

可以得到那个问号,是一个校验到期日期的校验位。而且校验位的方法也给出了。所以我们只需要按照他给的方法,就能 很方便的求出那个问号是7。

下面展示实现代码

```
a = [1,1,1,1,1,6]
b = [7,3,1,7,3,1]
for i in range(0,6):
    c = c + a[i]*b[i]
    res = c % 10
```

这样就得到了最终的护照信息是

12345678<8<<<1110182<1111167<<<<<<<<

2.求key

这个就是此题的关键部分, 也是我搞得最久的部分。

大体上分为

- 2、求Ka和Kb
- 3、对Ka和Kb奇偶校验生成key

2.1求Kseed

这部分也是按照参考文章,就可以轻松的得到Kseed了。

支持基本访问控制的机读旅行证件芯片须对非授权的阅读企图 (包括对逻辑数据结构中的(被保护的)文件的选 择) 作出"没有满足安全状态"(0x6982) 的响应。为认证查验系统,须进行下述步骤:

1. 查验系统按照Doc 9303号文件第1部分第1卷中第9段和15段的描述,使用OCR-B阅读器从机读区读取 "MRZ_information",该信息由并置的证件号码、出生日期和到期日构成,并包括它们各自的校验位。 或者可以将所需的信息凝上去。在这种情况下,所需的信息领随机读区内的显示打入。这一 "MRZ_information" SHA-1散列中的最高有效16字节被用作密钥种子,通过附录5.1描述的密钥衍生机 制导出证件基本访问密钥。

简单来说,就是把-证件的那些数字和校验位,直接sha1散列,然后取前16位即可。

2.2求Ka和Kb

证件基本访问密钥 $(K_{ENC}$ 与 $K_{MAC})$ 和安全通信会话密钥都是通过对一个密钥种子 (K_{seed}) 产生的两个主要的 3DES 密钥进行计算来建立的。

使用一个 32 位的计数器 c, 以便能够从一个单一的种子密钥中衍生出多个密钥。根据密钥是被用来加密的,还 是用来进行 MAC 计算的, 须分别选用下列值:

```
— c = 1 (i.e. '0x 00 00 00 01'),用于加密。
— c = 2 (i.e. '0x 00 00 00 02'),用于MAC计算。
```

执行下列步骤,以便从密钥种子 Kseed 和 c 中衍生出两个主要的 3DES 密钥:

1. 假定D为 K_{seed} 和 c的并置 (D= $K_{seed} \parallel c$)。

- 2. 计算H = SHA-1(D), 即: D的SHA-1散列。
- 3. H的字节1..8 形成密钥K_a, H的字节9..16形成密钥K_b。
- 4. 调整密钥K_a和 K_b的奇偶校验位形成正确的DES密钥。

这段话的主要意思就是,把之前生成的Kseed和c级联,然后再进行一次sha1散列生成了d,然后ka是d的前十六位,kb是

```
ka = shal(codecs.decode(d,"hex")).hexdigest()[:16]
kb = shal(codecs.decode(d,"hex")).hexdigest()[16:32]
```

2.3对Ka和Kb奇偶校验生成key

根据上段话,其实学过计算机网络的话其实非常好理解,就是算1的个数并且把第八位当作奇偶校验位。 这里就不多说什么了,直接上代码了,如果有什么不懂的可以在评论里面问我或者去百度或者google一下,网上的教程有 很多。

```
k_1 = jiaoyan(ka)
k_2 = jiaoyan(kb)
key = k_1 + k_2
print(key)
```

三、总结

因为找到了题目中参考文章的中文版本,所以阅读和理解起来其实还算挺轻松的。 这里面主要的难点就是里面的几个进制转换问题,这个我没有过多的去介绍,因为我也没特别明白,而且这几天也没有时间去投入精力,所以如果有问题评论私信都可以,我会尽量的去解答。 我也没有写sha1散列和AES的相关知识,我觉得做这种题的人应该对这几个密码都很熟悉的(笑)。 还有里面用到的校验位和奇偶校验问题,这个知识其实计算机网络里面讲的特别详细易懂,网上的教程应该也挺多的,我 就不多讲了。 有任何问题都可以在评论区里面问我。 最后附上相关文件的百度云网盘地址: 链接: https://pan.baidu.com/s/1sl-gBIMsEidYtNvgbGilAw 提取码: 4k74 Malformed UTF-8 characters, possibly incorrectly encoded qq_34228881的博客 ① 2万+ 错误信息如下:通过断点调试,错误信息出在链接数据库的地方,仔细检查了链接数据库的配置信息,还真有问题,真tm... Malformed UTF-8 characters, possibly incorrectly encoded 或中文乱码 是返回的数据有特殊字符,编码转换回来就好了mb_convert_encoding(\$value, 'UTF-8', 'UTF-8');中文乱码可以用... 抢沙发评论 PHP 报错 Malformed UTF-8 characters, possibly incorrectly encoded 编码转换问题 a810929296的博客 ① 2万+ ormed UTF-8 characters, possibly incorrectly encoded这个异常。 使用mb_convert_encoding和iconv都... PHP-Laravel 接口报错malformed utf-8 characters, possibly incorrectly encoded 使用PHPStorm突然报错编码错误malformed utf-8 characters, possibly incorrectly encoded 可能是系统的语言被更改了 ..Base64-encoded key bytes may only be_xiaopeng_th..._CSDN博客 Exception in thread "main" java.lang.lllegalArgumentException: Base64-encoded key bytes may only be specified for HMAC signatures.. ..invalid code, hints: [req_id: HQd79a0747th31..._CSDN博客 //正常返回的JSON数据包 { "openid": "OPENID", "session_key": "SESSIONKEY", } //满足UnionID返回条件时,返回的JSON数据包 { "ope... 人脸对齐--Face Alignment In-the-Wild: A Survey AI小作坊 的博客 ◎ 7275 Wild: A Survey Computer Vision and Image Understanding Volume 162, September 2017, Pages 1-22 https://w Problem (2) in the Chunked-Encoded data解决 本文转载自: http://www.windgreen.me/problem-2-in-the-chunked-encoded-data#more-382 今天遇到了一个很诡异的问题,是的,只能... ...Make sure map keys don't contain dots in th_fall..._CSDN博客 出现这个报错是因为mongodb的map类型里的key不能包含dots(.),把点去掉就好 ...Make sure map keys don't contain dots in th keda... CSDN博客 错误原因:mongodb当中的**key**存在,这种字符,比如说:dataFieldMap.name,需要将这种字符进行转义;以下是我的mongo的xml文件配置,具... AES128-ecb加解密 最近使用AES加解密的过程中遇到了一些问题,我这段采用的是openssi的AES.h的库进行加密的,因为传输的数据并不重要,考虑到并... Unicode-objects must be encoded before hashing 错误解决办法 提交注册用户数据后出来这个,错误原因是update()必须指定要加密的字符串的字符编码 s1 = sha1() s1.update(upwd.encode("utf8")) # .. AES自动生成base64密钥加密解密 高级加密标准(英语:Advanced Encryption Standard,缩写:AES),在密码学中又称Rijndael加密法,是美国联邦政府采用的一种区... CSDN开发助手, 生成开发者常用丁且, 提升开发效率 支持本地书签、tab页、历史记录搜索;集成CSDN搜索结果;他是一个时间转换工具;他是一个计算器;他是。。。,更多功能正在... RSA私钥和公钥文件格式 (pkcs#7, pkcs#8, pkcs#12, pem) ic Key file (PKCS#1) The RSA Public key PEM file is specific for RSA keys. It starts and ends with the tags: ----BEGIN RSA. ©2020 CSDN 皮肤主题: 数字20 设计师:CSDN官方博客 返回首页 关于我们 招贤纳士 广告服务 开发助手 ☎400-660-0108 ☑ kefu@csdn.net ⑤ 在线客服 工作时间 8:30-22:00 公安备家号11010502030143 京ICP备19004658号 京网文 [2020] 1039-165号 经营性网站务客信息 北东互联网街法和不良信息带接中心 网络110报警服务 中国互联网带报中心 家长监护 Chrome商店下载 ©1999-2020北京创新先和网络北木有限公司 版权与免费声明 版权申诉



