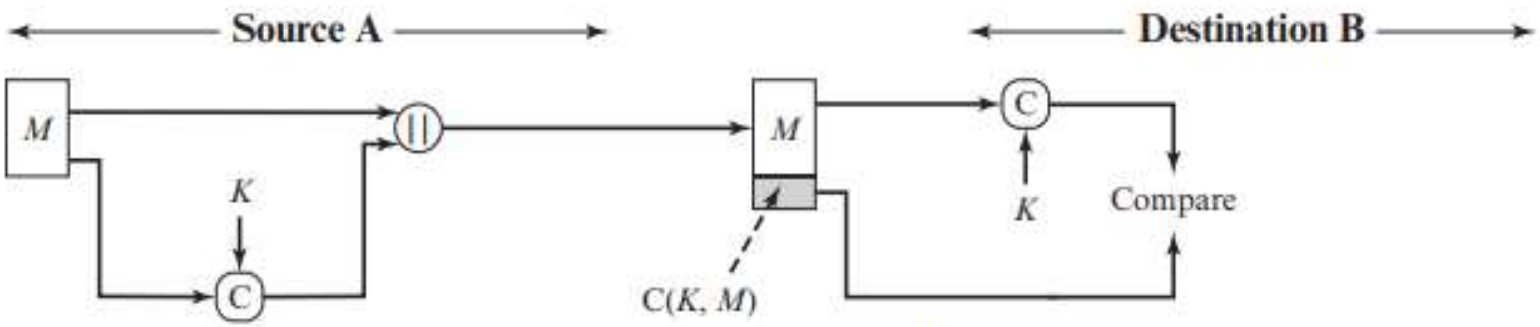
  – To a fixed-sized authenticator.

- Is a many-to-one function

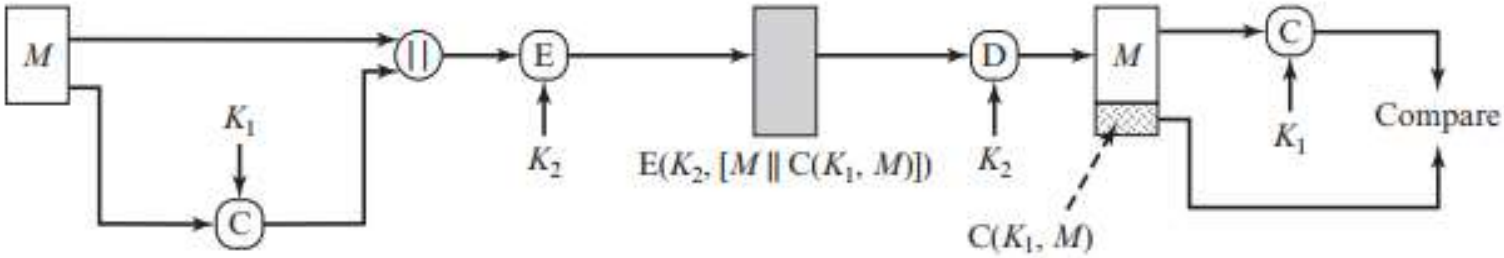
  – Potentially many messages have same MAC.

  – But finding these needs to be very difficult.

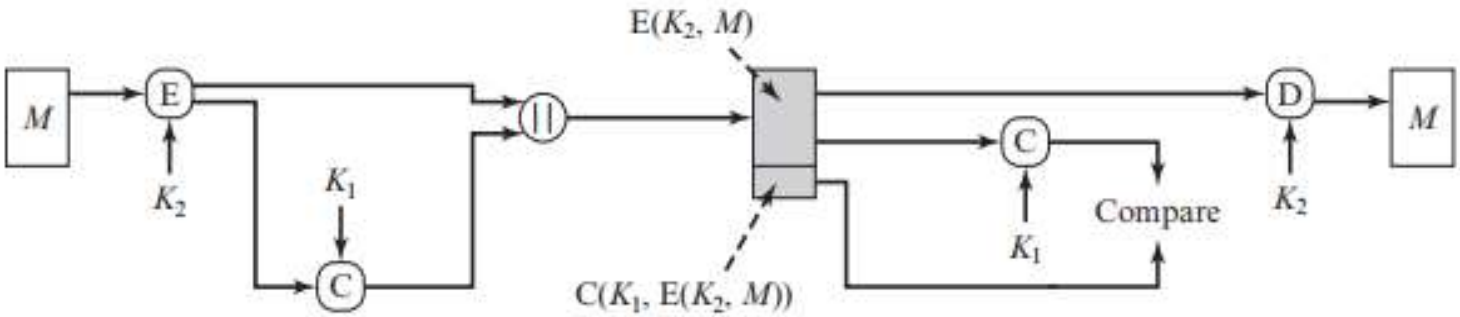
Message Authentication Code (cont.)



(a) Message authentication



(b) Message authentication and confidentiality; authentication tied to plaintext



(c) Message authentication and confidentiality; authentication tied to ciphertext

Requirements for MACs

- Taking into account the types of attacks need the MAC to satisfy the following:
  1. Knowing a message and MAC, is infeasible to find another message with same MAC.
  2. MACs should be uniformly distributed.
  3. MAC should depend equally on all bits of the message.

Brute-Force Attack

- Requires known message-tag pairs
  - A brute-force method of finding a collision is to pick a random bit string *y* and check if H(*y*) = H(*x*)

Two lines of attack:

- Attack the key space
  - If an attacker can determine the MAC key then it is possible to generate a valid MAC value for any input *x*.
- Attack the MAC value
  - Objective is to generate a valid tag for a given message or to find a message that matches a given tag.

Cryptanalysis

- Cryptanalytic attacks seek to exploit some property of the algorithm to perform some attack other than an exhaustive search.
- An ideal MAC algorithm will require a cryptanalytic effort greater than or equal to the brute-force effort.
- There is much more variety in the structure of MACs than in hash functions, so it is difficult to generalize about the cryptanalysis of MACs.

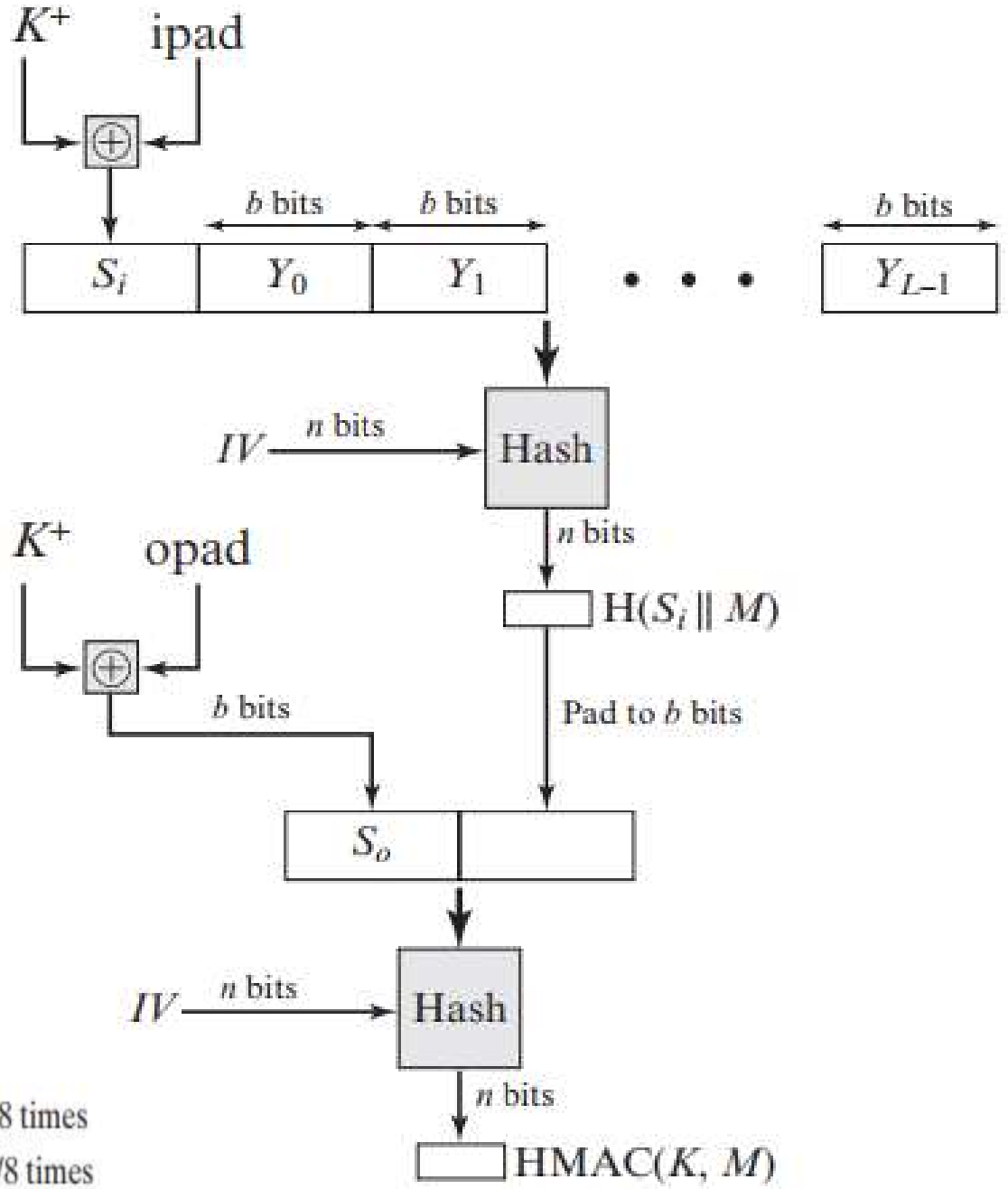
MACs Based on Hash Functions: **HMAC**

- There has been increased interest in developing a MAC derived from a cryptographic hash function.
- Motivations:
  - Cryptographic hash functions such as MD5 and SHA generally execute faster in software than symmetric block ciphers such as DES.
  - Library code for cryptographic hash functions is widely available.

- HMAC has been chosen as the mandatory-to-implement MAC for IP security.

- Has also been issued as a NIST standard (FIPS 198).

HMAC Structure



ipad = 00110110 (36 in hexadecimal) repeated $b/8$ times

opad = 01011100 (5C in hexadecimal) repeated $b/8$ times

Figure 12.5 HMAC Structure

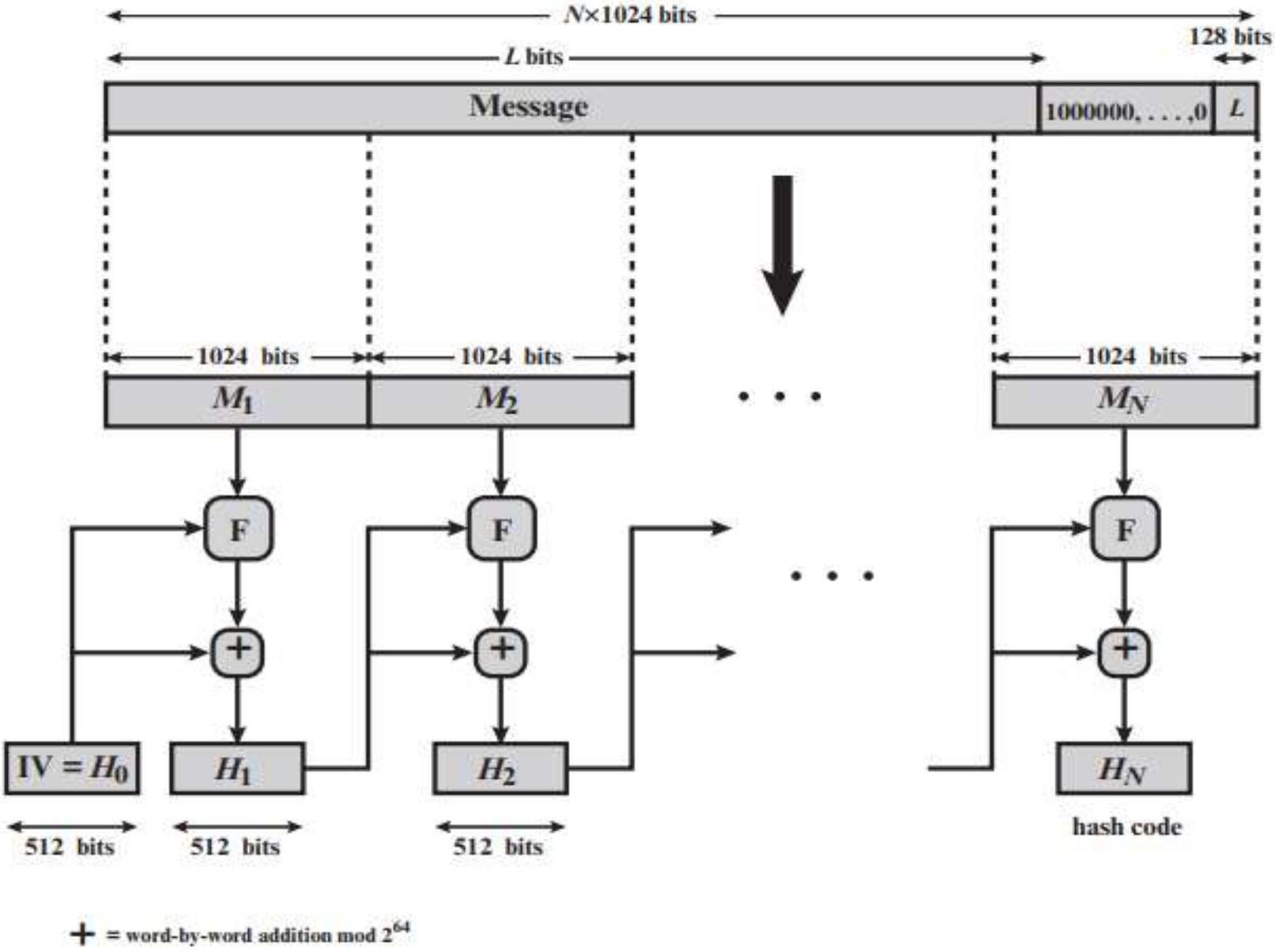


Figure 11.9 Message Digest Generation Using SHA-512

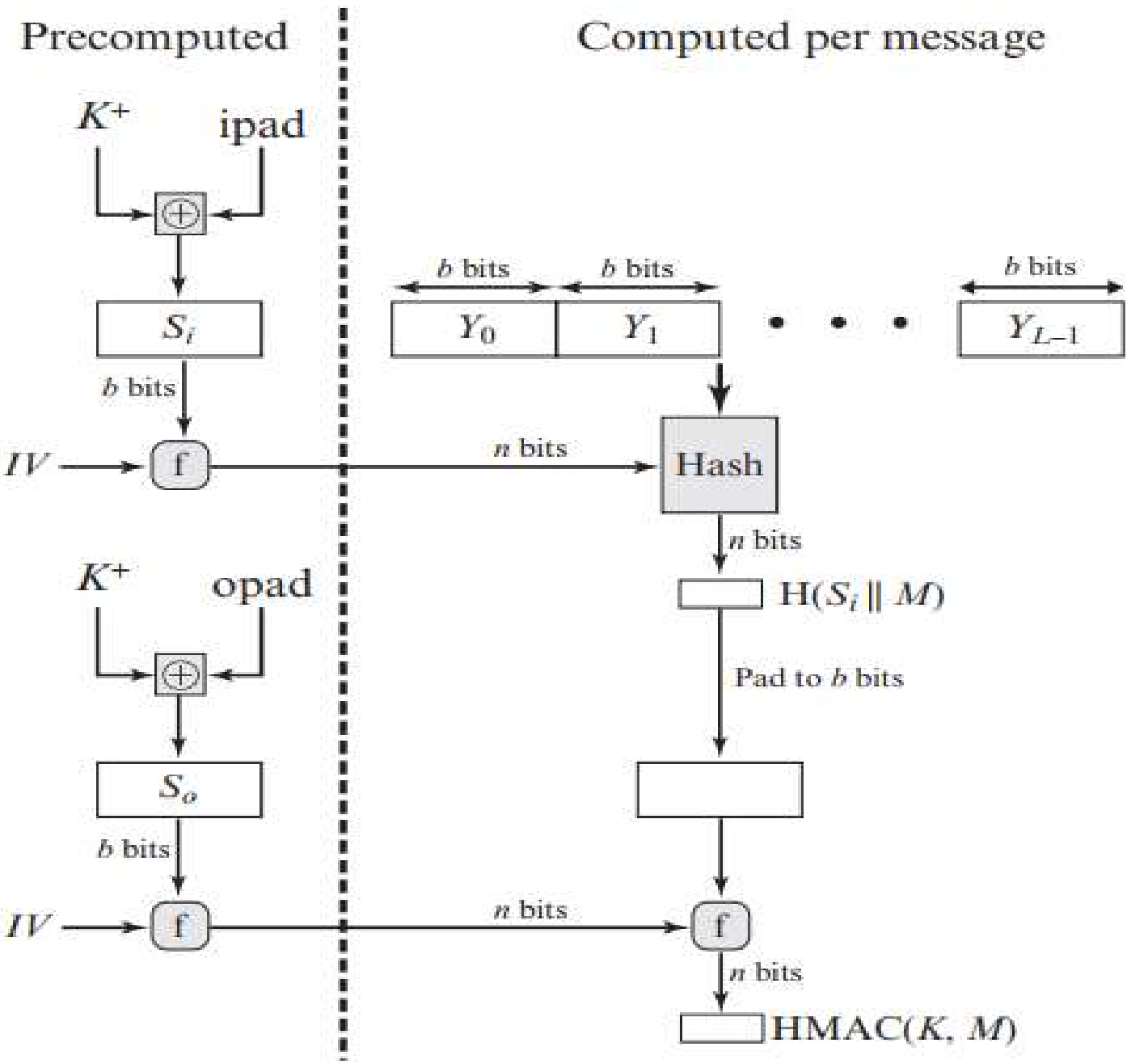


Figure 12.6 Efficient Implementation of HMAC