New Hashtag Options

PxPlus 2019 (v16)

PxPlus Hashing Function

- Hashing is a mathematical function that maps data of any size into fixed sized data
  - Typical uses include:
    - Password storage
    - Blockchain (Bitcoin)
    - Data/Message integrity (CRC/LRC)

- HSH(…) function to hash data

```
hashstring$ = HSH(string$, hashtype)
```

Supported Hash Types

Hash Type	Description
0	PxPlus 2-byte hash (default, if not specified))
1	MD5 *
2	MD4 *
3	MD2 *
4	SHA-1 *
5	MDC2 *
6	RIPEMD *
7	HMAC *
224	SHA-224 (28-byte value) *
256	SHA-256 (32-byte value) *
384	SHA-384 (48-byte value) *
512	SHA-512 (64-byte value) *
-1	SHA-1 – (20-byte value)

* Indicates uses OpenSSL libraries (all other hashing uses internal logic)

Supported Hash Types

Hash Type	Description
0	PxPlus 2-byte hash (default, if not specified))
1	MD5 *
2	MD4 *
3	MD2 *
4	SHA-1 *
5	MDC2 *
6	RIPEMD *
7	HMAC *
224	SHA-224 (28-byte value) *
256	SHA-256 (32-byte value) *
384	SHA-384 (48-byte value) *
512	SHA-512 (64-byte value) *
-1	SHA-1 – (20-byte value)
-2	SHA-256 (32-byte value)

* Indicates uses OpenSSL libraries (all other hashing uses internal logic)

SHA-256 Hashing

- SHA-256 hashing (*hashtype* 256)

```
hashstring$ = HSH(string$, 256)
```

  - Relies on OpenSSL to perform hashing

- Internal SHA-256 hashing (*hashtype* -2)

```
hashstring$ = HSH(string$, -2)
```

  - No dependency on OpenSSL and faster
  - Returns HTA( ) of the actual hash; suitable to store in files with delimiters

Chunked Hashing

Getting Around Memory Constraints

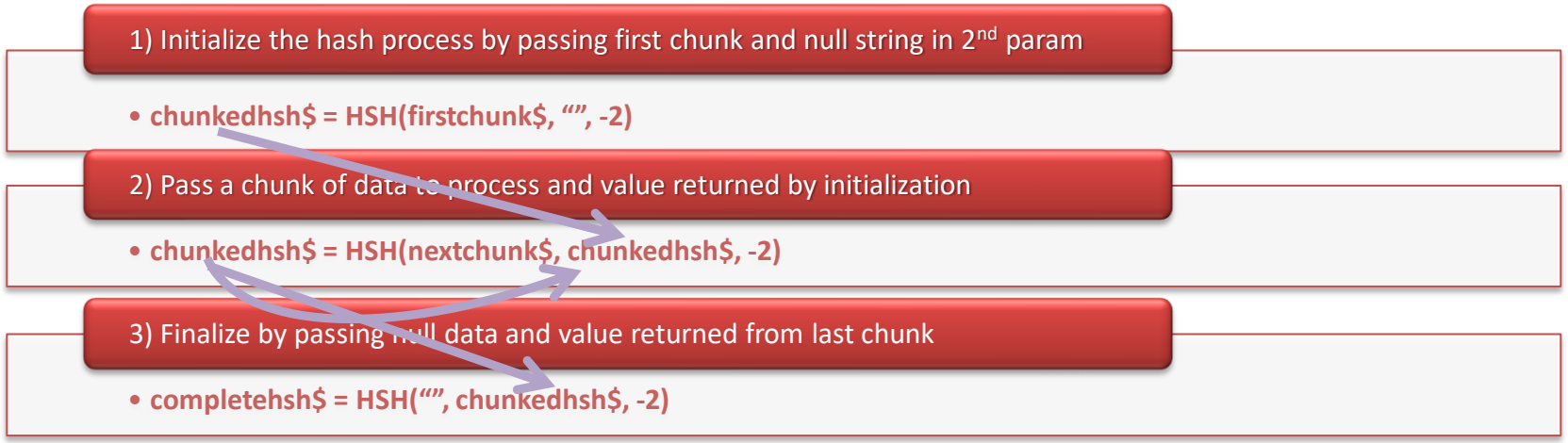
- Common to hash large amounts of data
  - HSH function requires passing 'complete' string
  - Requires data to be in memory limited to space available

- PxPlus 2019 added option to hash the data in chunks
  - Uses less memory
  - Computation of hash on data of virtually unlimited length
  - Only available on these internal hash types
    - SHA-1 (-1)
    - SHA-256 (-2)

Chunked Hashing

How to use Hash in Chunks

- Process involves three steps



Chunked Hashing

Sample Program

- Typical SHA computation for large file

```
 open (1,isz=1)"bigfile"
!
 chunkedhsh$ = ""
!
while 1
 read record (1,siz=10000,end=*break) chunk$
 chunkedhsh$ = hsh(chunk$,chunkedhsh$,-2) !  Update hash for this chunk
wend
!
bigfilehsh$ = hsh("",chunkedhsh$,-2) !  Finish hash with no data
```

Additional Resources

The help link(s) below refer to the current on-line help pages. The functionality may have been further updated since the PxPlus 2019 (version 16) release.

- HSH() Generate Hash Value
- Chunked Hashing