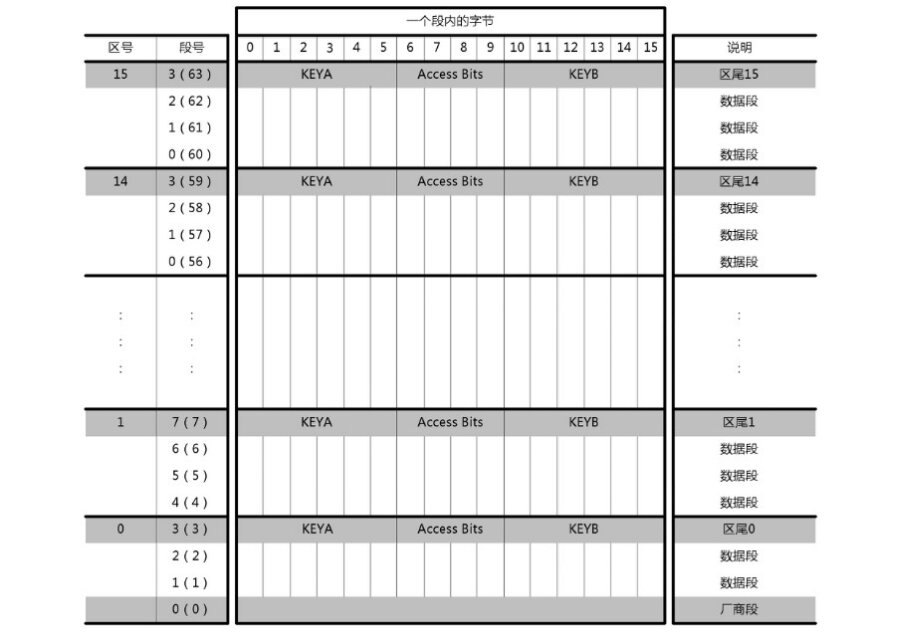
2008年的时候，荷兰恩智浦（NXP）公司开发的RFID产品Mifare Classic就被破解了，黑历史在这里就不在具体说了，想详细了解可以自己Google百度。现在还是重点说说关于Mifare Classic破解的内容。

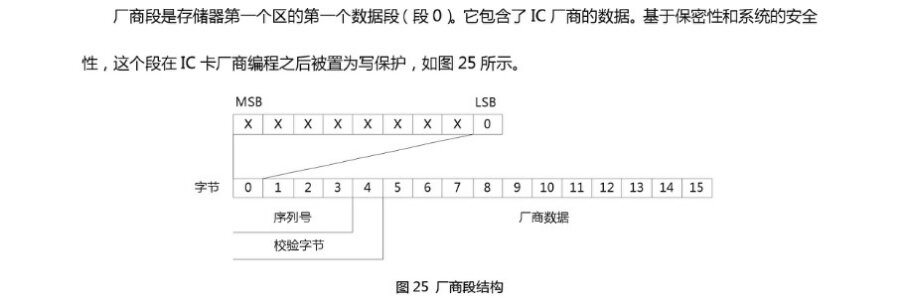
Mifare Classic提供1k-4k的容量，现在国内采用的多数是Mifare Classic 1k(S50)[后面简称M1卡]，而我以后的测试也大多是基于M1卡开展。

大家要先了解M1卡的结构，这能够为后期的破解做铺垫。

M1卡有从0到15共16个扇区，每个扇区配备了从0到3共4个段，每个段可以保存16字节的内容，为什么这里要强调从0开始呢？这跟C语言里面数组下标默认从0开始是差不多的，好计算地址偏移，我们不必太过在意，只是要记住是从0开始，写入数据的时候不要写错地方就可以了。每个扇区的第4个段（也就是3段）是用来保存KeyA，KeyB和控制位的，因为M1卡允许每个扇区有一对独立的密码保护，这样能够更加灵活的控制数据的操作，控制位就是这个扇区各种详细权限计算出来的结果。

每张M1卡都有一个全球唯一的UID号，这个UID号保存在卡的第一个扇区（0扇区）的第一段（0段），也称为厂商段，其中前4个字节是卡的UID，第5个字节是卡UID的校验位，剩下的是厂商数据。并且这个段在出厂之前就会被设置了写入保护，只能读取不能修改，当然也有例外，有种叫UID卡的特殊卡，UID是没有设置保护的，其实就是厂家不按规范生产的卡，M1卡出厂是要求要锁死UID的。下图很清晰的列出了M1卡的结构。

[](http://cdn.bobylive.com/wp-upload/wpid-rfid-1-1.jpg)

[](http://cdn.bobylive.com/wp-upload/wpid-rfid-1-2.jpg)

更多的M1卡结构可以下载这两个PDF仔细阅读。

[高频IC卡指南](http://s1.boby.im/other/rfid-practice.pdf)

[飞利浦官方M1卡文档](http://s1.boby.im/other/MF1S50YYX.pdf)

看完上面的文档我相信你对M1卡也有了一定的了解，现在就来简单谈谈M1卡的各种破解方法，后面会陆续发布相对应的实际案例。

（1）暴力破解

暴力破解是破解工作永远的话题，只要你拥有庞大的计算资源，管你什么密码都能破解。而且，在CRYPTO1算法的细节没有被泄露之前，最有效的方法就是暴破了。还有一个很重要的原因就是，M1卡是被动卡，需要读卡器为它提供能量，一旦读卡器切断了电源，卡中的临时数据就会丢失，这样就没有办法记录下攻击者究竟输错了多少次密码，卡永远不会因为密码输入错误太多而被锁定，只要攻击者有时间慢慢跟它耗，密码肯定会出来的。

这里列举一些常见的M1卡密钥

FFFFFFFFFFFF

A0A1A2A3A4A5

D3F7D3F7D3F7

000000000000

A0B0C0D0E0F0

A1B1C1D1E1F1

B0B1B2B3B4B5

4D3A99C351DD

1A982C7E459A

AABBCCDDEEFF

B5FF67CBA951

714C5C886E97

587EE5F9350F

A0478CC39091

533CB6C723F6

24020000DBFD

000012ED12ED

8FD0A4F256E9

EE9BD361B01B

（2）重放攻击

重放攻击是基于M1卡的PRNG算法漏洞实现的，当卡接近读卡器获得能量的时候，就会开始生成随机数序列，但这有一个问题，因为卡是被动式卡，本身自己不带电源，所以断电后数据没办法保存，这时基于LSRF的PRNG算法缺陷就出来了，每次断电后再重新接入电，卡就会生成一摸一样的随机数序列，所以我们就有可能把这个序列计算出来，所以只有我们控制好时间，就能够知道在获得能量后的某一刻时间的随机数是多少，然后进行重放攻击，就有可能篡改正常的数据。如果卡的所有权在我们手上的时候，我们甚至不需要浪费太多的时间就可以实现。

（3）克隆卡片

这是一个很简单也很实用的方法，因为M1卡自带扇区可以保存数据，所以大部分的卡片会选择加密扇区后将数据保存在里面，所以我们完全可以克隆一张带有一样数据的克隆卡。这就会用到一种叫uid卡的特殊M1模拟卡，前面说到每张M1卡在0扇区第1段都会有一个全球唯一的UID编号，而且这个块在出厂之后是被厂商设定保护无法修改的，uid卡就是没有设定0扇区保护的卡，所以你可以随意的修改你想要的uid，这样我们就可以克隆出一张连uid都相同的卡片了。

（4）密钥流窃听

利用神器proxmark 3可以嗅探到全部扇区都加密的M1卡，在卡和已经授权的读卡器交换数据的时候进行窃听，就能把tag数据读取出来，利用XOR算key工具就可以把扇区的密钥计算出来，这也是PRNG算法的漏洞所导致的。

（5）验证漏洞

验证漏洞是目前使用最多的M1破解手段，在读卡器尝试去读取一个扇区时，卡会首先发一个随机数给读卡器，读卡器接到随机数之后利用自身的算法加密这个随机数再反馈回给卡，卡再用自己的算法计算一次，发现结果一致的话就认为读卡器是授权了的，然后就用开始自己的算法加密会话并跟读卡器进行传送数据。这时候问题就来了，当我们再次尝试去访问另一个扇区，卡片又会重复刚才那几个步骤，但此时卡跟读卡器之间的数据交换已经是被算法加密了的，而这个算法又是由扇区的密钥决定的，所以密钥就被泄露出来了。因此验证漏洞要求我们至少知道一个扇区的密钥，但目前大部分的扇区都没有全部加密，所以很容易就会被破解。

破解M1卡当然不仅仅只有这几种方法，但对于我们来说已经足够了，目前国内80%的IC卡都是M1卡，例如门禁卡，饭卡，智能电卡之类的。

这里再提供两篇Radboud大学关于破解Mifare的论文，大家可以研究下，的确是受益匪浅。（注意是英语的哦。）

[The Mifare Hack](http://s1.boby.im/other/The-MIFARE-Hack.pdf)

[Dismantling MIFARE Classic](http://s1.boby.im/other/Dismantling-MIFARE-Classic.pdf)