

MySQL UDF: Whirlpool and Tiger

```
#####  
The article was obtained at the following URL: http://www.kfwebs.net/articles/article/13  
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 simple User Defined Function for MySQL adding support for Whirlpool (512 bit) and Tiger (192 bit)
Added: 2005-07-31 20:27:35 - Modified: 2006-03-09 02:49:15 - 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_oahash.so to /lib/
 4. Load the functions using the prototypes below

More details

Whirlpool

WHIRLPOOL is a hash function designed by Vincent Rijmen and Paulo S. L. M. Barreto that operates on messages less than 2^{256} bits in length, and produces a message digest of 512 bits.

WHIRLPOOL has been selected for the NESSIE portfolio of cryptographic primitives. The International Organization for Standardization (ISO) has decided to include the final version of WHIRLPOOL in the revised ISO/IEC 10118-3:2003(E) standard.

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 and can be downloaded at <http://www.kfwebs.net/files/config.h.diff> (sig)

Tiger

Tiger is a cryptographic hash function designed by Ross Anderson and Eli Biham in 1996 with a view for efficiency on 64-bit platforms. The size of a Tiger hash value is 192 bits. There also exists 128 and 160-bit versions of this algorithm, called Tiger/128 and Tiger/160. Both variants return truncated Tiger/192 hash values.

Compilation and prototypes

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

The MySQL prototypes that are provided by this library are

```
CREATE FUNCTION whirlpool RETURNS STRING SONAME 'mysql_ohash.so';  
CREATE FUNCTION tiger RETURNS STRING SONAME 'mysql_ohash.so';
```

Usage examples

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

```
+-----+  
| whirlpool('abc') |  
+-----+  
|  
8afc0527dcc0a19623860ef2369d0e25de8ebe2abaa40f598afaf6b07c002ed73e4fc0fc220fd4f54f74b5d6b07aa57764c3d  
|  
+-----+  
1 row in set (0.00 sec)
```

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

```
+-----+  
| tiger('abc') |  
+-----+  
| 2aab1484e8c158f2bfb8c5ff41b57a525129131c957b5f93 |  
+-----+  
1 row in set (0.00 sec)
```

Further development

Please support further development of this plugin

Source

http://www.kfwebs.net/files/mysql_ohash.cpp (sig)

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:

[SHA512,SHA384 and SHA256 support in MySQL](http://www.kfwebs.net/articles/article/12)[<http://www.kfwebs.net/articles/article/12>] ([SQL](#))