

# crypting

## Hashes and Crypto in GAP

0.10

28 October 2019

**Markus Pfeiffer**

**Markus Pfeiffer**

Email: [markus.pfeiffer+gap@morphism.de](mailto:markus.pfeiffer+gap@morphism.de)

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

# Contents

<b>1</b>	<b>CryptinG Functions</b>	<b>3</b>
1.1	Internal Types and Functions . . . . .	3
1.2	Hash functions . . . . .	4
1.3	HMAC . . . . .	4
	<b>Index</b>	<b>5</b>

# 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](#)