Cryptographic Hash Functions

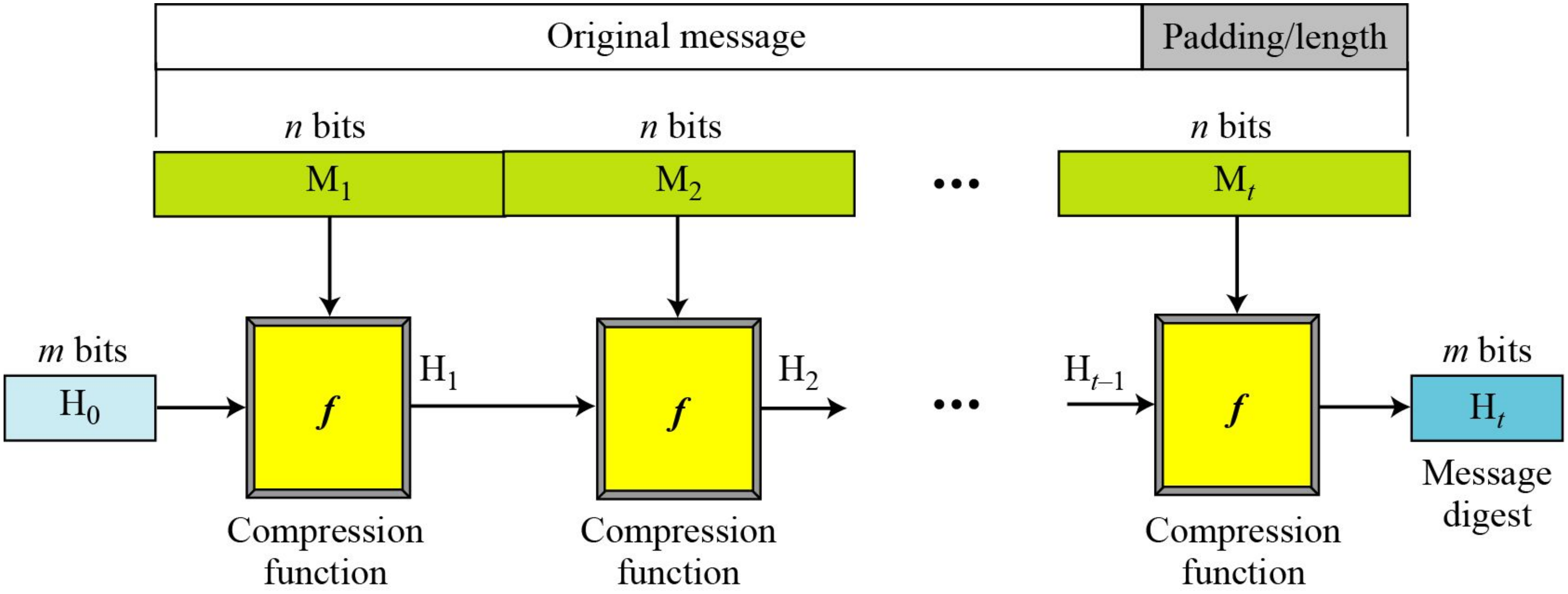
INTRODUCTION

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.

Iterated Hash Function

Merkle-Damgard Scheme

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

Characteristics of Secure Hash Algorithms

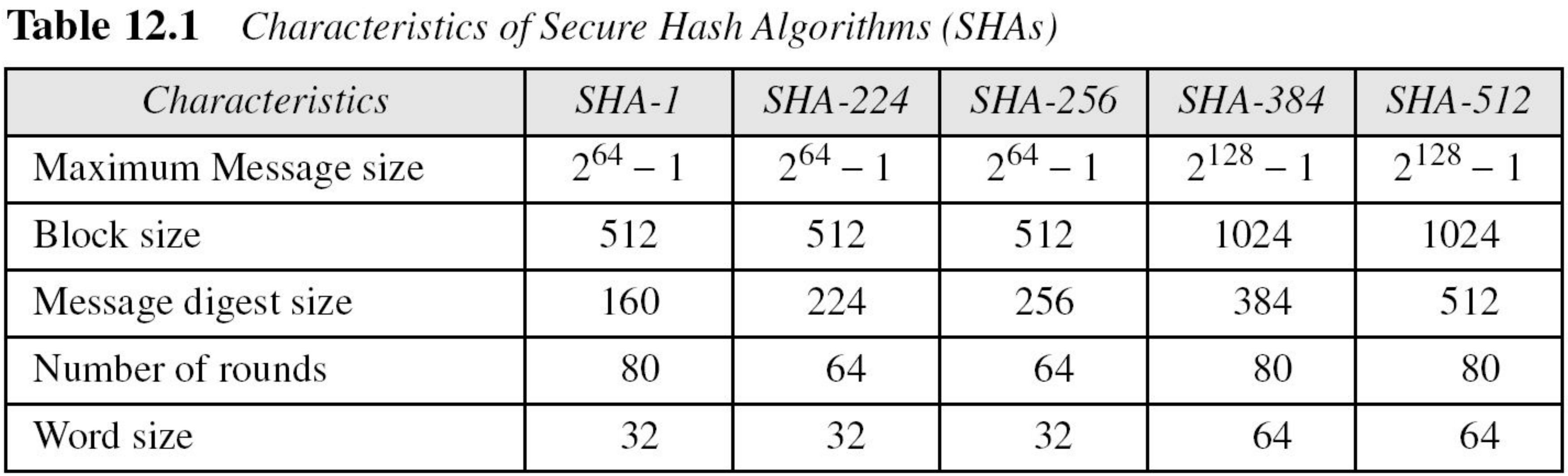


Table 12.1 *Characteristics of Secure Hash Algorithms (SHAs)*

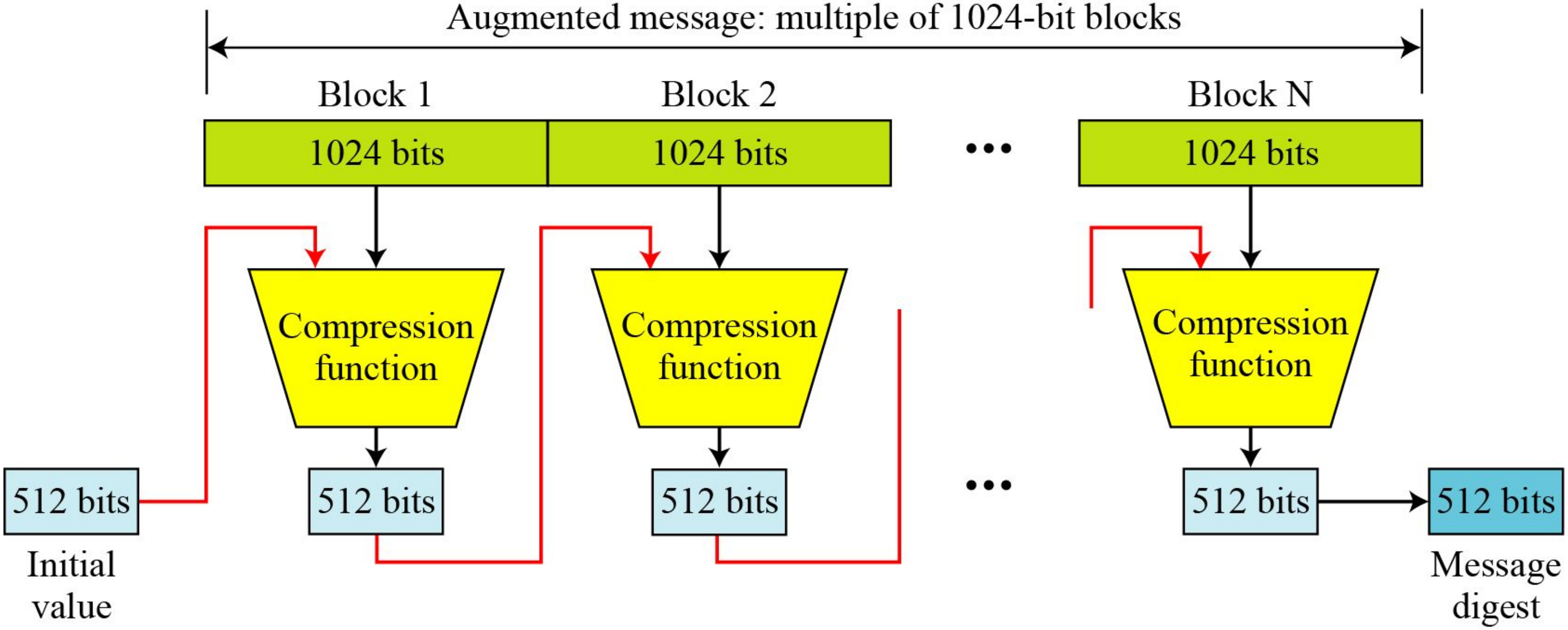
Characteristics	*SHA-1*	*SHA-224*	*SHA-256*	*SHA-384*	*SHA-512*
Maximum Message size	$2^{64} - 1$	$2^{64} - 1$	$2^{64} - 1$	$2^{128} - 1$	$2^{128} - 1$
Block size	512	512	512	1024	1024
Message digest size	160	224	256	384	512
Number of rounds	80	64	64	80	80
Word size	32	32	32	64	64

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.

Introduction

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



Continued

Message Preparation

SHA-512 insists that the length of the original message be less than 2^{128} bits.

Note

SHA-512 creates a 512-bit message digest out of a message less than 2^{128}.

Continued

Example 12.1

This example shows that the message length limitation of SHA-512 is not a serious problem. Suppose we need to send a message that is 2^{128} bits in length. How long does it take for a communications network with a data rate of 2^{64} bits per second to send this message?

Solution

A communications network that can send 2^{64} bits per second is not yet available. Even if it were, it would take many years to send this message. This tells us that we do not need to worry about the SHA-512 message length restriction.

Continued

Example 12.2

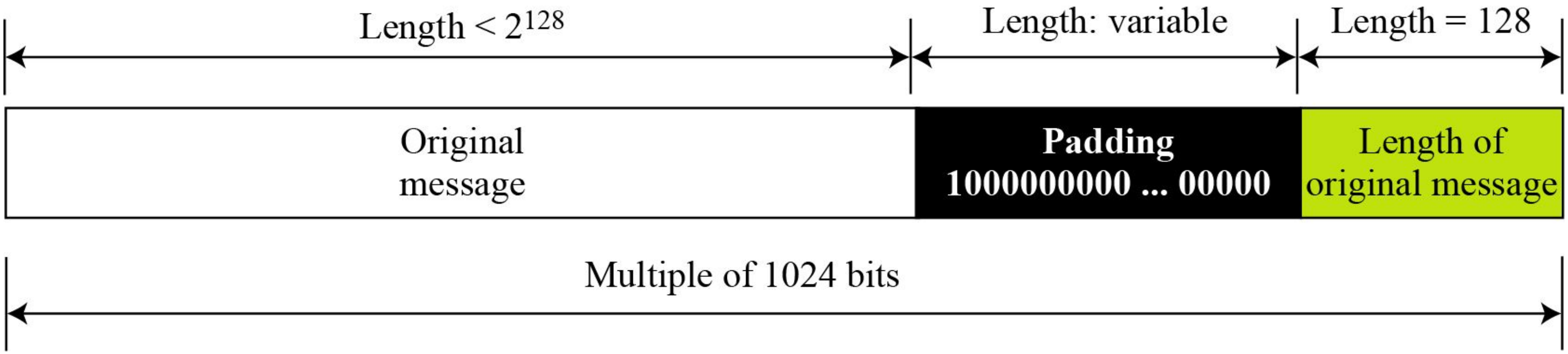
This example also concerns the message length in SHA-512. How many pages are occupied by a message of 2^{128} bits?

Solution

Suppose that a character is 32, or 2^6, bits. Each page is less than 2048, or approximately 2^{12}, characters. So 2^{128} bits need at least 2^{128} / 2^{18}, or 2^{110}, pages. This again shows that we need not worry about the message length restriction.

Continued

Figure 12.7 ***Padding and length field in SHA-512***



Continued

Example 12.3

What is the number of padding bits if the length of the original message is 2590 bits?

Solution

We can calculate the number of padding bits as follows:

$$|P| = (-\,2590 - 128) \bmod 1024 = -2718 \bmod 1024 = 354$$

The padding consists of one 1 followed by 353 0's.

Continued

Example 12.4

Do we need padding if the length of the original message is already a multiple of 1024 bits?

Solution

Yes we do, because we need to add the length field. So padding is needed to make the new block a multiple of 1024 bits.

Continued

Example 12.5

What is the minimum and maximum number of padding bits that can be added to a message?

Solution

a. **The minimum length of padding is 0 and it happens when (−M − 128) mod 1024 is 0. This means that |M| = −128 mod 1024 = 896 mod 1024 bits. In other words, the last block in the original message is 896 bits. We add a 128-bit length field to make the block complete.**

Continued

Example 12.5 *Continued*

b) The maximum length of padding is 1023 and it happens when (−|M| −128) = 1023 mod 1024. This means that the length of the original message is |M| = (−128 −1023) mod 1024 or the length is |M| = 897 mod 1024. In this case, we cannot just add the length field because the length of the last block exceeds one bit more than 1024. So we need to add 897 bits to complete this block and create a second block of 896 bits. Now the length can be added to make this block complete.