**飞比-樱花-有家动态密码生成运算说明**

**一、加密因子的概述：**

1、用户种子的概念：是用于区分保洁、用户等不同类型用户的唯一数值，由服务端单独下发给门锁，门锁需要保存；种子另区分1次性用户种子、2次性用户种子、3次性用户种子……n次性用户种子，服务器下发时会指明。

2、秘钥Key来源：“用户种子” + “IEEE地址”作为秘钥key。

3、原始密码Source 来源：“当天有效的时间 ” 作为原始密码Source 。

4、将”秘钥” 与 “原始密码” 以xxTea方式进行加密运算，将计算结果的十进制显示方式(低4位)作为“动态密码”的前四位十进制数，“前四位十进制数”与“当天有效的时间段”做混淆运算其得数作为“动态密码”的后四位十进制数。

1. **用户在锁键盘输入固定8位数值的意义**

例如：用户输入了5482 4268

解析：

前四位十进制数5482表示加密运算后的验证码，需锁端进行解密验证，验证请看下文。

后四位十进制数4268表示5482与“当天有效的时间段”与减法得数的绝对值，则当天有效的时间段的计算方式为 **|5482-4268|=1214（**混淆运算**）**，表示当天的12：00-14：00期间有效。

**三、动态密码生成举例：**

例：生成保洁啊姨A其用户种子为123456，于12：00-14：00之间有效的动态密码xxxx xxxx，。

保洁啊姨A的用户种子：123456

读取门锁IEEE为：00 12 4B 00 0F F4 31 40 (低三字节为：F4 31 40)

即秘钥key为: 第一步 “用户种子” + “IEEE” = 12 34 56 F4 31 40

第二步 修改 “用户种子” ，用“IEEE”对其进行异或运算，如下所示

key[0] ^= key[3];

key[1] ^= key[4];

key[2] ^= key[5];

原始密码Source：由有效时间段12：00-14：00得001214

使用秘钥key，对原始密码Source 进行xxTea加密，进行运算后Source加密成为0xBB 11 AD (十进制表示为12,259,757)；将结果低4位9,757作为“动态密码”的前四位十进制数；运算|9757-1214|=8543（混淆运算）作为“动态密码”的后四位十进制数；最后得出的完整8位动态密码为**9757 8543**。