

## SHA512,SHA384 and SHA256 support in MySQL

```
#####  
The article was obtained at the following URL: http://www.kfwebs.net/articles/article/12  
The article might be distributed further as long as it is provided as it is, with the credits stated.  
The Article was written and first published by KF Webs, at http://www.kfwebs.net  
#####
```

*This is a set of user defined functions adding support for the Secure Hash Algorithm with a digest size of 512, 384 and 256 bits. It use a modified version of Crypto++ for the actual hash operation, whereby the MySQL wrapper is written by me.*

*Added: 2005-07-25 01:04:49 - Modified: 2006-03-09 02:47:42 - Level: Advanced*

### Quick installation

1. Installing Crypto++
  1. Download [Crypto++](#)
  2. Apply patch using "patch < config.h.diff"; <http://www.kfwebs.net/files/config.h.diff> (sig)
  3. Follow installation instructions for Crypto++
2. Installing the plugin
  1. Dowload and verify integrity
  2. Compile the plugin using the command provided below
  3. Copy mysql\_sha.so to /lib/
  4. Load the functions using the prototypes below

### More details

The SHA (Secure Hash Algorithm) family is a set of related cryptographic hash functions. The most commonly used function in the family, SHA-1, is employed in a large variety of popular security applications and protocols, including TLS, SSL, PGP, SSH, S/MIME, and IPSec. SHA-1 is considered to be the successor to MD5, an earlier, widely-used hash function. The SHA algorithms were designed by the National Security Agency (NSA) and published as a US government standard.

The first member of the family, published in 1993, is officially called SHA; however, it is often called SHA-0 to avoid confusion with its successors. Two years later, SHA-1, the first successor to SHA, was published. Four more variants have since been issued with increased output ranges and a slightly different design: SHA-224, SHA-256, SHA-384, and SHA-512 - sometimes collectively referred to as SHA-2.

This library use a modified version of Crypto++. The difference is that the type definition of byte is moved into the CryptoPP namespace to avoid ambiguity with the MySQL definition of the same type. The provided .diff-file is against version 5.2.1.

The library was compiled using the following command

```
g++ -shared -o mysql_sha.so -I/usr/local/mysql/include mysql_sha.cpp /lib/libcryptopp.a
```

The MySQL prototypes that are provided by this library are

```
CREATE FUNCTION sha512 RETURNS STRING SONAME 'mysql_sha.so';
CREATE FUNCTION sha384 RETURNS STRING SONAME 'mysql_sha.so';
CREATE FUNCTION sha256 RETURNS STRING SONAME 'mysql_sha.so';
```

## Usage example

```
mysql> SELECT sha512('abc') as sha512;
```

```
+-----+
|sha512 |
+-----+
|ddaf35a193617abacc417349ae20413112e6fa4e89a97ea20a9eeee64b55d39a2192992a274fc1a836ba3c23a3feebbd454
|
+-----+
1 row in set (0.00 sec)
```

```
mysql> SELECT sha384('abc');
```

```
+-----+
| sha384('abc') |
+-----+
|
|cb00753f45a35e8bb5a03d699ac65007272c32ab0eded1631a8b605a43ff5bed8086072ba1e7cc2358baeca134c825a7
|
+-----+
1 row in set (0.00 sec)
```

```
mysql> SELECT sha256('abc') as sha256;
```

```
+-----+
| sha256 |
+-----+
|ba7816bf8f01cfea414140de5dae2223b00361a396177a9cb410ff61f20015ad |
+-----+
1 row in set (0.00 sec)
```

## Further development

Please support further development of this plugin

## Source



The source can be apprehended at

[Source](#)

[PGP signature](#)

## Installation help and feedback

If you need help installing this package, or have a comment regarding it, then please fill out a contact request at <http://www.kfwebs.net/contact.php>.

## Related articles:

[MySQL UDF: Whirlpool and Tiger](http://www.kfwebs.net/articles/article/13)[<http://www.kfwebs.net/articles/article/13>] ([SQL](#))