

# Sample code to understand how Hashing works

**Presented BY: Dr Abdurashid Turgunov**

**Course name: Blockchain Technology**

# 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:](#)

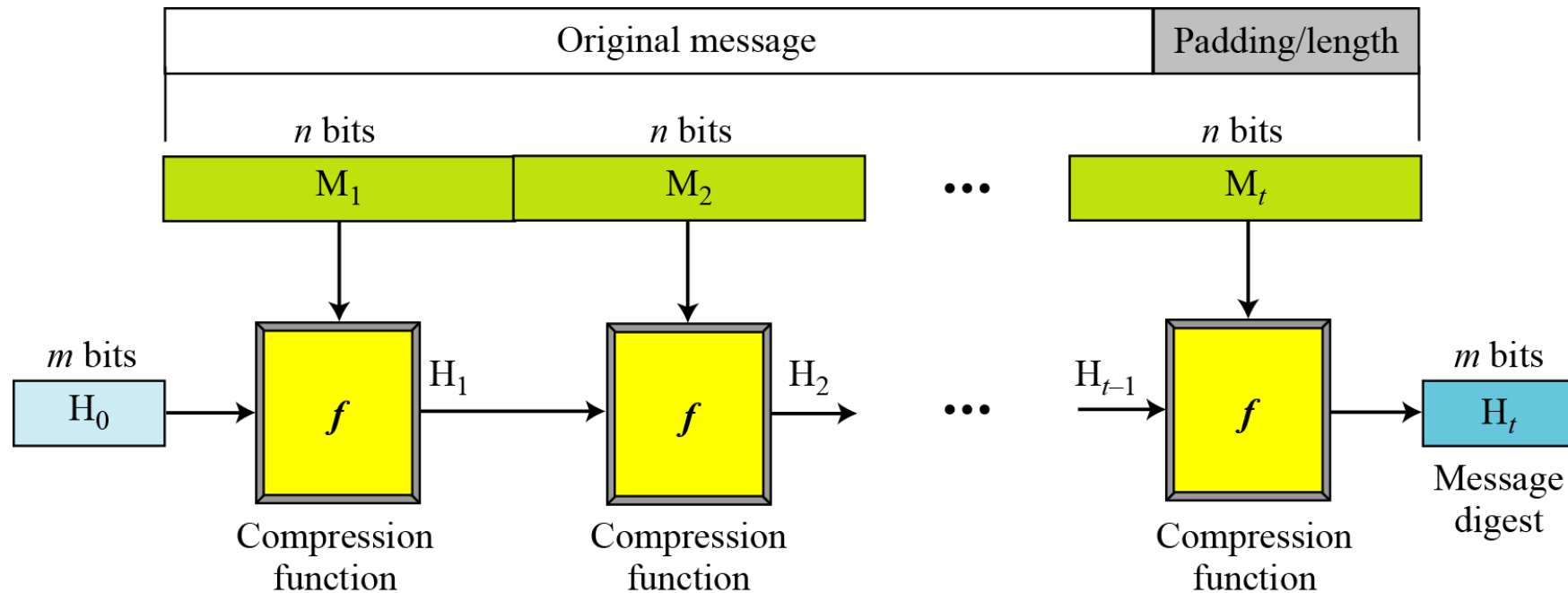
**Iterated Hash Function**

**Two Groups of Compression Functions**

# Iterated Hash Function

## Merkle-Damgard Scheme

Figure Merkle-Damgard scheme





## *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*

	<b>MD5</b>	<b>SHA-1</b>	<b>RIPEMD-160</b>
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	$\infty$	$2^{64} - 1$ bits	$2^{64} - 1$ bits
Primitive logical functions	4	4	5
Additive constants used	64	4	9
Endianness	Little-endian	Big-endian	Little-endian

<b>Algorithm</b>	<b>MBps</b>
MD5	26
SHA-1	48
RIPEND-160	31

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

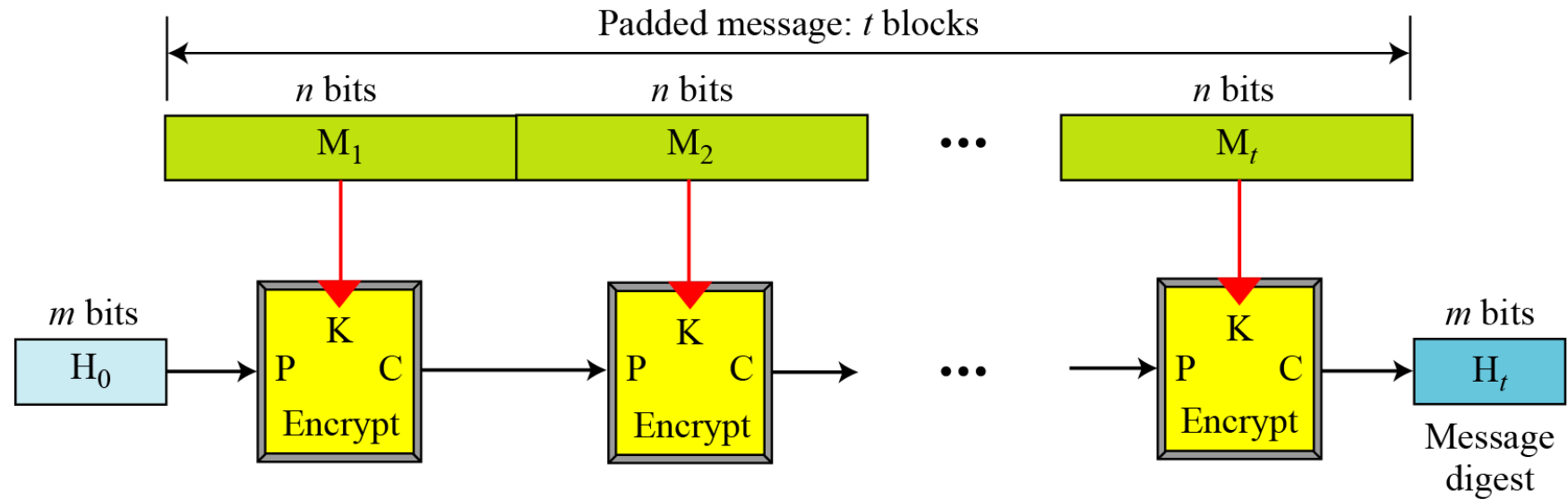


# *Continued*

<i>Characteristics</i>	<i>SHA-1</i>	<i>SHA-224</i>	<i>SHA-256</i>	<i>SHA-384</i>	<i>SHA-512</i>
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

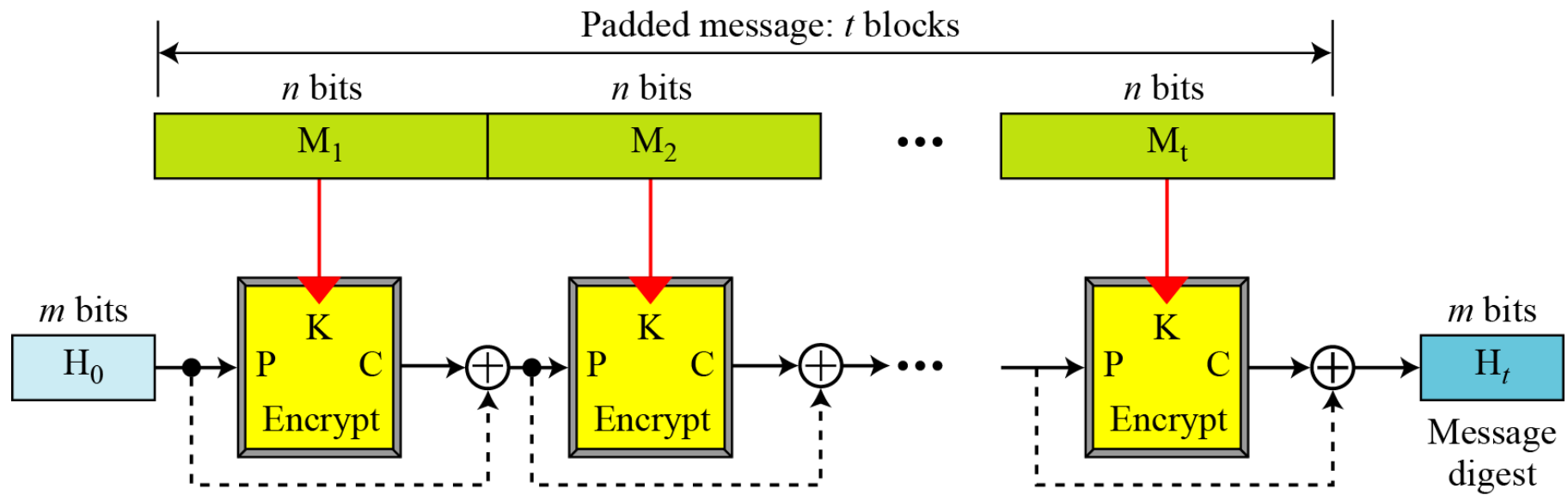
*Rabin Scheme*

**Figure 2** *Rabin scheme*



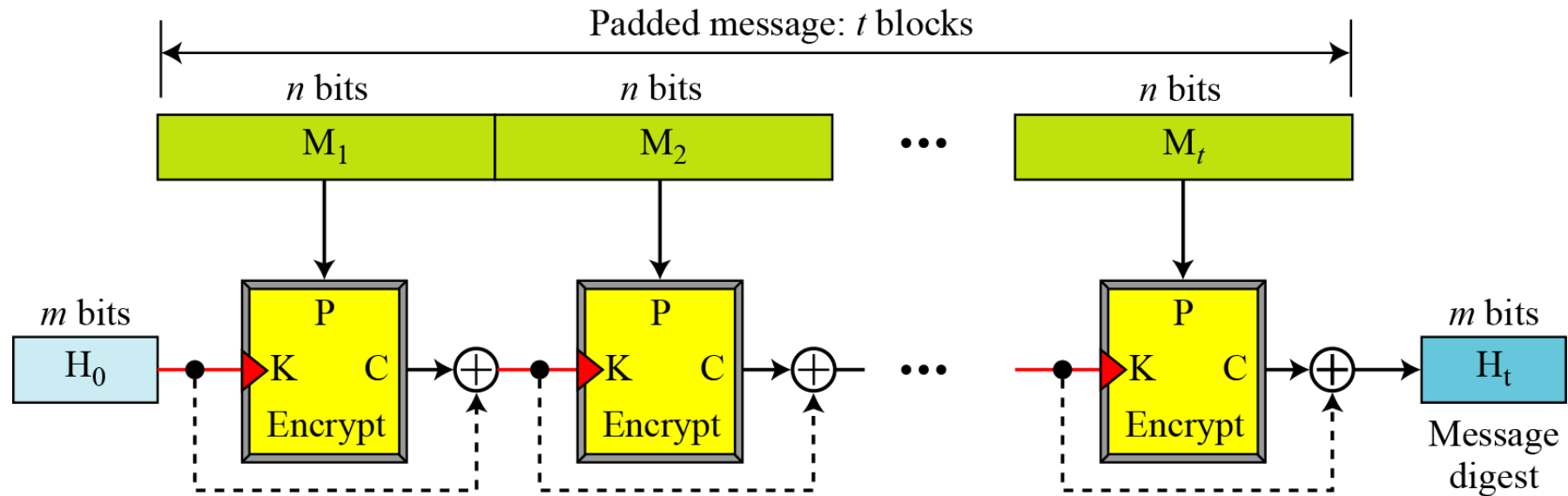
# Davies-Meyer Scheme

**Figure 3** *Davies-Meyer scheme*



## *Matyas-Meyer-Oseas Scheme*

**Figure 4** *Matyas-Meyer-Oseas scheme*

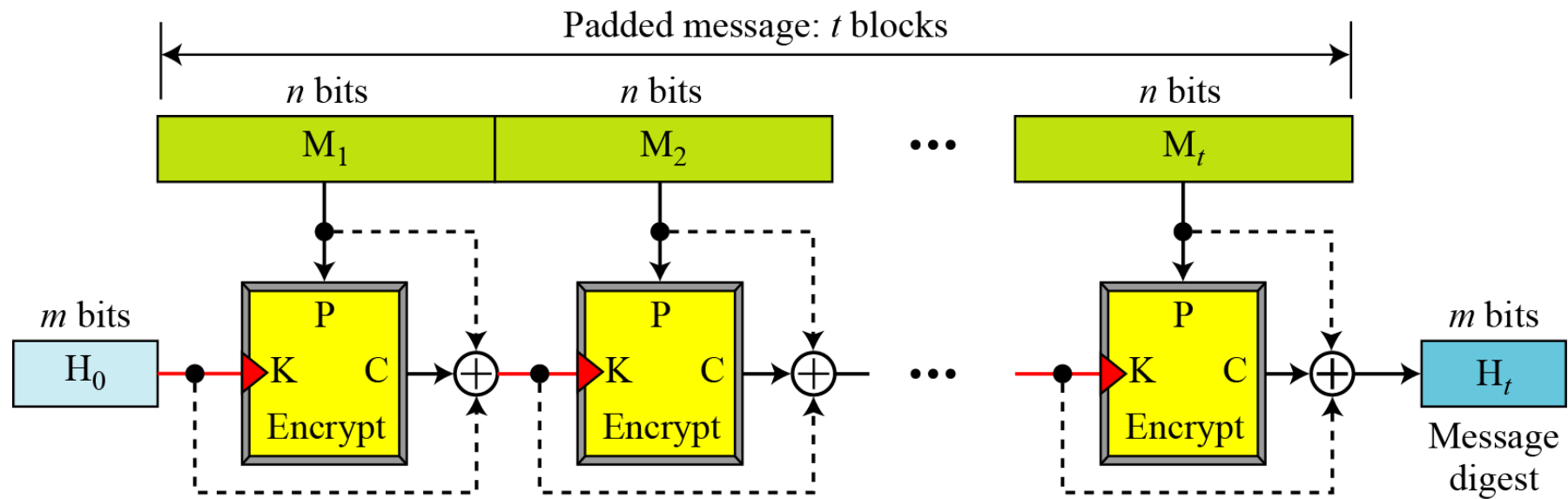




*Continued*

## *Miyaguchi-Preneel Scheme*

**Figure 5** *Miyaguchi-Preneel scheme*



# SHA-512

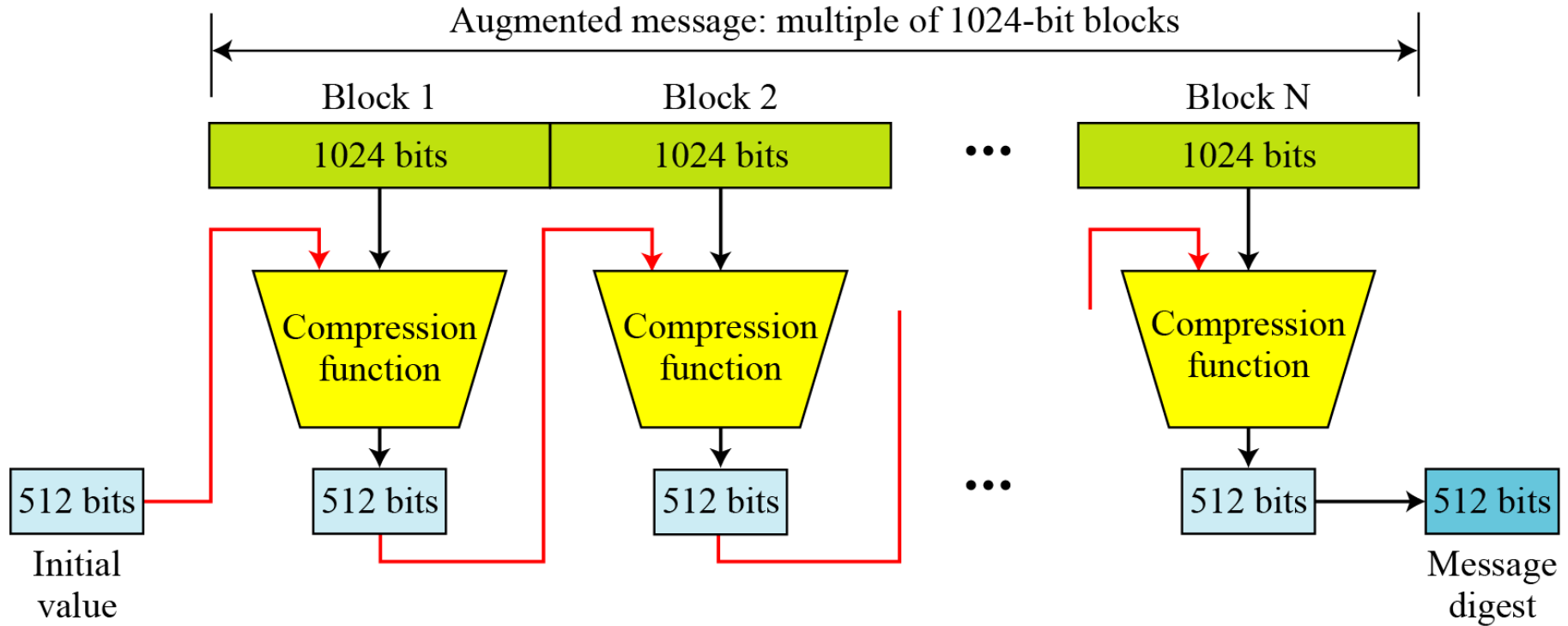
SHA-512 is the version of SHA with a 512-bit message digest. This version, like the others in the SHA family of algorithms, is based on the Merkle-Damgard scheme.

Topics discussed in this section:

- 1 Introduction**
- 2 Compression Function**
- 3 Analysis**

# Introduction

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



# 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:](#)

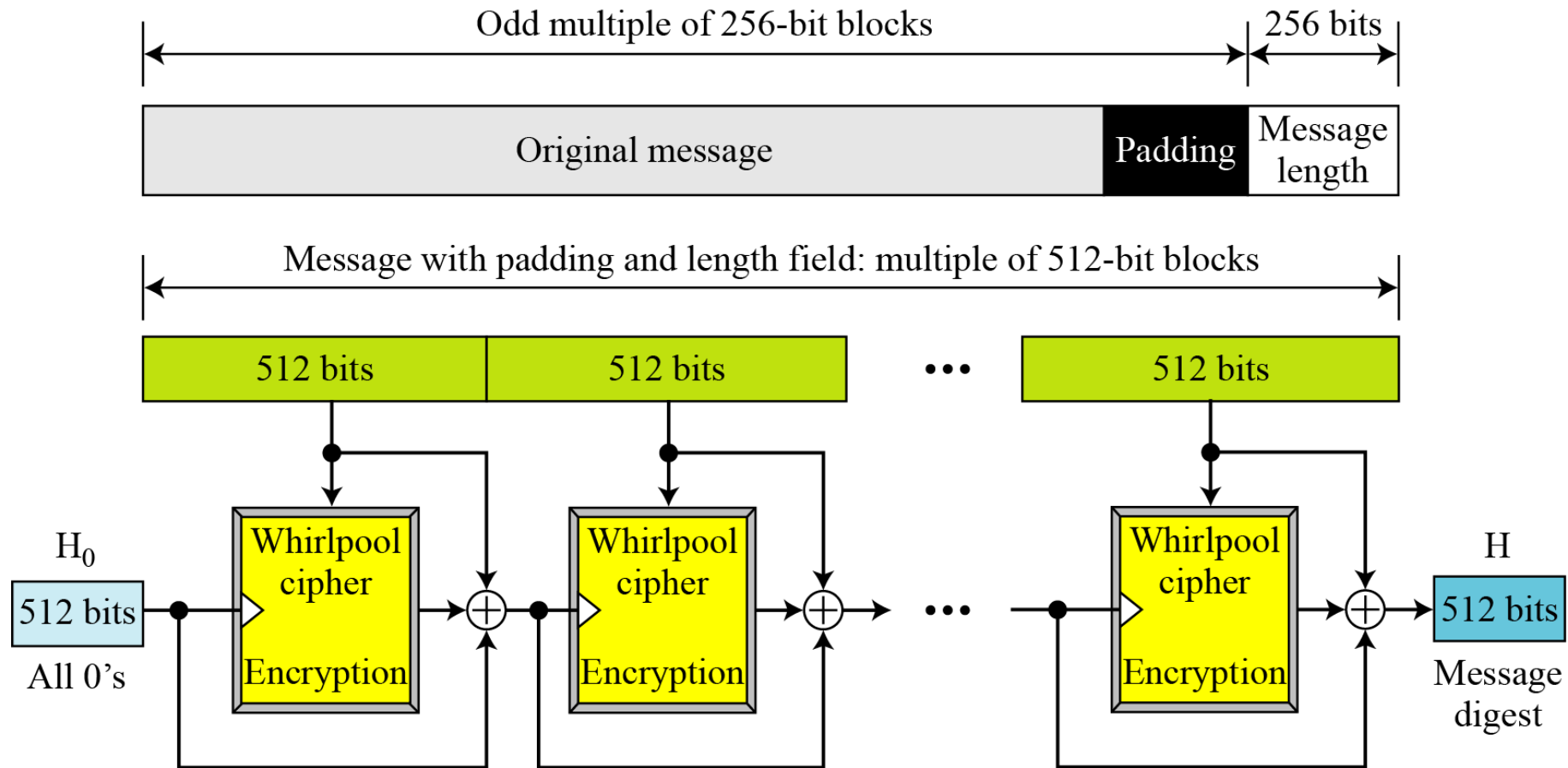
**Whirlpool Cipher**

**Summary**

**Analysis**

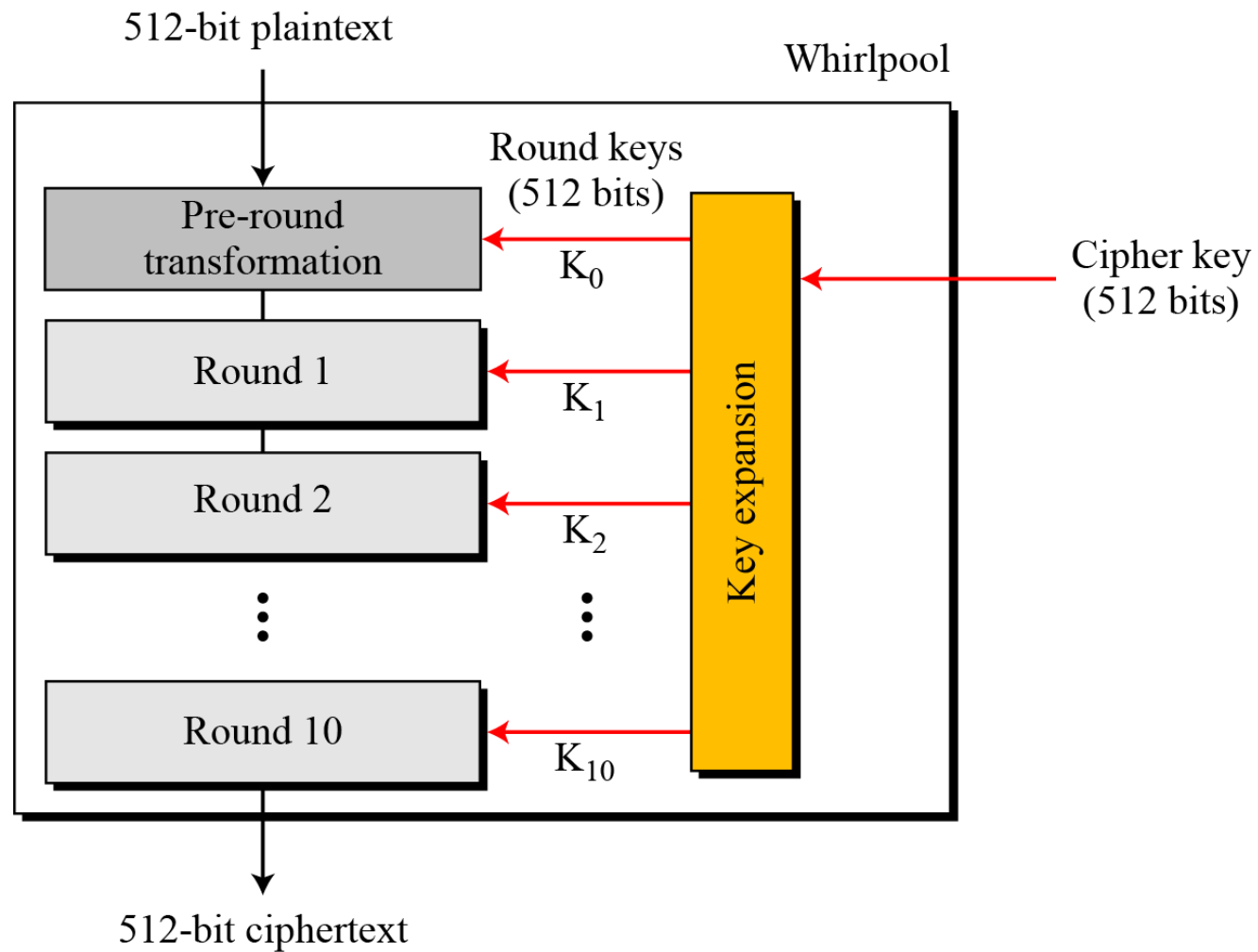
# Continued

**Figure 12** *Whirlpool hash function*



# Whirlpool Cipher

Figure 13 General idea of the Whirlpool cipher





# 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



## *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.*

# Reference and source

---

- 1. Bitcoin & Cryptocurrency Technologies: Bitcoin Mining, Blockchain Basics And Cryptocurrency Trading & Investing For Beginners | 7 Books In 1 by Boris Weiser (Author)
- 2. The Basics of Bitcoins and Blockchains: An Introduction to Cryptocurrencies and the Technology that Powers Them (Cryptography, Crypto Trading, Derivatives, Digital Assets) – Illustrated, September 15, 2018 by Antony Lewis (Author)
- 3. Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies Is Changing the World – June 12, 2018 by Don Tapscott (Author), Alex Tapscott (Author)
- 4. Blockchain Technology for IoT Applications (Blockchain Technologies) 1st ed. 2021 Edition
- by Seok-Won Lee (Editor), Irish Singh (Editor), Masoud Mohammadian (Editor)
- 5. Blockchain Basics: A Non-Technical Introduction in 25 Steps by Daniel Drescher (Author) Format
- 6. Cryptoassets: The Innovative Investor's Guide to Bitcoin and Beyond – October 19, 2017 by Chris Burniske (Author), Jack Tatar (Author)