Password Encryption

ANSI X9.8 Format (带主帐号信息)

- PIN BLOCK 格式: 等于 PIN 按位异或主帐号
- PIN 格式: (个人识别码 Personal Identity Number) 总共有8个byte长度, 分为两个部分; (类似数据包的格式)

  > Byte 1 PIN的长度
  >
  > Byte 2 – Byte 3/4/5/6/7 4--12个PIN(每个PIN占4个BIT)
  >
  > Byte4/5/6/7/8 – Byte 8 FILLER “F” (每个“F“占4个BIT)

- PAN (主帐号 Primary Account Number) 同样包含8个byte, 格式如下:

  > Byte 1 — Byte 2 0x00 0x00
  >
  > Byte 3 — Byte 8 12个主帐号字符 (最后一位为校验位)
  >
  > 12位字符主帐号的取法: 取主帐号的右12位 (不包括最右边的校验位), 不足12位左补“0X00”。

加密举例

- 明文 P `123456`
- 主帐号 P `123456789012345678`
- `678901234567` (最后一位校验位8的前12位字符为截取的主帐号)
- 则用于 `0x00 0x00 0x67 0x89 0x01 0x23 0x45 0x67`
- 则 PIN BLOCK (PIN按位异或主帐号PAN)

  > 即是为: 0x06 0x12 0x34 0x56 0xFF 0xFF 0xFF 0xFF
  >
  > 异或上: 0x00 0x00 0x67 0x89 0x01 0x23 0x45 0x67
  >
  > 结果为: 0x06 0x12 0x53 0xDF 0xFE 0xDC 0xBA 0x98

Revision #1
Created 22 July 2021 16:22:51 by zhangkexin
Updated 22 July 2021 16:23:20 by zhangkexin