

# BaroCRYPT Guide(MySQL/MariaDB)

## Index

Index .....	<b>0</b>
1. BaroCRYPT .....	<b>1</b>
1.1 BaroCRYPT Overview.....	1
1.2 BaroCRYPT Features/Benefits .....	1
2. BaroCRYPT Integration API .....	<b>3</b>
2.1 Integration API configuration.....	3
2.2 Integration API functions.....	3
3. Create/Use/Delete functions.....	<b>4</b>
3.1 Create function .....	4
3.2 Use function.....	4
3.3 Delete function .....	5
4. About BaroCRYPT.....	<b>6</b>



SQL statements.

※ What is a Feistel Cipher?

It is a repetitive block cipher in which the ciphertext is encrypted from the plaintext while repeating the same substitution and substitution. It is a cipher similar to the Data Encryption Standard (DES). The other halves do an exclusive OR (XOR) and then swap each other. Do this process in the same pattern for each permutation, but do not exchange each other in the last permutation. The subkey used during encryption is reversed during decryption.

## 2. BaroCRYPT Integration API

### 2.1 Integration API configuration

Dynamic linking library related to BaroCRYPT is used to encrypt and decrypt data.

API Class	Description	Etc
libbaroudf.so	BaroCRYPT dll for MySQL/MariaDB	

### 2.2 Integration API functions

#### 1) TO\_ENCRYPTS function

- NAME  
TO\_ENCRYPTS
- SYNOPSIS  
void \* TO\_ENCRYPTS(const void \* data)
- DESCRIPTION  
A function that encrypts data.  
data: data to encrypt
- RETURN VALUES  
return encrypted data

#### 2) TO\_DECRYPTS function

- NAME  
TO\_DECRYPTS
- SYNOPSIS  
void \* TO\_DECRYPTS(const void \* data)
- DESCRIPTION  
A function to decrypt data.  
data: data to decrypt
- RETURN VALUES  
Return the decrypted data

## 3. Create/Use/Delete functions

### 3.1 Create function

MySQL/MariaDB's UDF (User Defined Function) is used when calling an external program written in C or C++ in MySQL/MariaDB or sending data.

It must be written in C or C++, and the operating system must support dynamic loading.

Copy the attached files (libbaroudf.so) to the directory with the following command result in mysql shell.

```
Mysql> SHOW VARIABLES LIKE 'plugin_dir';
```

Variable_name	Value
plugin_dir	/usr/lib64/mariadb/plugin/

1 row in set (0.002 sec)

To create the TO\_ENCRYPTS, TP\_DECRYPTS functions, execute the following commands in mysql shell.

```
MariaDB> create function TO_ENCRYPTS returns string soname 'libbaroudf.so';
MariaDB> create function TO_DECRYPTS returns string soname 'libbaroudf.so';
```

### 3.2 Use function

To use the TO\_ENCRYPTS, and TP\_DECRYPTS functions, execute the following commands in mysql shell.

```
MariaDB> select * from func;
```

name	ret	dl	type
TO_DECRYPTS	0	libbaroudf.so	function
TO_ENCRYPTS	0	libbaroudf.so	function

2 rows in set (0.00 sec)

```
MariaDB> select TO_ENCRYPTS('I am Tom');
```

TO_ENCRYPTS('I am Tom')
W11HfaAAnMZDKuUe

1 row in set (0.00 sec)

```
MariaDB> select TO_DECRYPTS('W11HfaAAnMZDKuUe');
```

```
+-----+
| TO_DECRYPTS('W11HfaAAnMZDKuJe') |
+-----+
| I am Tom                          |
+-----+
1 row in set (0.00 sec)
```

### 3.3 Delete function

To delete the TO\_ENCRYPTS, and TP\_DECRYPTS functions, execute the following command in mysql shell.

```
MariaDB> drop function if exists TO_ENCRYPTS;
MariaDB> drop function if exists TO_DECRYPTS;
```

## 4. About BaroCRYPT



Version 1.0 – Official Release – 2016.12.1  
Copyright © Nuri it corp. All rights reserved.  
<http://www.nurit.co.kr>

Company: Nurit Co., Ltd.  
Registration Number: 258-87-00901  
CEO: Jongil Lee  
Tel: +82-2-2665-0119(Technical support, sales inquiry)  
email: [mc529@nurit.co.kr](mailto:mc529@nurit.co.kr)  
Address: #913, 15, Magokjungang 2-ro, Gangseo-gu, Seoul (Magok-dong, Magok Techno Tower 2)