crypting

Hashes and Crypto in GAP

0.10.4

2 November 2022

Markus Pfeiffer

Markus Pfeiffer
Email: markus.pfeiffer+gap@morphism.de
Homepage: http://www.morphism.de/~markusp/

Contents

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