|  |
| --- |
| Github账号：spttt |
| **实验摘要：**  根据题目描述的电子护照信息查找相关资料获取密钥计算方法，计算密钥，解密消息。锻炼代码能力、英文理解能力，了解密码学的一个实际应用。 |
| **实验题目**  AES密钥—在欧洲护照的机读区中使用  一个由AES加密过的消息已转发给您（CBC加密模式，初始向量为0，填充模式为01-00）。此外，您还收到了对应的密钥信息，此密钥信息是以身份证明文件上使用的机器可读区域（MRZ）的形式给出的，例如欧洲使用的ePassports。很遗憾，您收到的密钥信息不太完整。    目的是找到以下base64编码消息的明文。  9MgYwmuPrjiecPMx61O6zIuy3MtIXQQ0E59T3xB6u0Gyf1gYs2i3K9Jxaa0zj4gTMazJuApwd6+jdyeI5iGHvhQyDHGVlAuYTgJrbFDrfB22Fpil2NfNnWFBTXyf7SDI  为了加密，已生成并应用了基于基本访问控制协议（BAC）的密钥KENC。为了解密，以下字符已经传送给您，从这些字符中可以导出KENC，（参考文献[1]描述了这些字符的编码规则）：  12345678<8<<<1110182<111116?<<<<<<<<<<<<<<<4  不幸的是，在传输过程中丢失了一个字符，并用“？”突出显示了该字符。不过，您可以在[2]的帮助下计算出“？”。为了以后能够计算密钥KENC，您可以在[3]，[4]和[5]中找到其使用的密钥生成协议。  AES加密的原始消息包含要输入“密语”，那就是此题目的解答。  参考文献  可以在线获取以下文档：https://www.icao.int/  [1] ICAO MRTD DOC 9303 Part 1 Vol 1, p. IV-16 (Data structure of the lower machine readable line) and p. IV-42  [2] ICAO MRTD DOC 9303 Part 1 Vol 1, p. IV-24 to IV-26 (Check digits in the machine readable zone)  [3] ICAO MRTD DOC 9303 Part 1 Vol 2, p. IV-13 (MRTD Basic Access Control)  [4] ICAO MRTD DOC 9303 Part 1 Vol 2, p. IV-32  [5] ICAO MRTD DOC 9303 Part 1 Vol 2, p. IV-40 IV-41 |
| **实验内容**   1. **实验基本原理及步骤**   1、资料获取  在[国际民航组织官网](https://www.icao.int/Pages/default.aspx)上搜索DOC 9303，下载[中文版参考文档](https://www.icao.int/Security/mrtd/Downloads/Forms/Default.aspx?RootFolder=%2FSecurity%2Fmrtd%2FDownloads%2FDoc%209303%2FDoc%209303%20Chinese&FolderCTID=0x0120009F8DC86A430F8C42B93391F24147F4B4&View=%7b32AE43DB-4BB8-4D6F-9352-638B2D3875CF%7d)，方便阅读。  2、求未知字符“？”  阅读[1]可知，字符串‘12345678<8<<<1110182<111116?<<<<<<<<<<<<<<<4’中，  1到9位为护照号码，第10位为其校验位；  14到19位为出生日期，第20位为其校验位；  22到27位为到期日，第28位为其校验位。  未知字符“？”是28位，即“？”是22到27位“111116”的校验位，文献[2]给出了校验位的计算方法，计算要点摘录如下：  校验位须在模数10 的基础上进行计算，不断地重复731 731……加权。   * 步骤1 从左到右，相应顺序位置上的加权数乘相关数字数据要素的每一位数。 * 步骤2 将每次乘法运算的乘积相加。 * 步骤3 将得出的和除以10（模数）。 * 步骤4 余数即为校验位。   根据以上计算方法，可以手工计算“111116”的校验位，(1\*7 + 1\*3 + 1\*1 + 1\*7 + 1\*3 + 6\*1) % 10 = 7，即未知字符“？”为7。  至此，恢复出了字符串‘12345678<8<<<1110182<1111167<<<<<<<<<<<<<<<4’  3、计算KENC  [3] [4] [5]描述了KENC的导出过程。  [3]描述了MRZ\_information是字符串中证件号码、出生日期和到期日，并包括它们各自的校验位组合而成的。按照这些信息对应的位置提取子字符串，并重新组合，可得到MRZ\_information。   1. MRZ\_line2 = b'12345678<8<<<1110182<1111167<<<<<<<<<<<<<<<4' 2. Number\_and\_check = MRZ\_line2[:10] 3. Birth\_and\_check = MRZ\_line2[13:20] 4. Expiry\_and\_check = MRZ\_line2[21:28] 5. mrz\_information = Number\_and\_check + Birth\_and\_check + Expiry\_and\_check   另外，[3]描述了密钥种子 (Kseed) 是“MRZ\_information”的SHA-1散列的前16字节。   1. K\_seed = hashlib.sha1(mrz\_information).hexdigest()[:32]   [4]描述了接下来的密钥生成方法，按照文件中的步骤操作即可。    图 1根据密钥种子计算密钥  1. D为Kseed 和 c的拼接 (D = Kseed || c)。（在加密中c = 0x 00 00 00 01）  2. 计算H = SHA-1(D)，即：H为D的SHA-1散列。  3. H的字节1..8 形成密钥Ka ，H的字节9..16形成密钥Kb。  4. 调整密钥Ka 和 Kb的奇偶校验位形成正确的DES密钥。  其中，1到3步的描述很明确，实现如下：   1. K\_seed = hashlib.sha1(mrz\_information).hexdigest()[:32] 2. D\_hex = K\_seed + '00000001' 3. Hash\_D = hashlib.sha1(binascii.a2b\_hex(D\_hex)).digest() 5. K\_a = Hash\_D[:8] 6. K\_b = Hash\_D[8:16]   第4步的调整奇偶校验位不是很明确。可以阅读[5]的处理过程实例分析这一步的操作。    图 2 调整奇偶校验位实例  观察发现，字符串按字节进行奇偶校验位的调整，所谓奇偶校验位就是每个字节8位中的最后1位，需要改变此位使得每个字节的二进制表示中有奇数个“1”。了解了其调整过程，便可编程实现，计算调整后的Ka 和 Kb，进而得到密钥K。   1. **def** adjust\_parity\_bit(bytestocheck): 2. res = b'' 3. **for** x **in** bytestocheck: 4. **if**(bin(x).count('1') % 2 == 0): 5. x = x ^ 1 6. res += x.to\_bytes(1, 'big') 7. **return** res 9. K\_a\_adjust = adjust\_parity\_bit(K\_a) 10. K\_b\_adjust = adjust\_parity\_bit(K\_b) 11. key = K\_a\_adjust + K\_b\_adjust   ４、解密  初始的密文需要先进行base64解密得到密文的字节码，加密模式为CBC，初始向量为0，调用AES解密可得到解密结果。   1. cipher\_base64 = '9MgYwmuPrjiecPMx61O6zIuy3MtIXQQ0E59T3xB6u0Gyf1gYs2i3K9Jxaa0zj4gTMazJuApwd6+jdyeI5iGHvhQyDHGVlAuYTgJrbFDrfB22Fpil2NfNnWFBTXyf7SDI' 2. cipher\_bytes = base64.b64decode(cipher\_base64) 3. IV = b'\x00'\*16 4. m = AES.new(key, AES.MODE\_CBC, IV).decrypt(cipher\_bytes)   解密结果为：b'Herzlichen Glueckwunsch. Sie haben die Nuss geknackt. Das Codewort lautet: Kryptographie!\x01\x00\x00\x00\x00\x00\x00'  手动移除01-00 填充，可得到明文 Herzlichen Glueckwunsch. Sie haben die Nuss geknackt. Das Codewort lautet: Kryptographie!   1. **实验结果**     图 3 实验结果   1. **实验结果的分析**   尝试翻译该明文，发现翻译软件提示其为德文。大意为：恭喜你，你破解了难题。该密语是：密码学！ |
| **实验总结**  1、英文的题目描述不易明白，需要利用软件翻译、查单词等手段帮助理解。认真阅读，理解题意。  2、题目参考文档的内容很多，需要只看有用的部分节约时间。 |
| **参考文献**  [6] Koz\_0. mysterytwisterc3-challenge-AES key — encoded in the machine readable zone of a European ePassport. [EB/OL]. (2020-11-07)[2020-11-12]. <https://blog.csdn.net/Koz_0/article/details/109540921>  [7] Joel-Q-Xu. MT3-mysterytwisterc3. [DB/OL]. (2019-05-10)[2020-11-12]. <https://github.com/Joel-Q-Xu/MT3-mysterytwisterc3> |