CRYPT$ - Return CRYPT$ hash

The CRYPT$ routine can be used to calculate a hash-sum using the Microsoft CryptAPI.

1. Invocation

To use the CryptAPI to calculate a hash-sum code:

```
CALL CRYPT$ USING ha
```

where *ha* is a control block of the following format:

```
01    HA
  02  HAVERS      PIC 9(4) COMP     * CONTROL BLOCK VERSION NUMBER
                                    * MUST BE 1
  02  HAALG       PIC 9(4) COMP     * HASH ALGORITHM
                                    * 0 = INVALID
                                    * 1 = SHA1 binary result returned
                                    * 2 = SHA1 ASCII result returned
                                    * 3 = SHA1 ASCII result (lower-case)
                                    * 4 = MD5 binary result returned
                                    * 5 = MD5 ASCII result returned
                                    * 6 = MD5 ASCII result (lower-case)
                                    * OTHER VALUES RESERVED FOR FUTURE USE
  02  HALEN1      PIC 9(4) COMP     * LENGTH OF STRING TO CALCULATE HASH FROM
                                    * (0 = ASSUME STRING IS ZERO TERMINATED)
  02  HAPTR1      PIC PTR           * POINTER TO STRING TO CALCULATE HASH FROM
  02  HALEN2      PIC 9(4) COMP     * SIZE OF RESULT BUFFER AREA
  02  HAPTR2      PIC PTR           * POINTER TO RESULT BUFFER (SIZE HALEN2)
                                    * TO ACCEPT THE HASH SUM
  02  HALENR      PIC 9(4) COMP     * ACTUAL LENGTH OF HASH-SUM RETURNED HERE
                                    * HAALG = 1 EXPECT 20 BYTES
                                    * HAALG = 2 EXPECT 40 BYTES
                                    * HAALG = 3 EXPECT 40 BYTES
                                    * HAALG = 4 EXPECT 16 BYTES
                                    * HAALG = 5 EXPECT 32 BYTES
                                    * HAALG = 6 EXPECT 32 BYTES
  02  HARES1      PIC 9(4) COMP     * FAILED FUNCTION IDENTIFIER
  02  HARES2      PIC 9(9) COMP     * WINDOWS ERROR CODE
```

2. STOP Codes and Exception Conditions

The following STOP codes may be generated by CRYPT$:

STOP code	Description
24120	Unknown version of HA control block (i.e. HAVERS does not contain 1)
24121	Unknown algorithm (i.e. HAALG does not contain 1 to 6, inclusive)
24122	HALEN2 too small for returned hash result.

The following exception conditions may be returned by CRYPT$:

EXIT code	$$COND	Description
24101	01	Exception from Windows encryption API.

3. Programming Notes

CRYPT$ is only available with GSM SP-30 and GLOBAL.EXE V4.10, or later.

HAALG values 4,5 and 6 (for MD5 hashing) are only supported by GSM SP-35, and later; and GLOBAL.EXE V5.6, and later.

A series of Windows functions are executed in order to return a hash-sum. If any of these functions fails CRYPT$ returns an EXIT 24101 with the last Windows error code in HARES2 and the failed function-id in HARES1:

Failed function-id (HARES1)	Windows function
1	The version of GLOBAL.EXE (or the Global Client Service) does not support the SVC-61 function required by CRYPT$.
234	CryptAcquireContext()
235	CryptCreateHash()
236	CryptHashData()
237	CryptGetHashParam()

Please refer to Microsoft documentation for details of Windows error code.

4. Examples

[EXAMPLE REQUIRED]

5. Copy-Books

None.

6. See Also

HASH$ Create hash-sum “by hand” using home-brew Alder-32 algorithm
HASHE$ Create hash-sum “by hand” using home-brew Alder-32 algorithm
HASHX$ Create hash-sum “by hand” using home-brew Alder-32 algorithm