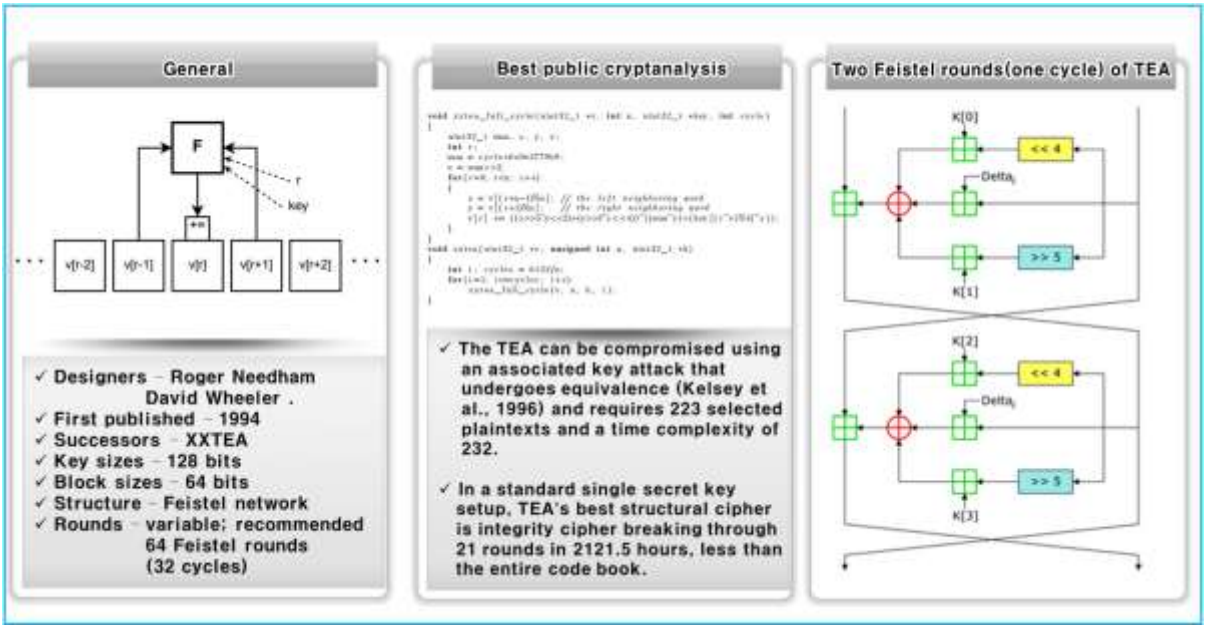
BaroCRYPT Guide(MySQL/MariaDB)

Index

1. BaroCRYPT

1.1 BaroCRYPT Overview

The BaroCRYPT solution is a lightweight and fastest encryption algorithm based on the XXTEA (Extended Extended Tiny Encryption Algorithm), a compact and easy-to-implement block encryption algorithm using the Feistel cipher.



1.2 BaroCRYPT Features/Benefits

Based on the XXTEA (aka Corrected Block TEA) encryption algorithm, the BaroCRYPT solution is an optimal solution capable of quickly encrypting and decrypting data even under extreme constraints such as legacy hardware systems (embedded) with a minimum amount of usable RAM. Is as follows.

- ■ It is a small and easy-to-implement block encryption algorithm based on the Feistel cipher, which is small in size, fast and easy to implement.
- ■ It is a small-sized algorithm based on the Feistel cipher, and has high encryption strength compared to its size.
- ■ Although the size of the algorithm is small, it is the fastest and safest algorithm in existence.
- ■ Compared to other block encryption algorithms, it is easy to implement, easy to apply to environments with large hardware specification constraints, and freely used.
- ■ It is a block encryption algorithm that encrypts 64 bits (8 bytes) and uses a 128 bit (16 byte) key.
- ■ Corrected Block TEA (XXTEA) is a block cipher algorithm originally designed to correct the weakness of Block TEA
- ■ Provides free customizing and convenience of interlocking development with various application programs. (API integration in Java and C languages)
- ■ TO_ENCRYPTS (encryption) and TO_DECRYPTS (decryption) functions are provided for easy use in

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
BaroUDF_MySQL.dll	BaroCRYPT dll for MySQL	
BaroUDF_MariaDB.dll	BaroCRYPT dll for MariaDB	

2.2 MySQL integration API functions

1) libBaroUDF_MySQL_info function

- NAME
  libBaroUDF_MySQL_info

- SYNOPSIS
  char * libBaroUDF_MySQL_info()

- DESCRIPTION
  Get information about the currently installed version of lib_mysqludf_sys.

- RETURN VALUES
 Returns lib_mysqludf_sys version information.

2) 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

3) 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

2.3 MariaDB integration API function

1) libBaroUDF_MariaDB_info function

- NAME
libBaroUDF_MariaDB_info

- SYNOPSIS
char * libBaroUDF_ MariaDB_info()

- DESCRIPTION
Get information about the currently installed version of lib_mysqludf_sys.

- RETURN VALUES
lib_mysqludf_sys 버전 정보를 반환

2) TO_ENCRYPTS 함수

- 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

3) TO_DECRYPTS 함수

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

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

Copy the attached files (BaroUDF_MySQL.dll, BaroUDF_MariaDB.dll) to the directory with the following command result in mysql shell.

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

To create the libBaroUDF_MySQL_info, libBaroUDF_MariaDB_info, TO_ENCRYPTS, TP_DECRYPTS functions, execute the following commands in mysql shell.

1) For MySQL

```
mysql> create function libBaroUDF_MySQL_info returns string soname 'BaroUDF_MySQL.dll';
mysql> create function TO_ENCRYPTS          returns string soname 'BaroUDF_MySQL.dll';
mysql> create function TO_DECRYPTS          returns string soname 'BaroUDF_MySQL.dll';
```

2) For MariaDB

```
mysql> create function libBaroUDF_MariaDB_info returns string soname 'BaroUDF_MariaDB.dll';
mysql> create function TO_ENCRYPTS            returns string soname 'BaroUDF_MariaDB.dll';
mysql> create function TO_DECRYPTS            returns string soname 'BaroUDF_MariaDB.dll';
```

3.2 Use function

To use the libBaroUDF_MySQL_info, libBaroUDF_MariaDB_info, TO_ENCRYPTS, and TP_DECRYPTS functions, execute the following commands in mysql shell.

1) For MySQL

```
mysql> select * from func;
+---------------------+-----+-------------------+----------+
| name                | ret | dl                | type     |
+---------------------+-----+-------------------+----------+
| TO_DECRYPTS         |   0 | BaroUDF_MySQL.dll | function |
| TO_ENCRYPTS         |   0 | BaroUDF_MySQL.dll | function |
| libBaroUDF_MySQL_info |   0 | BaroUDF_MySQL.dll | function |
+---------------------+-----+-------------------+----------+
3 rows in set (0.00 sec)

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

```
+-------------------------+
| TO_ENCRYPTS('I am Tom') |
+-------------------------+
| W11HfaAAnMZDKuUe        |
+-------------------------+
1 row in set (0.00 sec)

mysql> select TO_DECRYPTS('W11HfaAAnMZDKuUe');
+-----------------------------------+
| TO_DECRYPTS('W11HfaAAnMZDKuUe') |
+-----------------------------------+
| I am Tom                          |
+-----------------------------------+
1 row in set (0.00 sec)
```

2) For MariaDB

```
mysql> select * from func;
+-------------------------+-----+--------------------+----------+
| name                    | ret | dl                 | type     |
+-------------------------+-----+--------------------+----------+
| TO_DECRYPTS             |   0 | BaroUDF_MariaDB.dll | function |
| TO_ENCRYPTS             |   0 | BaroUDF_MariaDB.dll | function |
| libBaroUDF_MariaDB_info |   0 | BaroUDF_MariaDB.dll | function |
+-------------------------+-----+--------------------+----------+
3 rows in set (0.00 sec)

mysql> select TO_ENCRYPTS('I am Tom');
+-------------------------+
| TO_ENCRYPTS('I am Tom') |
+-------------------------+
| W11HfaAAnMZDKuUe        |
+-------------------------+
1 row in set (0.00 sec)

mysql> select TO_DECRYPTS('W11HfaAAnMZDKuUe');
+-----------------------------------+
| TO_DECRYPTS('W11HfaAAnMZDKuUe') |
+-----------------------------------+
| I am Tom                          |
+-----------------------------------+
1 row in set (0.00 sec)
```

3.3 Delete function

To delete the libBaroUDF_MySQL_info, libBaroUDF_MariaDB_info, TO_ENCRYPTS, and TP_DECRYPTS functions, execute the following command in mysql shell.

1) For MySQL

```
mysql> drop function if exists libBaroUDF_MySQL_info;
mysql> drop function if exists TO_ENCRYPTS;
mysql> drop function if exists TO_DECRYPTS;
```

2) For MariaDB

```
mysql> drop function if exists libBaroUDF_MariaDB_info;
mysql> drop function if exists TO_ENCRYPTS;
mysql> drop function if exists TO_DECRYPTS;
```

4. About BaroCRYPT

Version 1.0 - Official Release - 2016.12.1

http://www.nurit.co.kr

Company: Nurit Co., Ltd.
Registration Number: 258-87-00901
CEO: Jongil Lee
Tel: +8210-2771-4076(Technical support, sales inquiry)
email: mc529@nurit.co.kr
Address: #913, 15, Magokjungang 2-ro, Gangseo-gu, Seoul (Magok-dong, Magok Techno Tower 2)