

crypting

Hashes and Crypto in GAP

0.9

22 September 2018

Markus Pfeiffer

Markus Pfeiffer

Email: markus.pfeiffer@st-andrews.ac.uk

Homepage: <http://www.morphism.de/~markusp/>

Address: School of Computer Science

North HaughSt Andrews

Fife

KY16 9SX

United Kingdom

Contents

1	CryptinG Functions	3
1.1	Internal Types and Functions	3
1.2	Hash functions	4
1.3	HMAC	4
	Index	5

Chapter 1

CryptinG Functions

1.1 Internal Types and Functions

1.1.1 IsSHA256State (for IsObject)

▷ IsSHA256State(*arg*) (filter)
Returns: true or false

1.1.2 CRYPTING_SHA256_State_Family

▷ CRYPTING_SHA256_State_Family (global variable)

1.1.3 CRYPTING_SHA256_State_Type

▷ CRYPTING_SHA256_State_Type (global variable)

1.1.4 CRYPTING_HexStringIntPad

▷ CRYPTING_HexStringIntPad(*int*, *pad*, *length*) (function)

Call **Reference: HexStringInt** on the argument *int* then pad the string on the left to *length* using padding letter *pad*

1.1.5 CRYPTING_HexStringIntPad8

▷ CRYPTING_HexStringIntPad8(*int*) (function)

Call **Reference: HexStringInt** on the argument *int* then pad the string on the left to length 8 using padding letter 0.

1.2 Hash functions

1.2.1 SHA256String

▷ `SHA256String(string)` (function)

Compute the SHA256 hash of the argument *string* in `IsStringRep`

1.3 HMAC

1.3.1 HMACSHA256

▷ `HMACSHA256(key, string)` (function)

Compute the HMAC SHA256 given a *key* and a *string* in `IsStringRep`.

Index

CRYPTING_HexStringIntPad, [3](#)
CRYPTING_HexStringIntPad8, [3](#)
CRYPTING_SHA256_State_Family, [3](#)
CRYPTING_SHA256_State_Type, [3](#)

HMACSHA256, [4](#)

IsSHA256State
 for IsObject, [3](#)

SHA256String, [4](#)