Information & System Security

Lecture 32

VIT-AP
UNIVERSITY

Cryptographic Hash Functions

List of some Hash functions

The usual (non-cryptographic) hash functions:

- Summing (SUM8, SUM16, SUM24, SUM32, XOR8)
- CRC series (CRC16, CRC32, CRC64)

The cryptographic (secure) hash functions:

- MD series (MD2, MD4, MD5)
- SHA series (SHA, SHA-1, SHA-224, SHA-256, SHA-384, SHA-512)
- RIPEMD series (RIPEMD-128, RIPEMD-160, RIPEMD-320)
- HAVAL
- Tiger

12-1 INTRODUCTION

- *A cryptographic hash function takes a **message** of **arbitrary** length and creates a **message digest** of **fixed** length.*

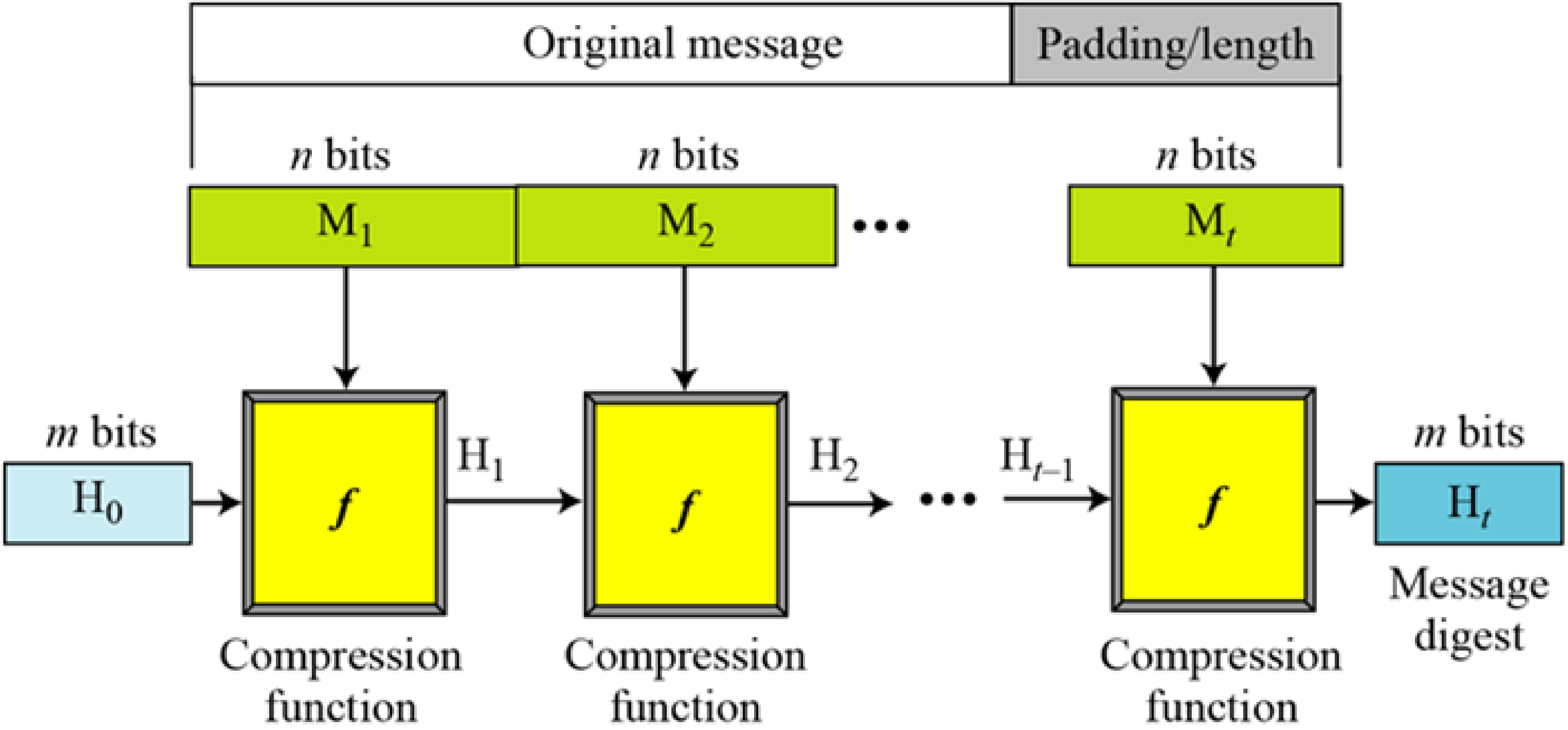
- *The ultimate goal of this chapter is to discuss the details of the two most promising cryptographic hash algorithms— **Whirlpool** and **SHA-512**.*

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



12.1.2 Two Groups of Compression Functions

1. The compression function is made from scratch.

Message Digest (MD), Secure Hash Algorithm (SHA)

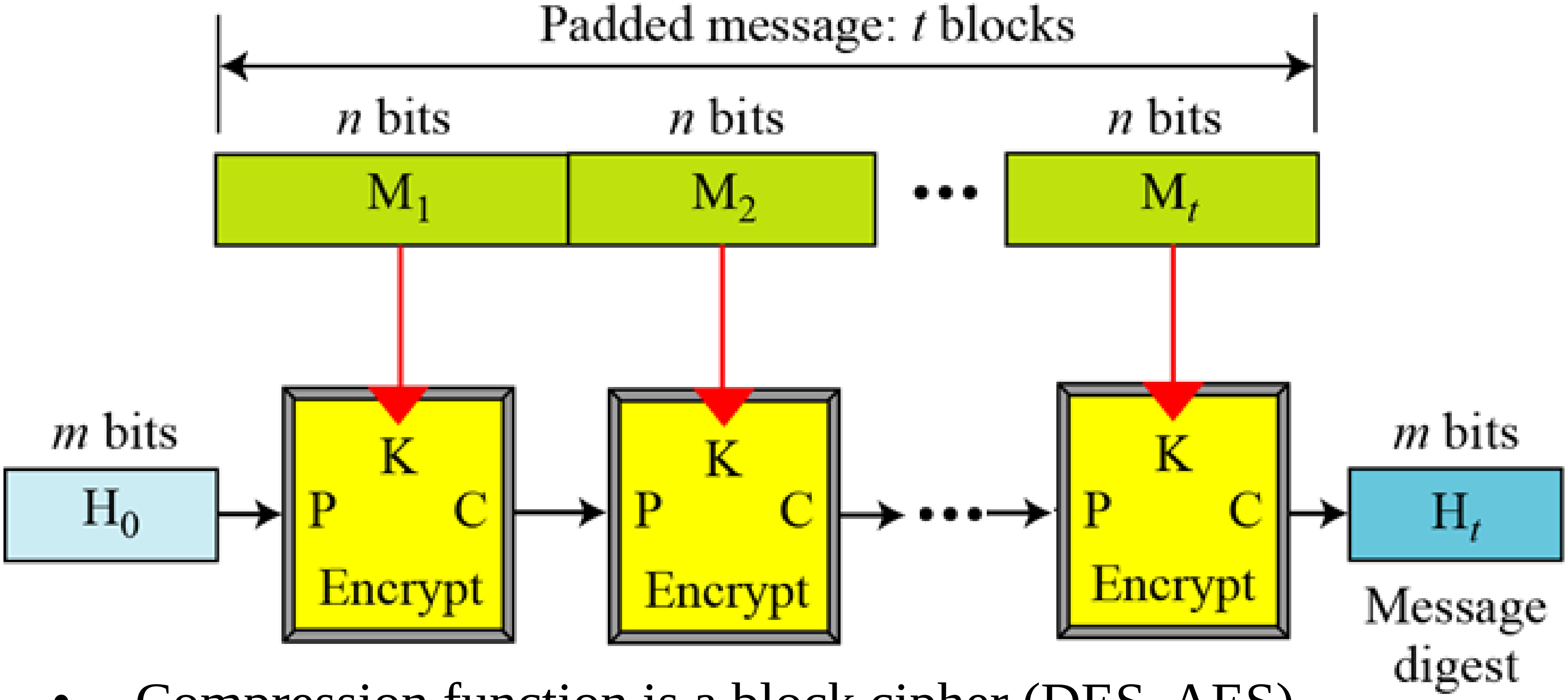
2. A symmetric-key block cipher serves as a compression function.

Whirlpool

12.1.2 Continued

Rabin Scheme

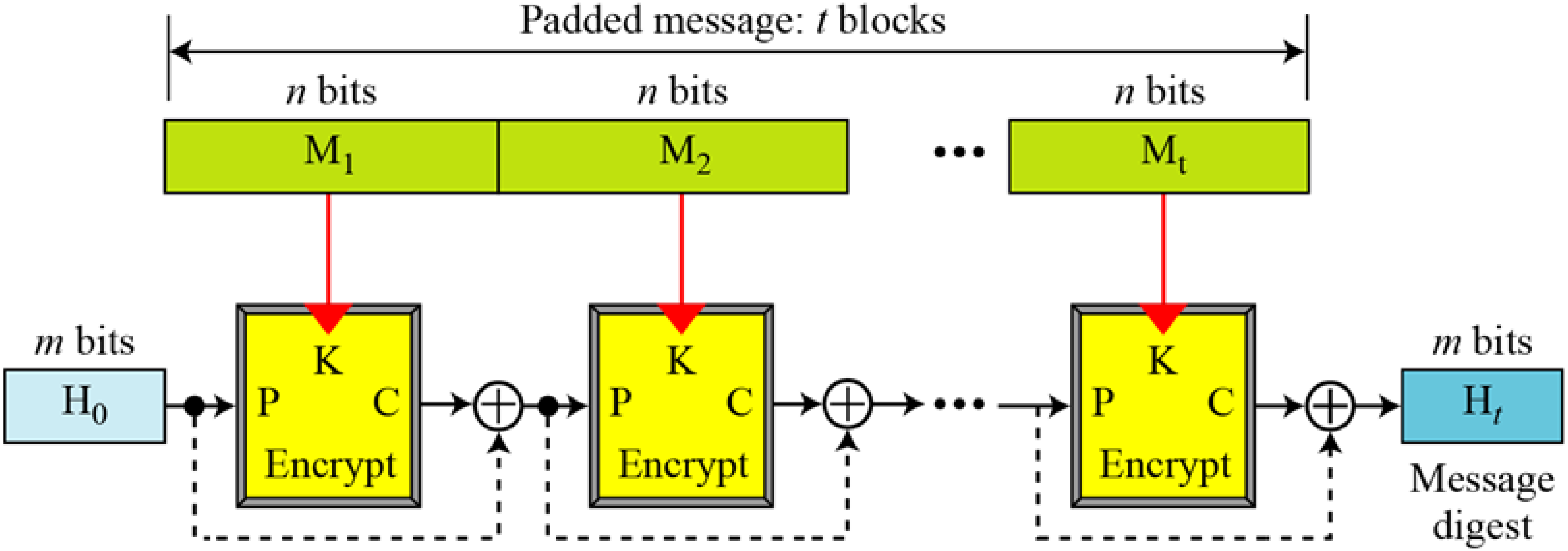
- Based on Merkle-Damgard scheme



- Compression function is a block cipher (DES, AES)
- Key is *n*-bits block of data
- Plaintext is the previous Ciphertext (message digest).
- Size of the message digest is the size of plaintext of the cipher.

12.1.2 Continued

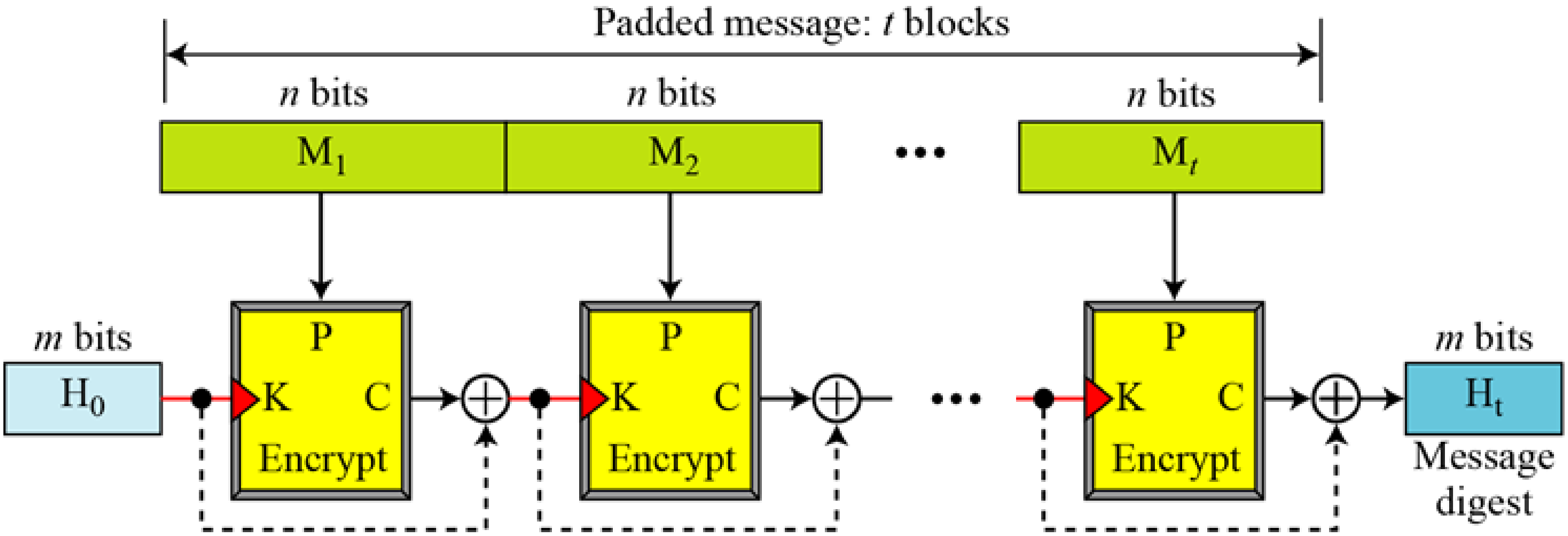
Davies-Meyer Scheme



- Same as Rabin scheme except that it uses forward feed to protect against meet-in-the-middle attack.

12.1.2 Continued

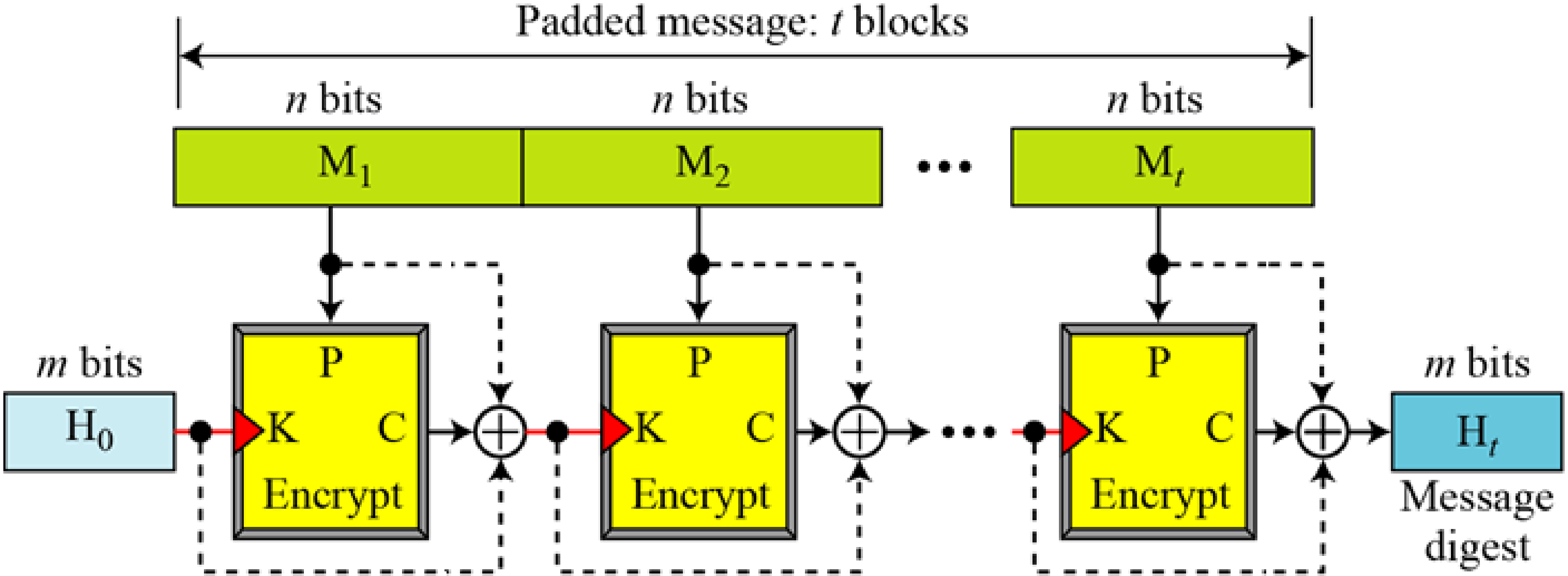
Matyas-Meyer-Oseas Scheme



- Is a dual version of the Davies-Meyer scheme: the message block is used as the key to the cryptosystem.
- Used when size of data block and the key are of same size.

12.1.2 Continued

Miyaguchi-Preneel Scheme



- Is an extended version of the Matyas-Meyer-Oseas scheme.
- The plaintext, ciphertext, and the key are all ex-ored to create the new digest.
- Used in Whirlpool hash function.

12-2 WHIRLPOOL

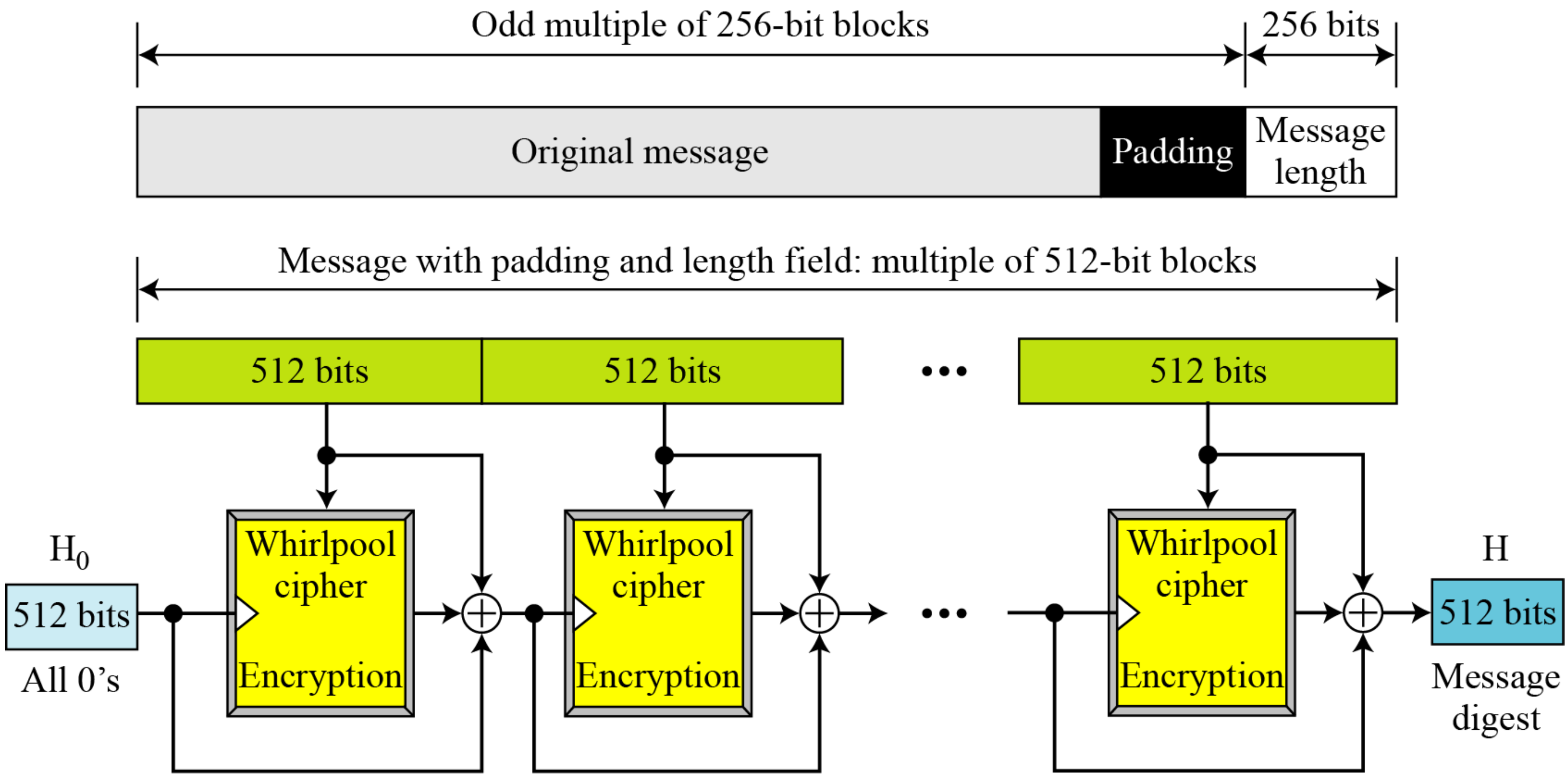
- *Whirlpool is an iterated cryptographic hash function, based on the Miyaguchi-Preneel scheme, that uses a symmetric-key block cipher in place of the compression function.*

- *The block cipher is a modified AES cipher that has been tailored for this purpose.*

Topics discussed in this section:

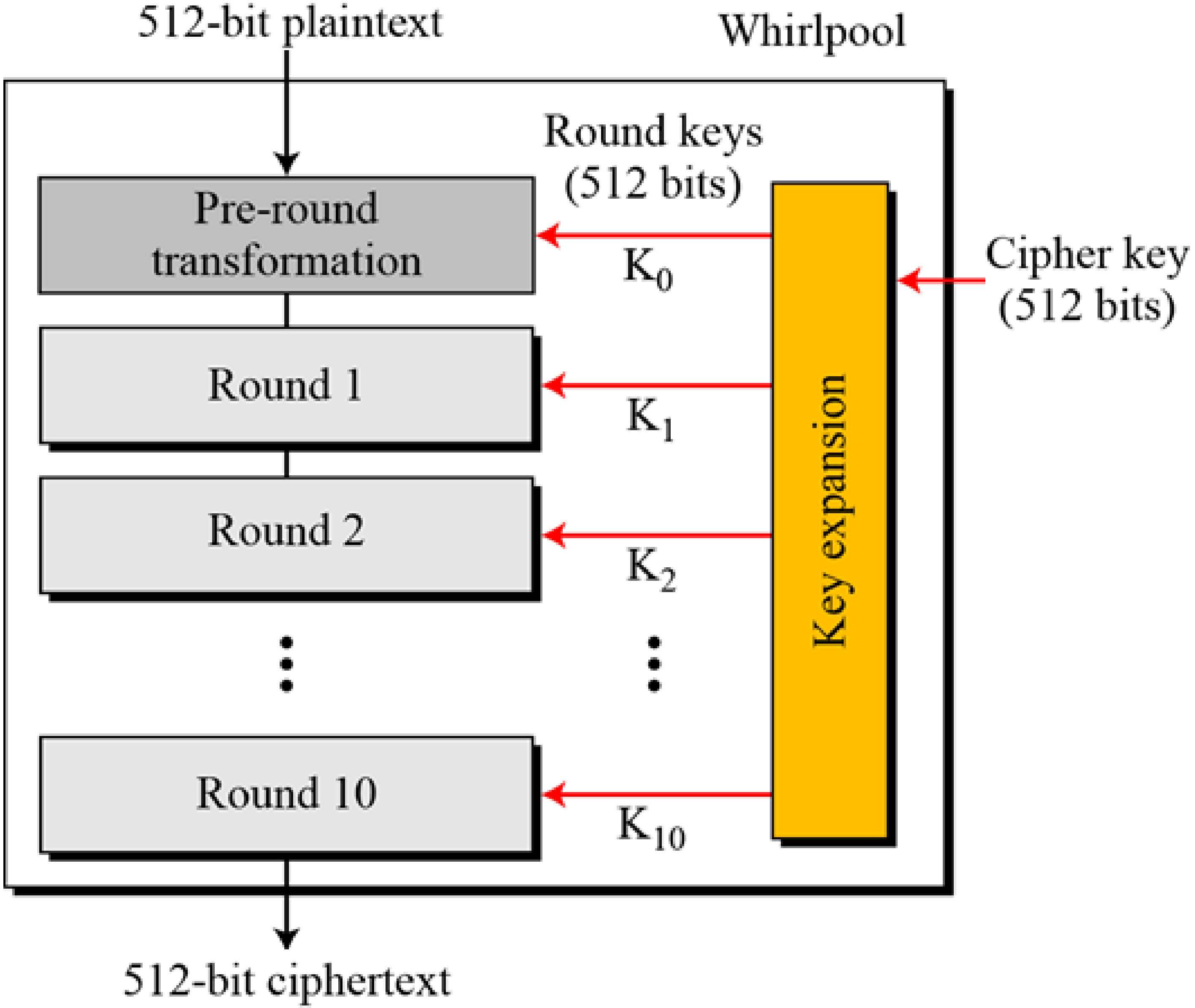
12.2.1 Whirlpool Cipher
12.2.2 Summary
12.2.3 Analysis

12-2 Continued



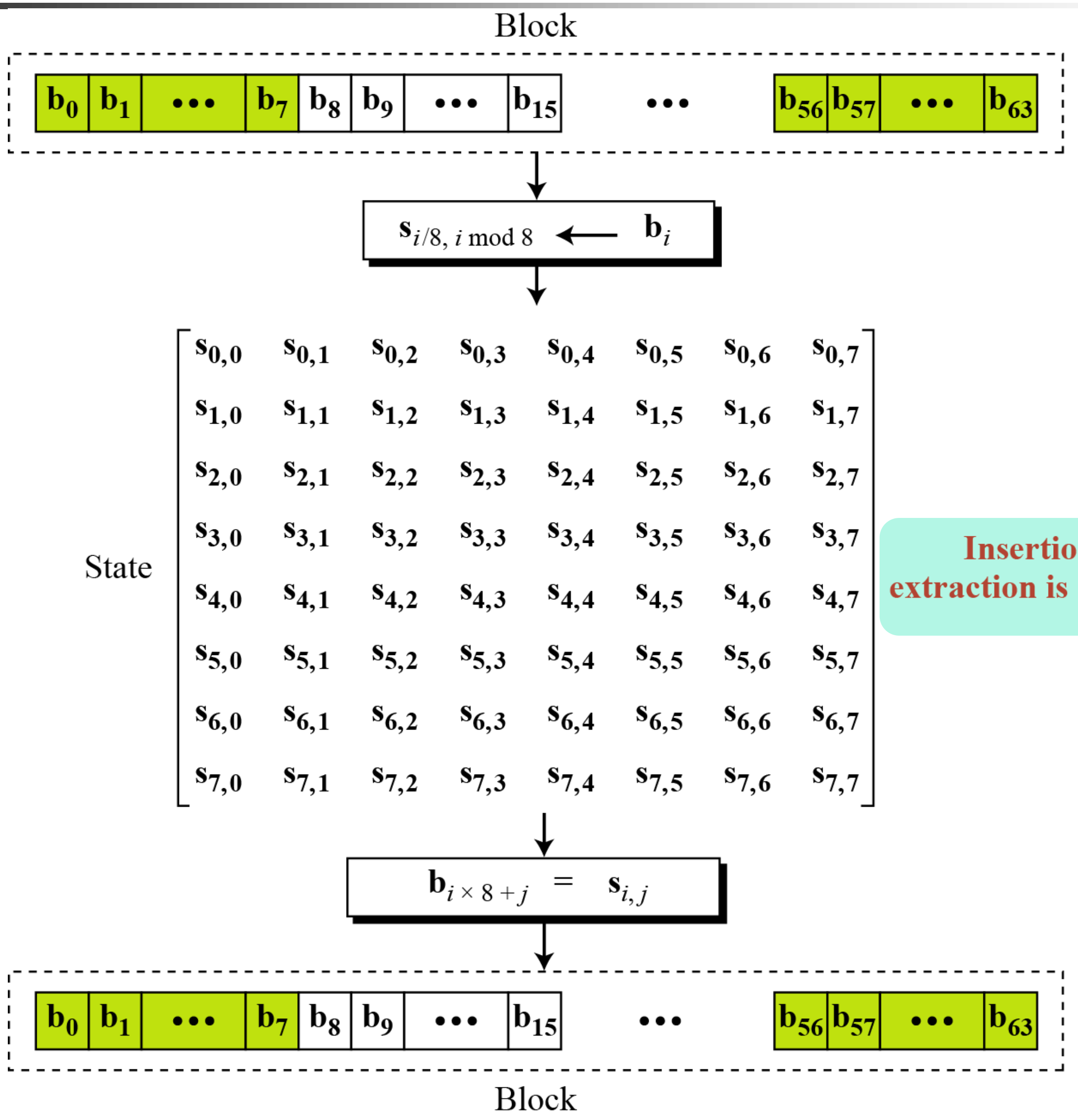
Whirlpool hash function

12.2.1 Whirlpool Cipher



General idea of the Whirlpool cipher

12.2.1 Continued


Block
b0 b1 ••• b7 b8 b9 ••• b15 ••• b56 b57 ••• b63
$s_{i/8,\ i \bmod 8} \leftarrow b_i$
State
$b_{i \times 8 + j} = s_{i,j}$
b0 b1 ••• b7 b8 b9 ••• b15 ••• b56 b57 ••• b63
Block

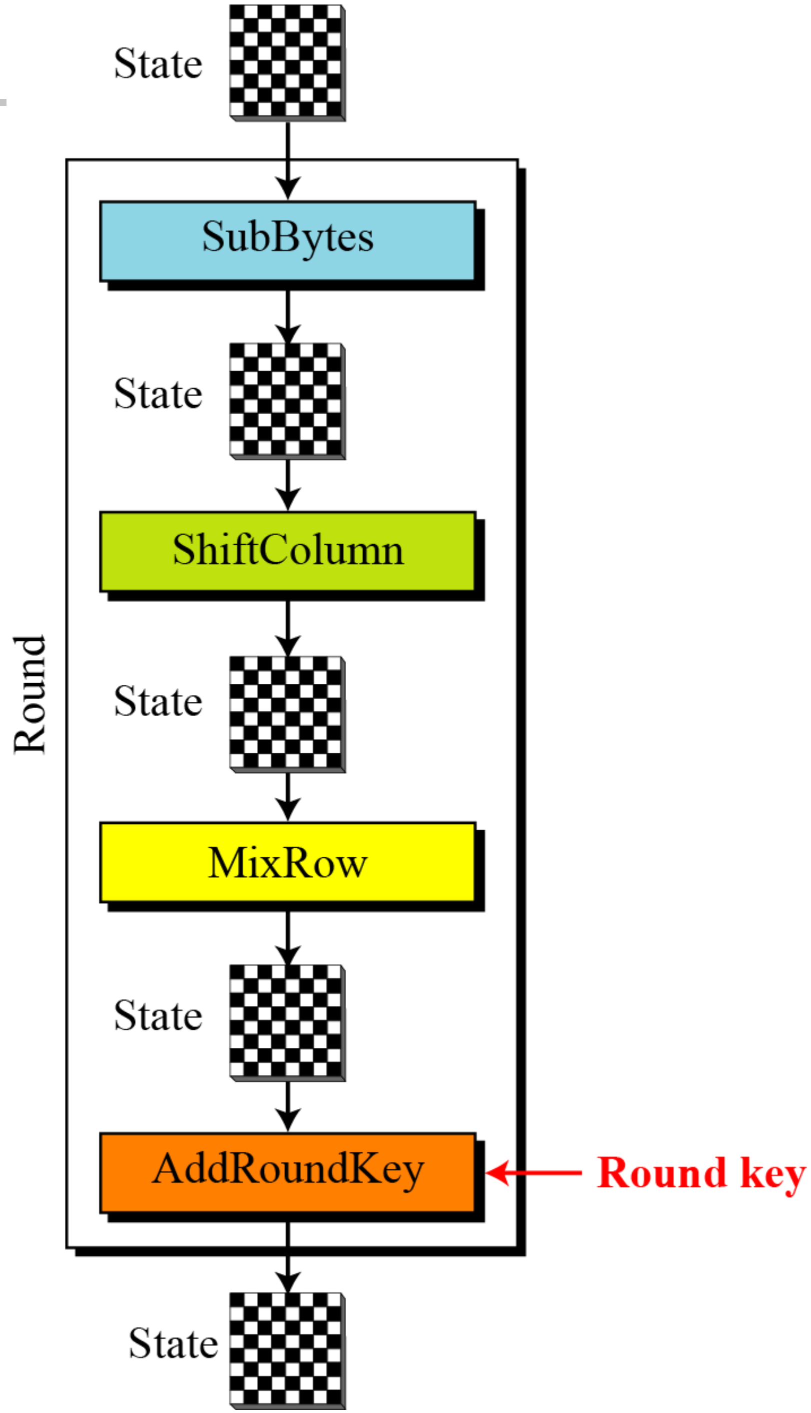
$$\begin{bmatrix} s_{0,0} & s_{0,1} & s_{0,2} & s_{0,3} & s_{0,4} & s_{0,5} & s_{0,6} & s_{0,7} \\ s_{1,0} & s_{1,1} & s_{1,2} & s_{1,3} & s_{1,4} & s_{1,5} & s_{1,6} & s_{1,7} \\ s_{2,0} & s_{2,1} & s_{2,2} & s_{2,3} & s_{2,4} & s_{2,5} & s_{2,6} & s_{2,7} \\ s_{3,0} & s_{3,1} & s_{3,2} & s_{3,3} & s_{3,4} & s_{3,5} & s_{3,6} & s_{3,7} \\ s_{4,0} & s_{4,1} & s_{4,2} & s_{4,3} & s_{4,4} & s_{4,5} & s_{4,6} & s_{4,7} \\ s_{5,0} & s_{5,1} & s_{5,2} & s_{5,3} & s_{5,4} & s_{5,5} & s_{5,6} & s_{5,7} \\ s_{6,0} & s_{6,1} & s_{6,2} & s_{6,3} & s_{6,4} & s_{6,5} & s_{6,6} & s_{6,7} \\ s_{7,0} & s_{7,1} & s_{7,2} & s_{7,3} & s_{7,4} & s_{7,5} & s_{7,6} & s_{7,7} \end{bmatrix}$$

Insertion and extraction is row by row

Block and state in the Whirlpool cipher

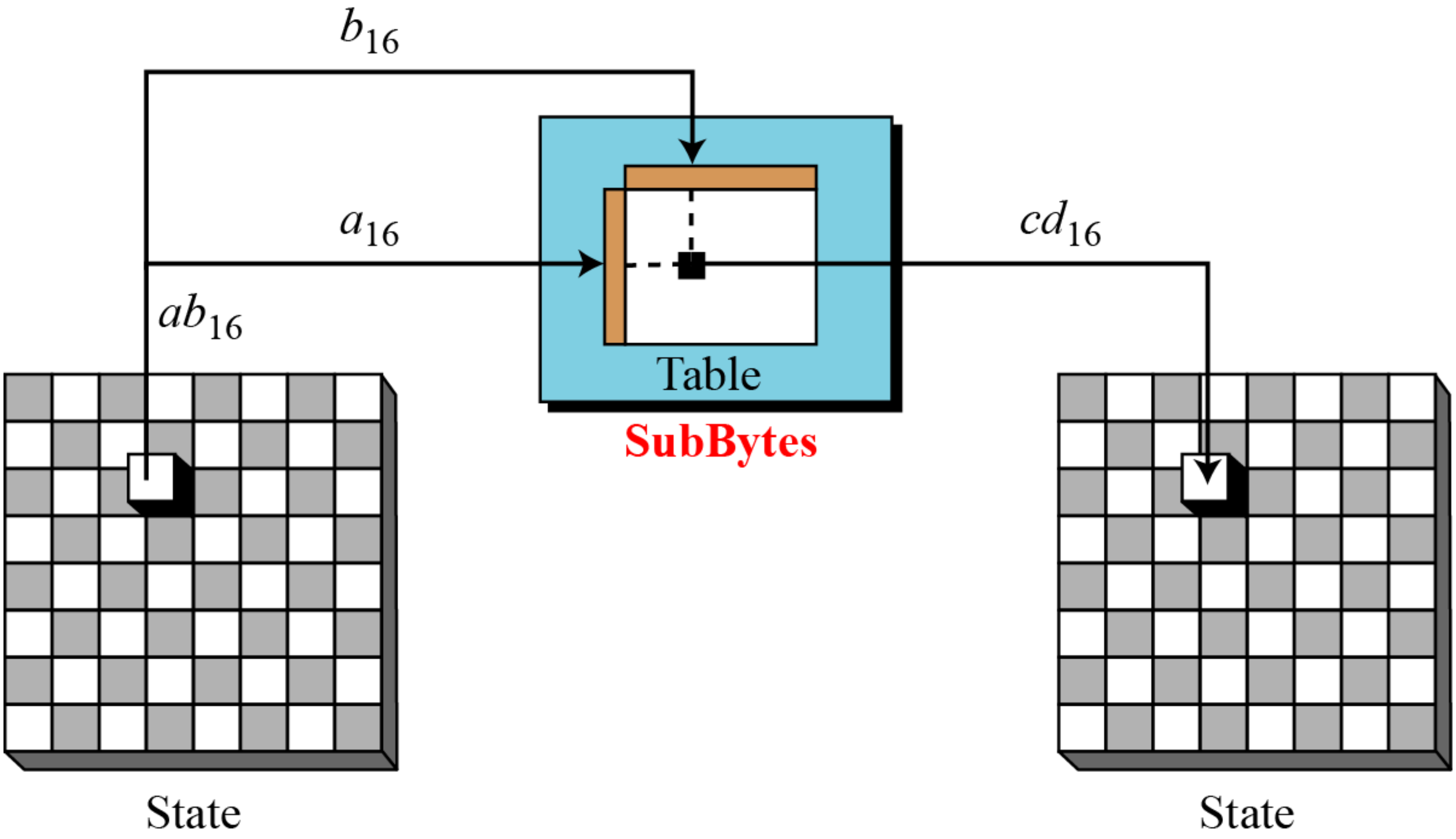
12.2.1 Continued

Structure of Each Round in the Whirlpool cipher uses four transformations.



12.2.1 Continued

SubBytes ***Like in AES, SubBytes provide a nonlinear transformation.***



SubBytes transformations in the Whirlpool cipher

12.2.1 Continued

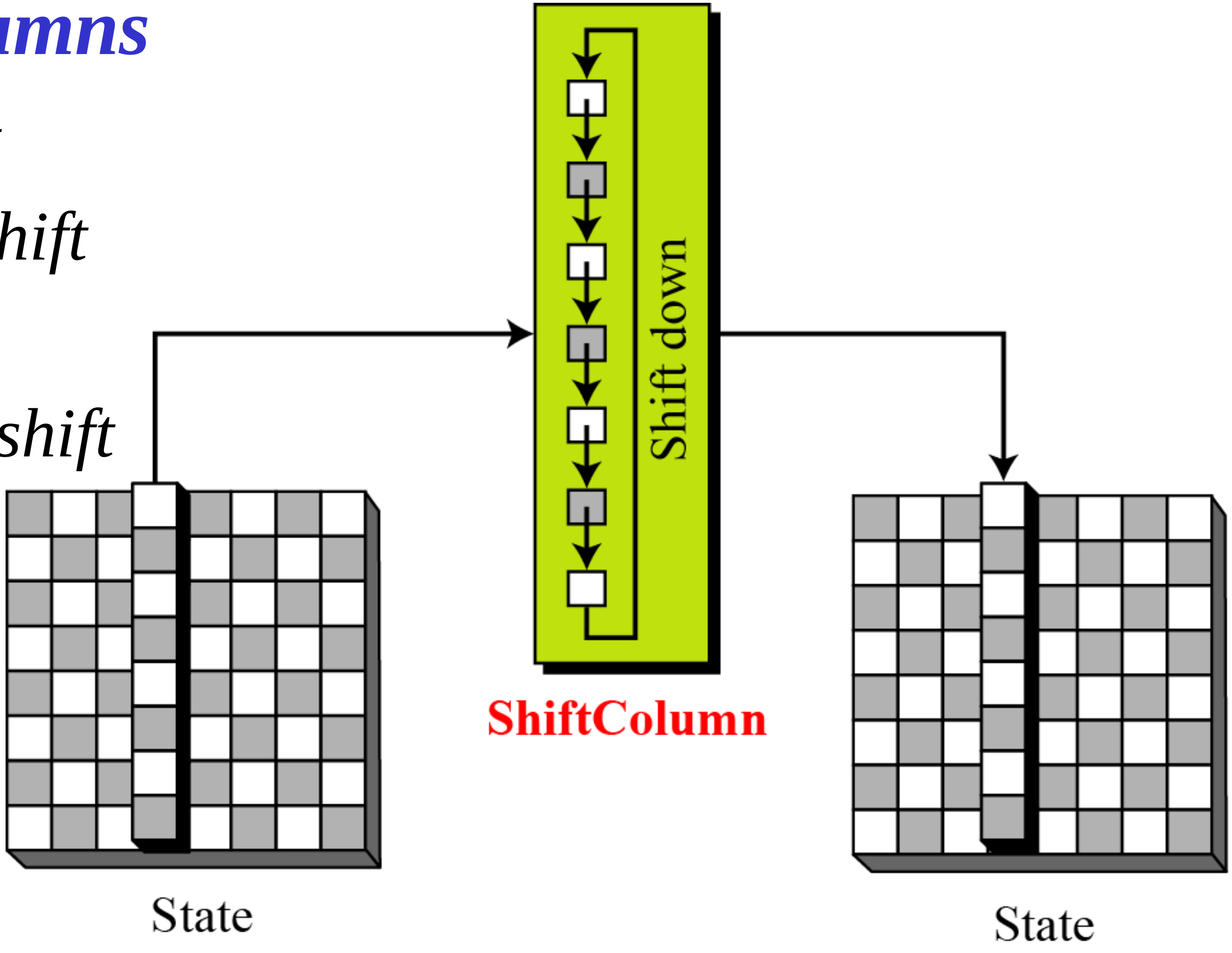
SubBytes transformation table (S-Box)

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	18	23	C6	E8	87	B8	01	4F	36	A6	D2	F5	79	6F	91	52
1	16	BC	9B	8E	A3	0C	7B	35	1D	E0	D7	C2	2E	4B	FE	57
2	15	77	37	E5	9F	F0	4A	CA	58	C9	29	0A	B1	A0	6B	85
3	BD	5D	10	F4	CB	3E	05	67	E4	27	41	8B	A7	7D	95	C8
4	FB	EF	7C	66	DD	17	47	9E	CA	2D	BF	07	AD	5A	83	33
5	63	02	AA	71	C8	19	49	C9	F2	E3	5B	88	9A	26	32	B0
6	E9	0F	D5	80	BE	CD	34	48	FF	7A	90	5F	20	68	1A	AE
7	B4	54	93	22	64	F1	73	12	40	08	C3	EC	DB	A1	8D	3D
8	97	00	CF	2B	76	82	D6	1B	B5	AF	6A	50	45	F3	30	EF
9	3F	55	A2	EA	65	BA	2F	C0	DE	1C	FD	4D	92	75	06	8A
A	B2	E6	0E	1F	62	D4	A8	96	F9	C5	25	59	84	72	39	4C
B	5E	78	38	8C	C1	A5	E2	61	B3	21	9C	1E	43	C7	FC	04
C	51	99	6D	0D	FA	DF	7E	24	3B	AB	CE	11	8F	4E	B7	EB
D	3C	81	94	F7	9B	13	2C	D3	E7	6E	C4	03	56	44	7E	A9
E	2A	BB	C1	53	DC	0B	9D	6C	31	74	F6	46	AC	89	14	E1
F	16	3A	69	09	70	B6	C0	ED	CC	42	98	A4	28	5C	F8	86

12.1.1 Continued

ShiftColumns

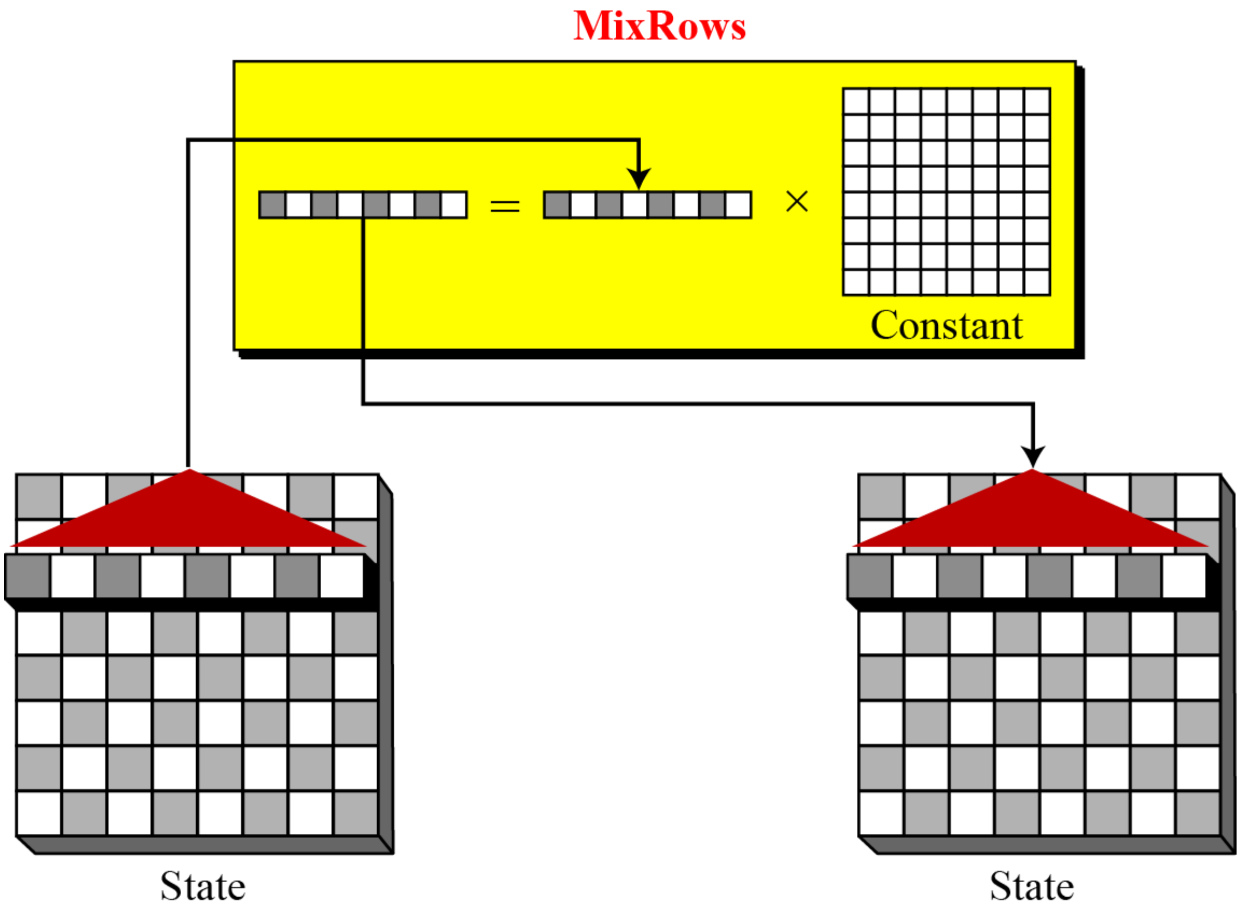
- *Col 0- No shift*
- *Col 1- 1 byte shift*
- …
- *Col 7- 7 bytes shift*



ShiftColumns transformation in the Whirlpool cipher

12.1.1 Continued

MixRows



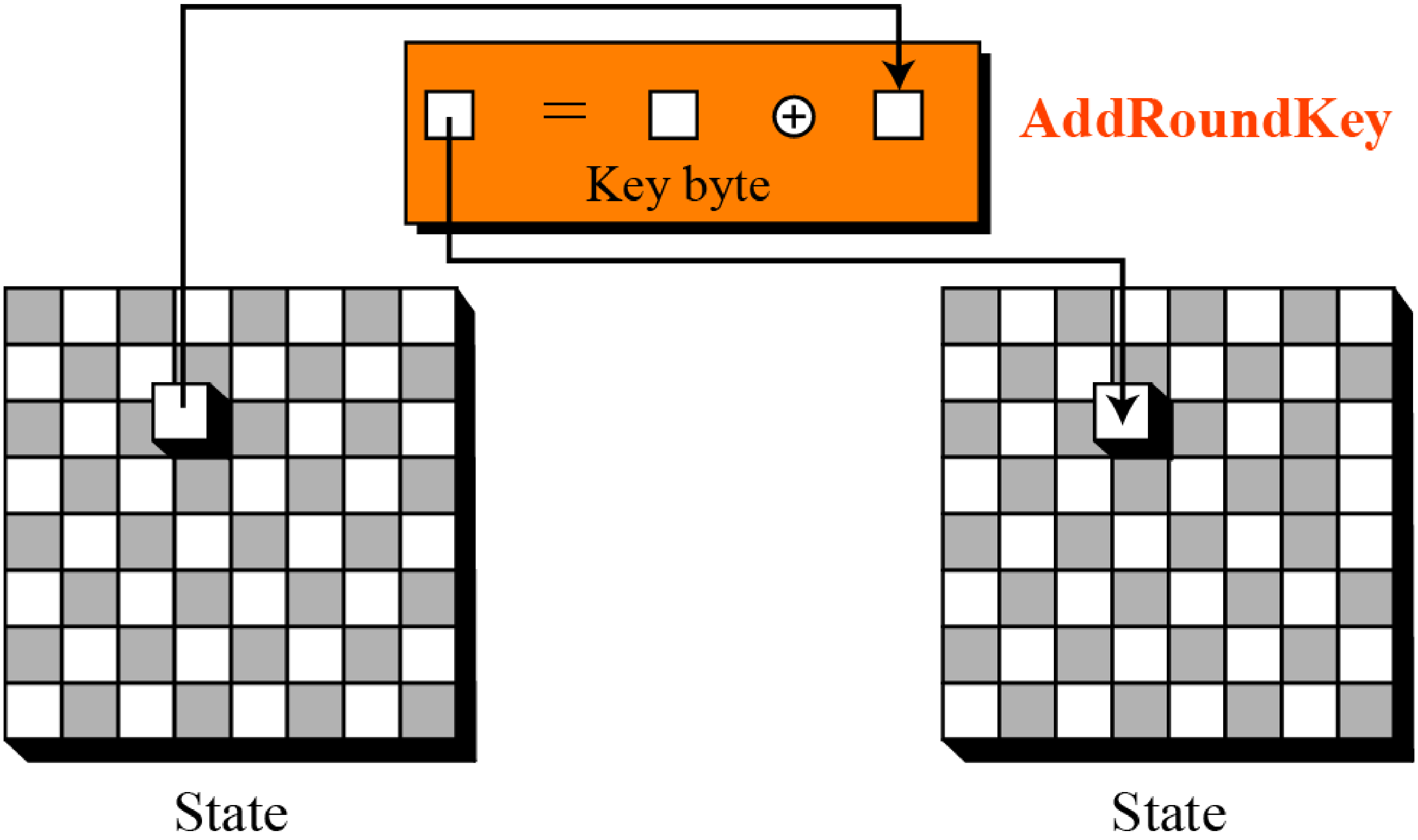
$$\begin{bmatrix} 01 & 01 & 04 & 01 & 08 & 05 & 02 & 09 \\ 09 & 01 & 01 & 04 & 01 & 08 & 05 & 02 \\ 02 & 09 & 01 & 01 & 04 & 01 & 08 & 05 \\ 05 & 02 & 09 & 01 & 01 & 04 & 01 & 08 \\ 08 & 05 & 02 & 09 & 01 & 01 & 04 & 01 \\ 01 & 08 & 05 & 02 & 09 & 01 & 01 & 04 \\ 04 & 01 & 08 & 05 & 02 & 09 & 01 & 01 \\ 01 & 04 & 01 & 08 & 05 & 02 & 09 & 01 \end{bmatrix}$$

Constant matrix

MixRows transformation in the Whirlpool cipher

12.1.1 Continued

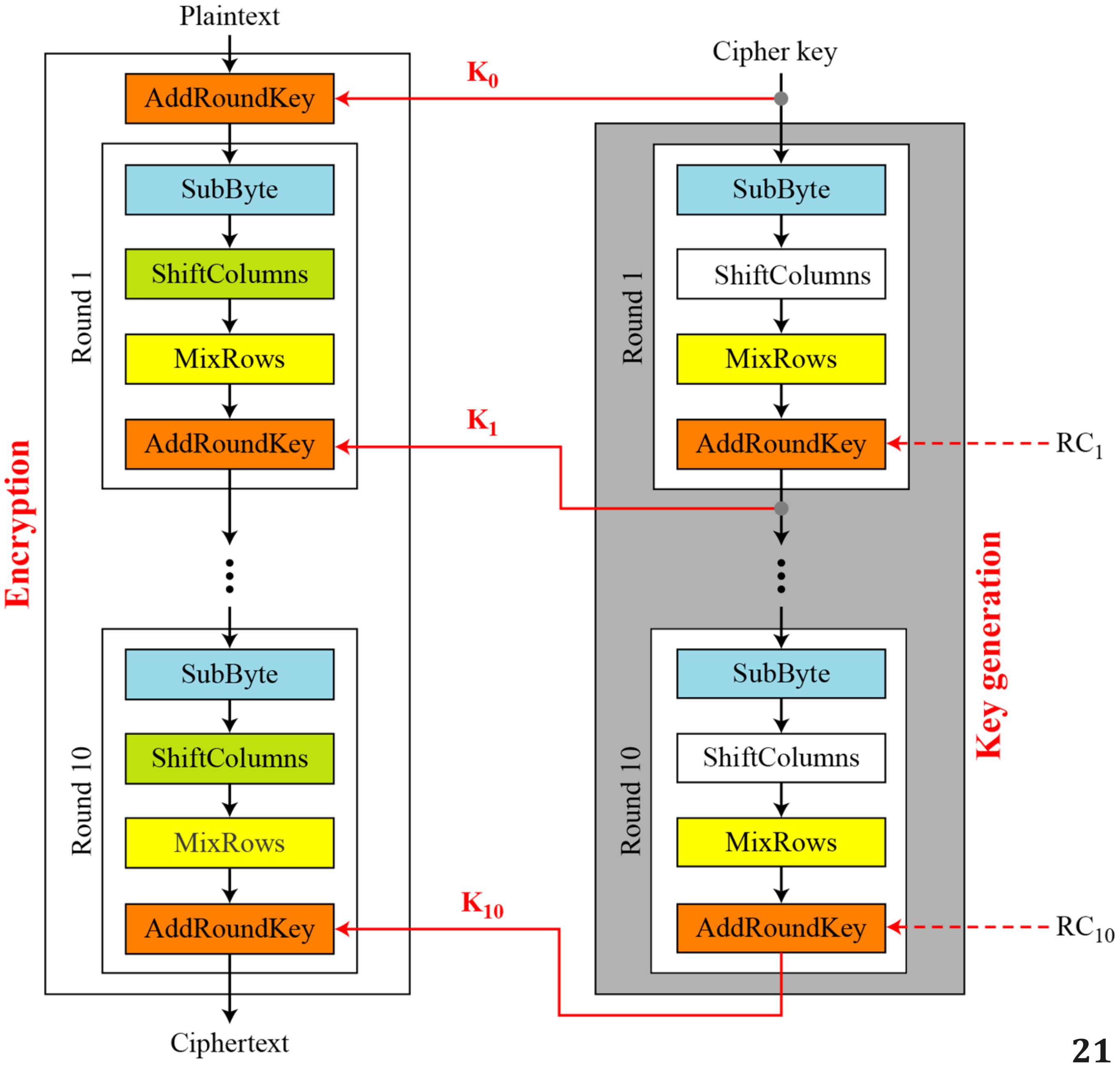
AddRoundKey



AddRoundKey transformation in the Whirlpool cipher

12.1.1 Continued

Key expansion in the Whirlpool cipher



12.1.1 Continued

Round constant for the i th ***round is given by***

RC_i[row,column] = SubBytes[8(i-1) + column]

$$\text{e.g., } RC_3 = \begin{bmatrix} \mathbf{1D} & \mathbf{E0} & \mathbf{D7} & \mathbf{C2} & \mathbf{2E} & \mathbf{4B} & \mathbf{FE} & \mathbf{57} \\ 00 & 00 & 00 & 00 & 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 & 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 & 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 & 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 & 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 & 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 & 00 & 00 & 00 & 00 \end{bmatrix}$$

12.1.2 Summary

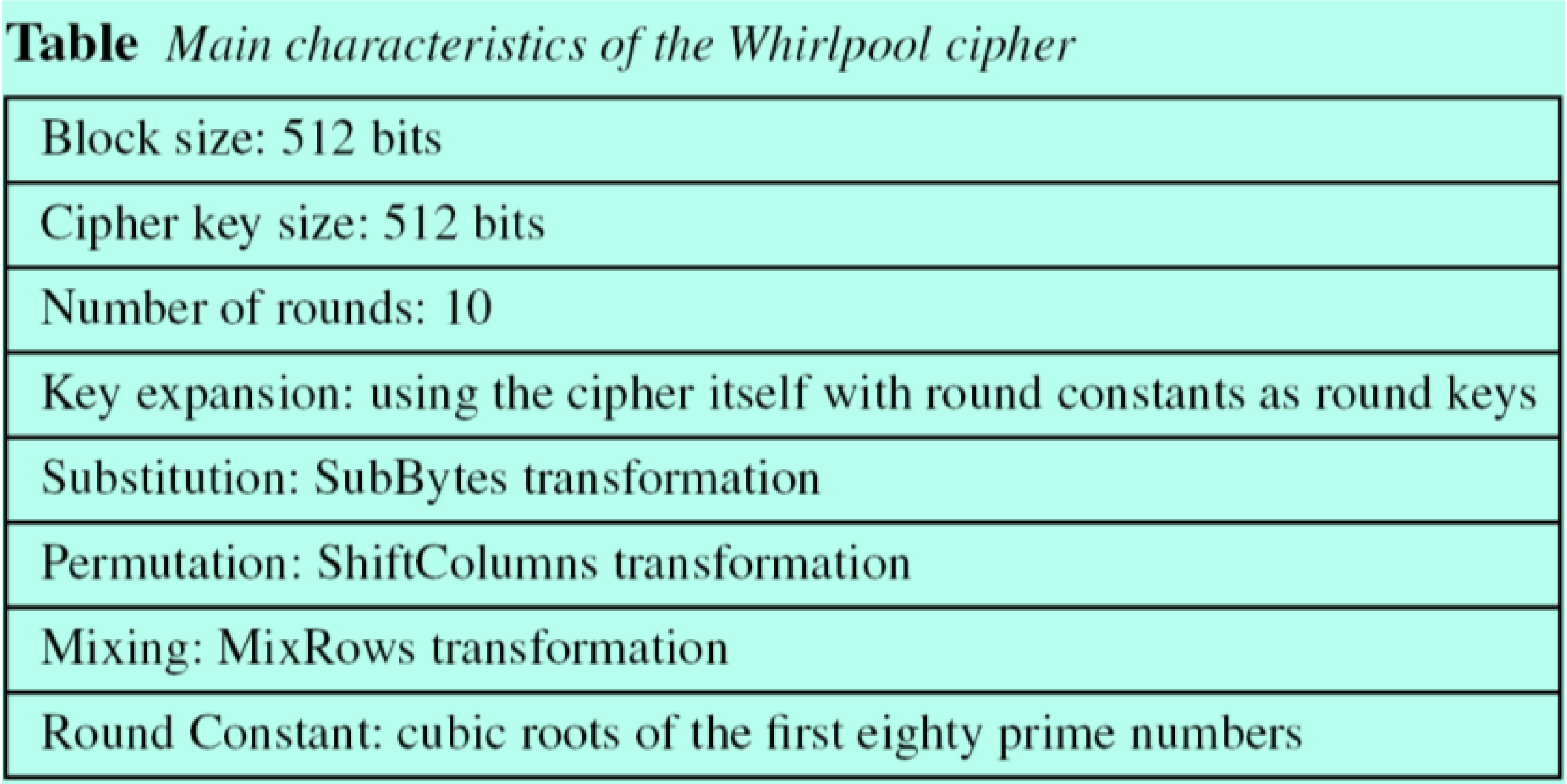


Table *Main characteristics of the Whirlpool cipher*

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

12.1.3 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.***

References

- **Chapter 12 -** Behrouz A Forouzan, Debdeep Mukhopadhyay, Cryptography and Network Security, Mc Graw Hill, 3rd Edition, 2015.

- **Chapter 12 -** William Stallings, Cryptography and Network Security Principles and Practices, 7th Edition, Pearson Education, 2017.