Chapter 12

Cryptographic Hash Functions

Chapter 12

Objectives

- ❑ To introduce general ideas behind cryptographic hash functions
- ❑ To discuss the Merkle-Damgard scheme as the basis for iterated hash functions
- ❑ To distinguish between two categories of hash functions:
- ❑ To discuss the structure of SHA-512.
- ❑ To discuss the structure of Whirlpool.

12-1 INTRODUCTION

A cryptographic hash function takes a message of arbitrary length and creates a message digest of fixed length. The ultimate goal of this chapter is to discuss the details of the two most promising cryptographic hash algorithms—SHA-512 and Whirlpool.

Topics discussed in this section:

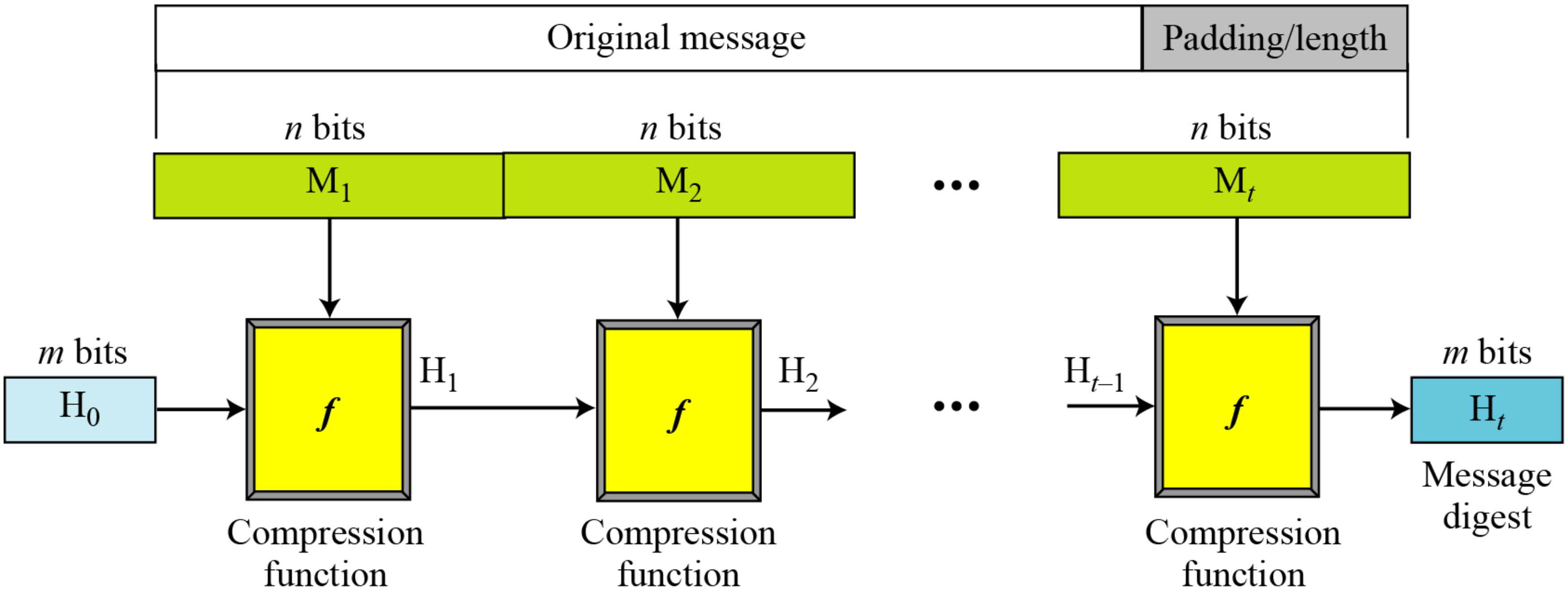
12.1.1 Iterated Hash Function

12.1.2 Two Groups of Compression Functions

12.1.1 Iterated Hash Function

Merkle-Damgard Scheme

Figure 12.1 ***Merkle-Damgard scheme***



12.1.2 Two Groups of Compression Functions

1. The compression function is made from scratch.

Message Digest (MD)

2. A symmetric-key block cipher serves as a compression function.

Whirlpool

Table 12.8 A Comparison of MD5, SHA-1, and RIPEMD-160

	MD5	SHA-1	RIPEMD-160
Digest length	128 bits	160 bits	160 bits
Basic unit of processing	512 bits	512 bits	512 bits
Number of steps	64 (4 rounds of 16)	80 (4 rounds of 20)	160 (5 paired rounds of 16)
Maximum message size	∞	$2^{64} - 1$ bits	$2^{64} - 1$ bits
Primitive logical functions	4	4	5
Additive constants used	64	4	9
Endianness	Little-endian	Big-endian	Little-endian

Table 12.9 Relative Performance of Several Hash Functions (coded in C++ on a 850 MHz Celeron)

Algorithm	MBps
MD5	26
SHA-1	48
RIPEMD-160	31

Note: Coded by Wei Dai; results are posted at http://www.eskimo.com/~weidai/benchmarks.html

12.1.2 Continued

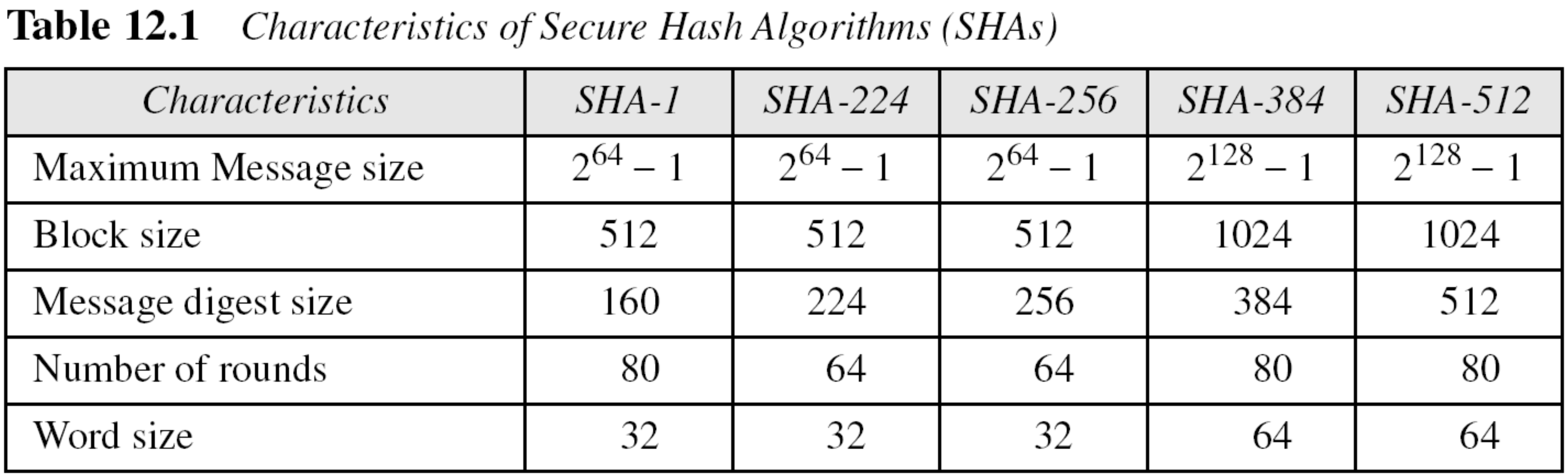


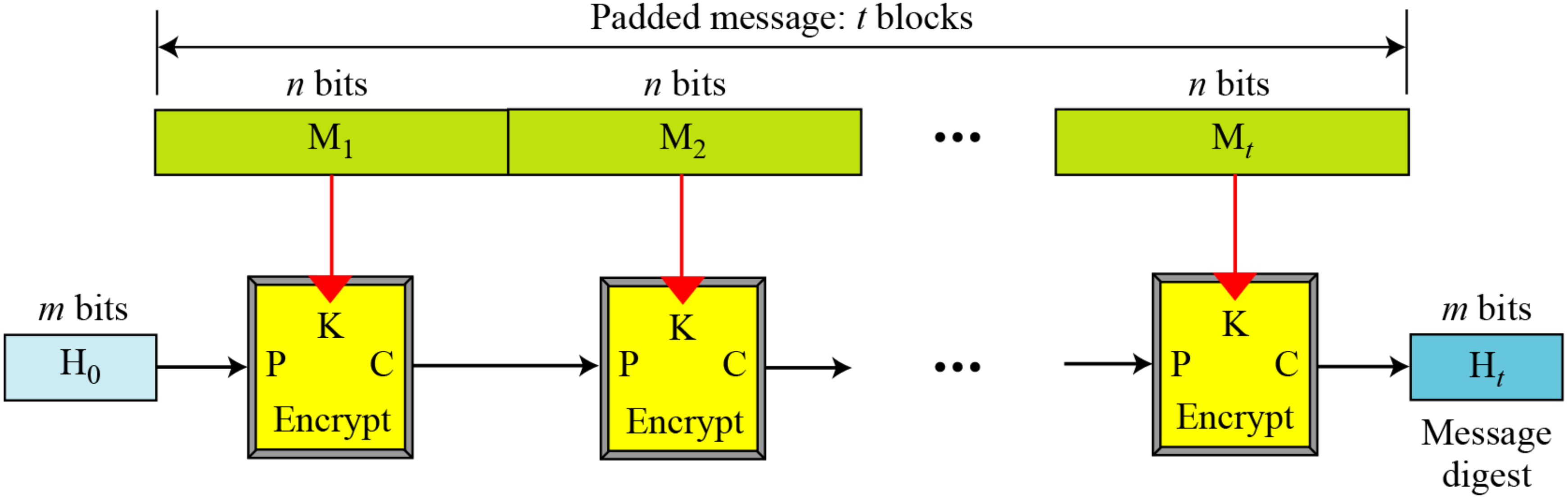
Table 12.1 *Characteristics of Secure Hash Algorithms (SHAs)*

Characteristics	*SHA-1*	*SHA-224*	*SHA-256*	*SHA-384*	*SHA-512*
Maximum Message size	$2^{64} - 1$	$2^{64} - 1$	$2^{64} - 1$	$2^{128} - 1$	$2^{128} - 1$
Block size	512	512	512	1024	1024
Message digest size	160	224	256	384	512
Number of rounds	80	64	64	80	80
Word size	32	32	32	64	64

12.1.2 Continued

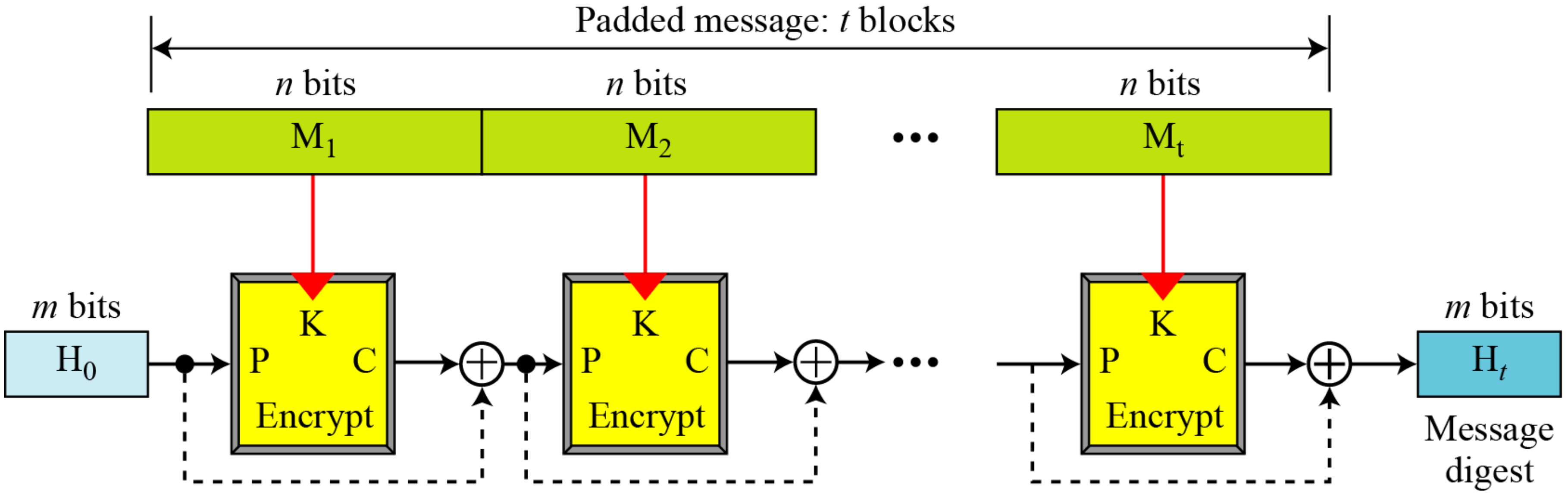
Rabin Scheme

Figure 12.2 ***Rabin scheme***



Davies-Meyer Scheme

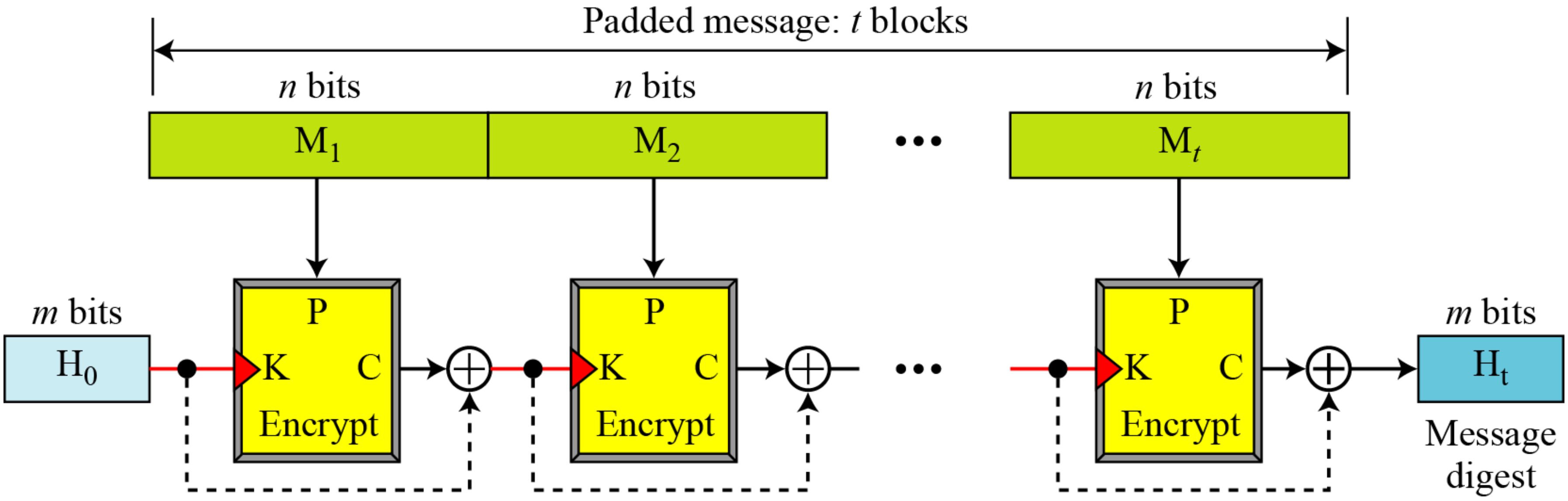
Figure 12.3 *Davies-Meyer scheme*



12.1.2 Continued

Matyas-Meyer-Oseas Scheme

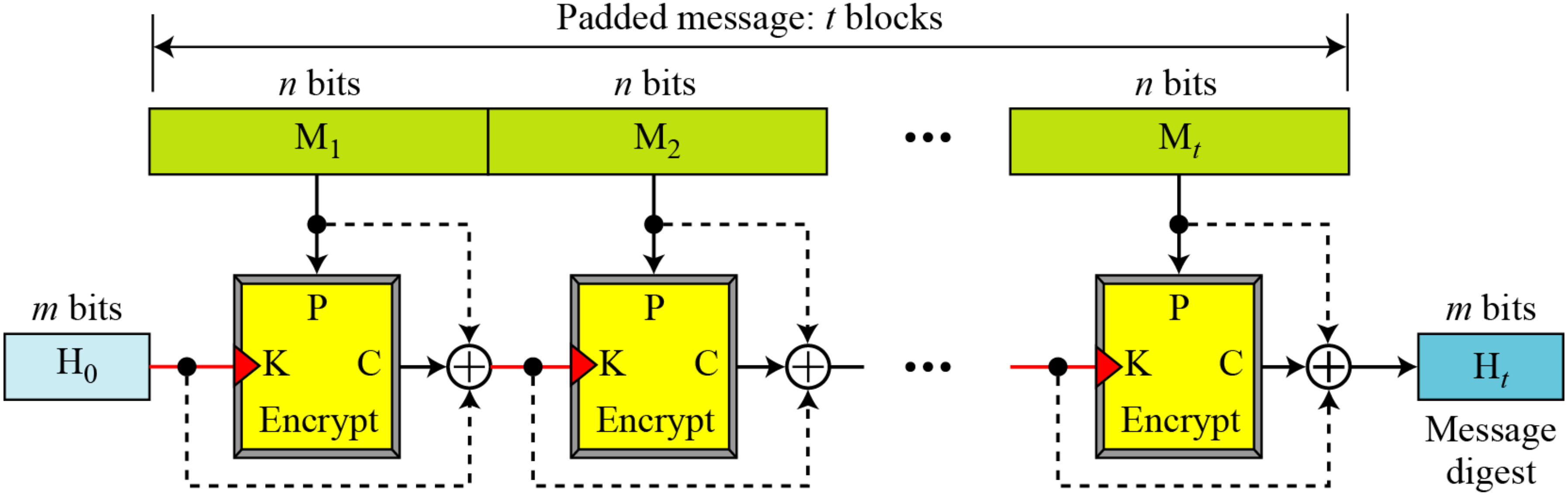
Figure 12.4 ***Matyas-Meyer-Oseas scheme***



12.1.2 Continued

Miyaguchi-Preneel Scheme

Figure 12.5 ***Miyaguchi-Preneel scheme***



12-2 SHA-512

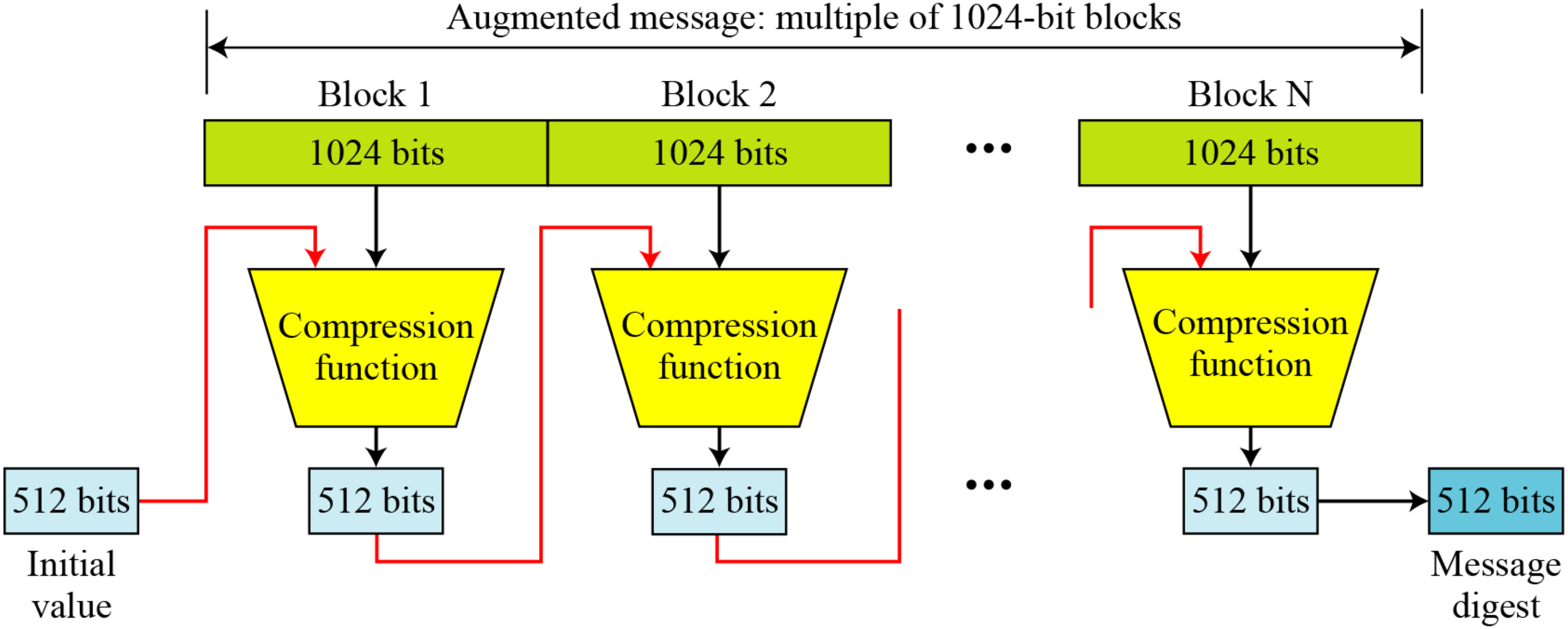
SHA-512 is the version of SHA with a 512-bit message digest. This version, like the others in the SHA family of algorithms, is based on the Merkle-Damgard scheme.

Topics discussed in this section:

12.2.1 Introduction
12.2.2 Compression Function
12.2.3 Analysis

12.2.1 Introduction

Figure 12.6 ***Message digest creation SHA-512***



12-3 WHIRLPOOL

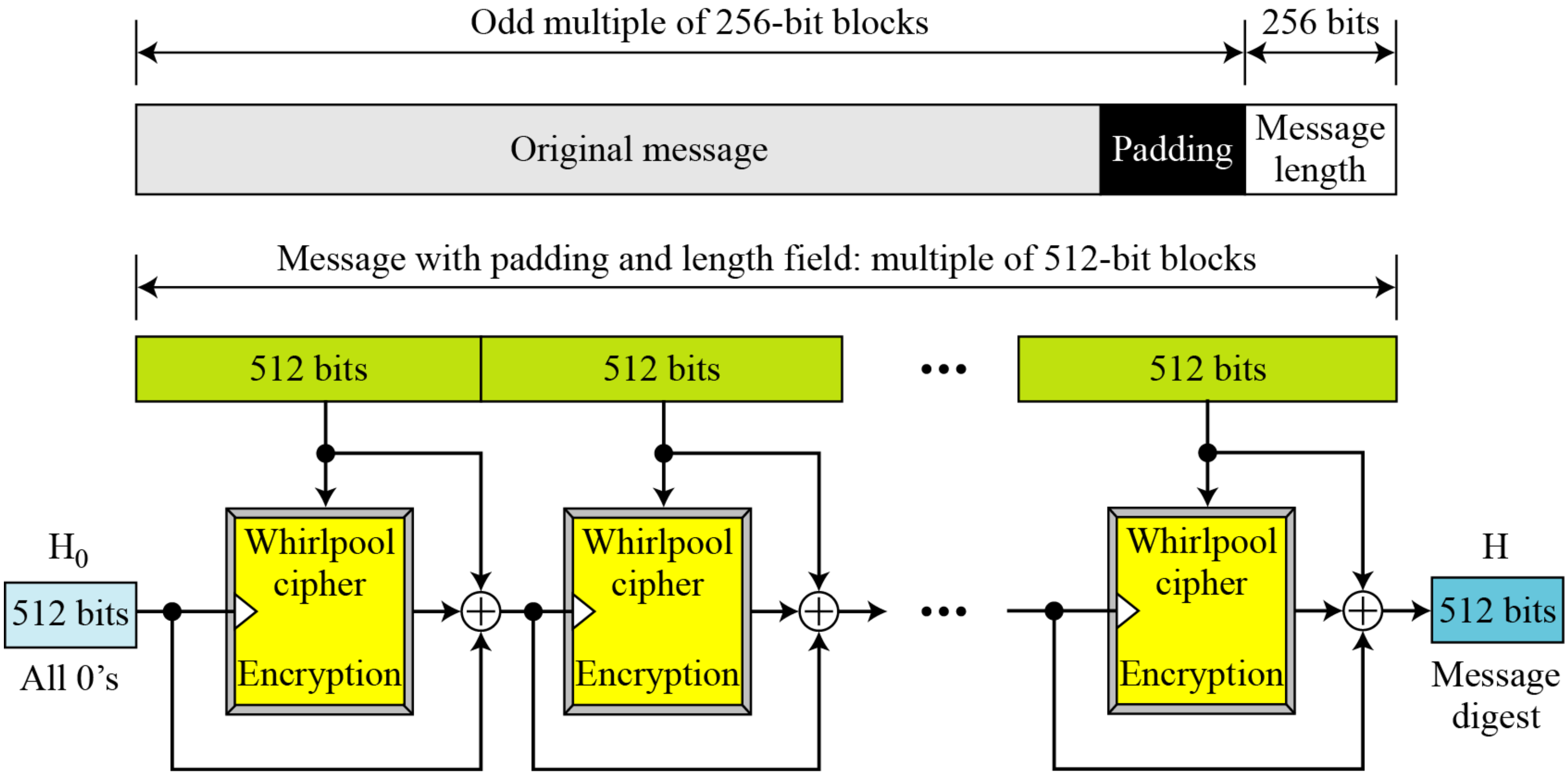
Whirlpool is an iterated cryptographic hash function, based on the Miyaguchi-Preneel scheme, that uses a symmetric-key block cipher in place of the compression function. The block cipher is a modified AES cipher that has been tailored for this purpose.

Topics discussed in this section:

12.3.1 Whirlpool Cipher
12.3.2 Summary
12.3.3 Analysis

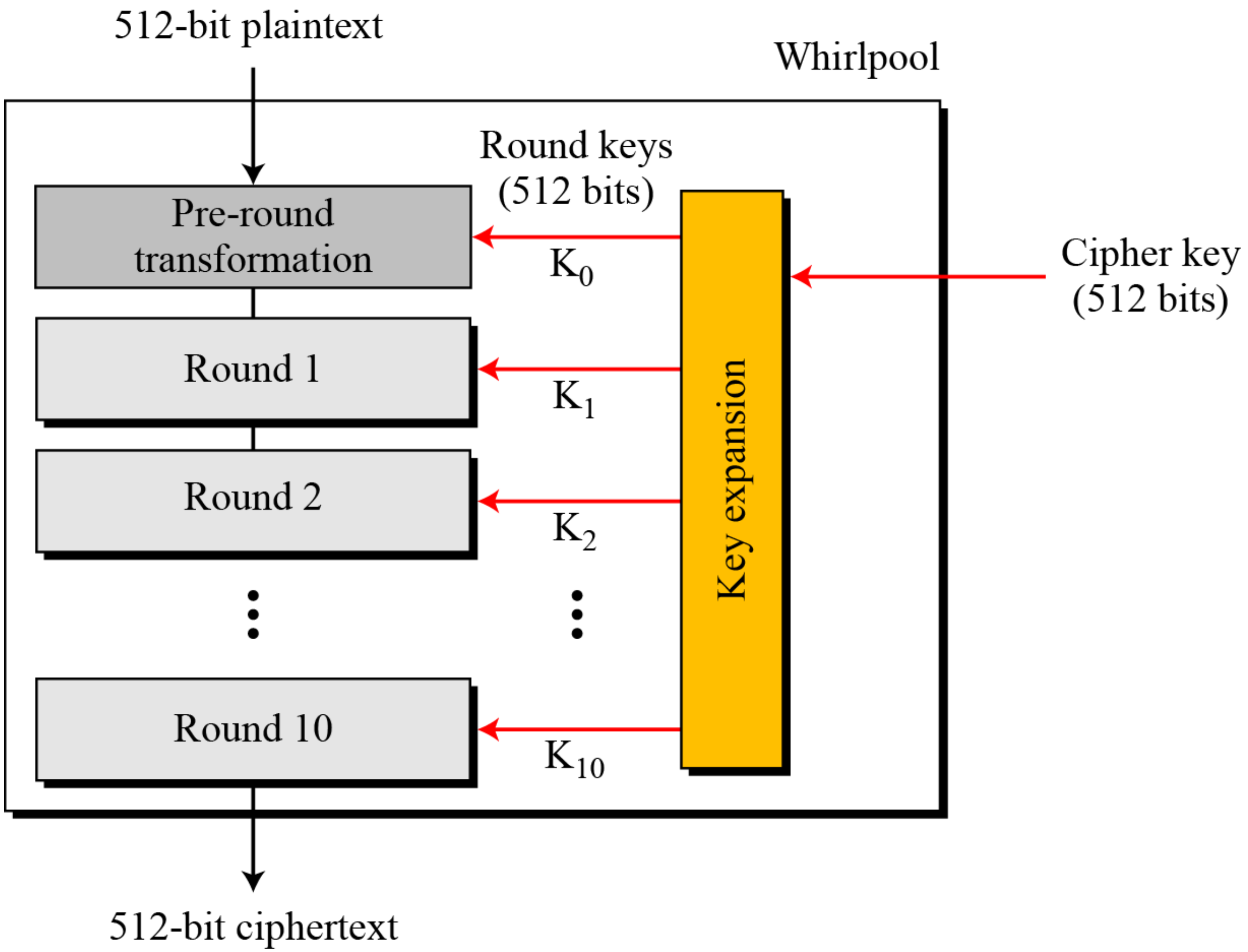
12-3 Continued

Figure 12.12 ***Whirlpool hash function***



12.3.1 Whirlpool Cipher

Figure 12.13 ***General idea of the Whirlpool cipher***



12.3.2 Summary

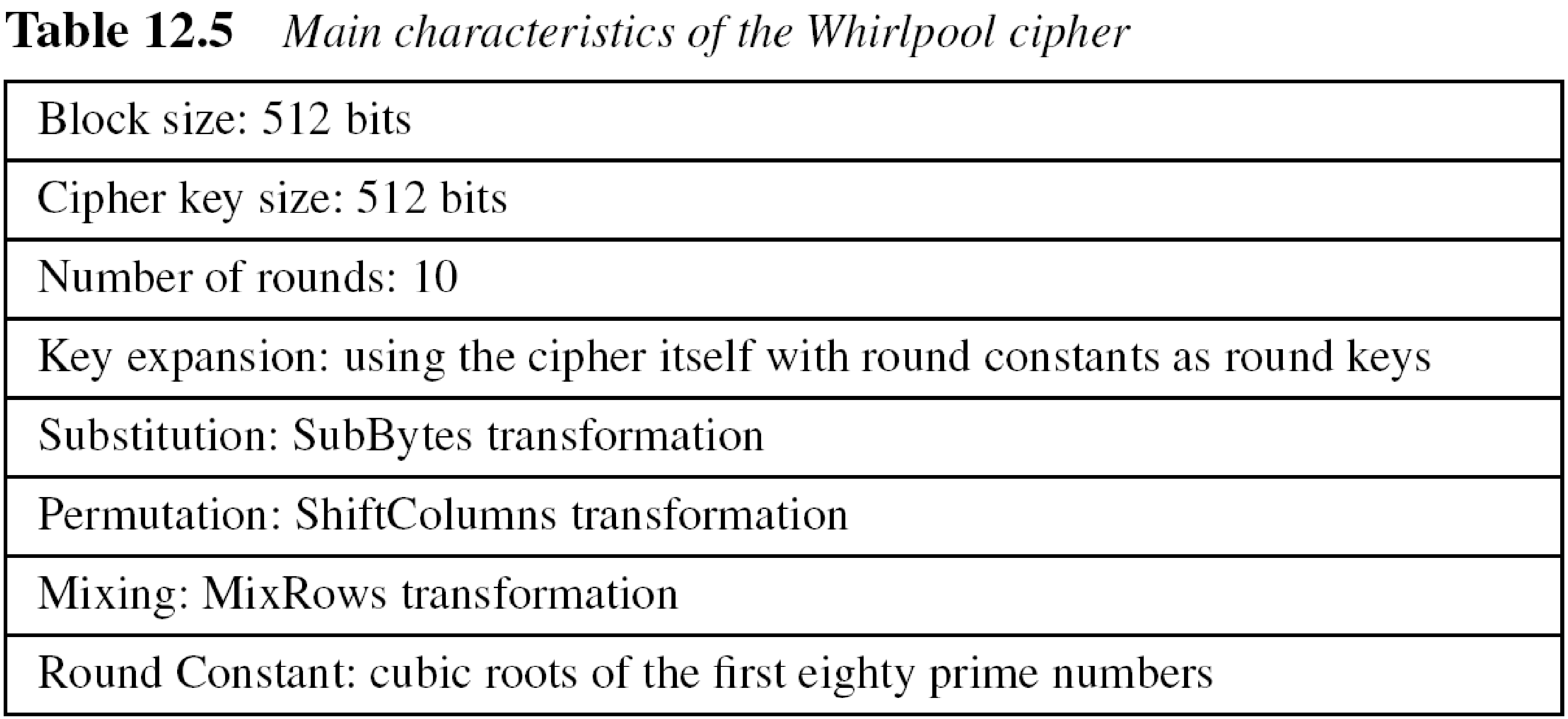


Table 12.5 *Main characteristics of the Whirlpool cipher*

Block size: 512 bits
Cipher key size: 512 bits
Number of rounds: 10
Key expansion: using the cipher itself with round constants as round keys
Substitution: SubBytes transformation
Permutation: ShiftColumns transformation
Mixing: MixRows transformation
Round Constant: cubic roots of the first eighty prime numbers

12.3.3 Analysis

Although Whirlpool has not been extensively studied or tested, it is based on a robust scheme (Miyaguchi-Preneel), and for a compression function uses a cipher that is based on AES, a cryptosystem that has been proved very resistant to attacks. In addition, the size of the message digest is the same as for SHA-512. Therefore it is expected to be a very strong cryptographic hash function.