|  |
| --- |
| **Github账号：Nora-Qiu** |
| **实验摘要：**  题目提供了一条经过AES加密，使用初始零向量和01-00填充的CBC模式 的消息。同时提供了能求出相应的密钥的字符串，但这个字符串并不完整。  实验目的是找到已给密文的明文。  实验分为三个步骤：  一、**求出传输过程中丢失的字符？**  **二、求密钥KENC**  **三、求出明文** |
| **实验题目**  题目提供了一条经过AES加密，使用初始零向量和01-00填充的CBC模式 的消息。同时提供了相应的密钥，但这个密钥并不完整。  实验目的是找到已给密文的明文。  基于基本访问控制(Basic Access Control, BAC)协议的密钥KENC被生成并应用。为了解密，已经传输了以下字符，从中可以导出KEN:  12345678<8<<<1110182<111116?<<<<<<<<<<<<<<<4  在传输过程中一个字符丢失了，并用?表示。为了求得KENC需要使？再次可现。经过AES加密的消息包含一个要作为解决方案输入的词。  **通过题目中所给的参考资料计算得到KENC并解密以下64编码的明文：**  9MgYwmuPrjiecPMx61O6zIuy3MtIXQQ0E59T3xB6u0Gyf1gYs2i3K9Jx aa0zj4gTMazJuApwd6+jdyeI5iGHvhQyDHGVlAuYTgJrbFDrfB22Fpil2N fNnWFBTXyf7SDI |
| **实验内容**  **根据题目信息，为了求出KENC并解得明文，按照以下步骤进行实验：**  **一、求出传输过程中丢失的字符？**    **根据[1]中给出的字符编码类型表可以确定已传输字符串中的？是第28位，为22到27位的校验位。**    **根据[2]中所给的信息，得到求出？值的方法：校验位用模10重复加权731 731…**  **步骤1：从左到右依次把数据中的元素和对应位权数相乘。**  **步骤2：把他们相乘的结果相加**  **步骤3：把相加和除以10**  **步骤4：余数为校验位数**  **代码实现如下：** |
| **可得？=7**  **完整的字符串为：**12345678<8<<<1110182<1111167<<<<<<<<<<<<<<  **二、求密钥KENC**    **根据[3]中的信息可知道，MRZ\_information的sha-1哈希散列中16字节被用作密钥种子，并用以下密钥派生机制来产生密钥。**  **求密钥种子K\_seed代码：**      **根据[4]可知，通过密钥种子K\_seed计算得出的两个3DES密钥被用来建立KENC。**  **函数KDF**（K，1）**在9.7.1中给出** |
| **KDF函数输入共享密钥K\_seed和一个32位的整数计数器，输出八位字节的数据串。**  **具体步骤如下：**  **步骤1：K\_seed和计数器c级联**  **步骤2：对级联结果用SHA1加密（这里要求哈希函数的位长大于或者等于产生密钥的长度）**  **步骤3：输出8位字节串keydata**  **生成keydata代码如下**      **两个3DES密钥通过如上方式得出：**   * **KDF函数输出的八位字节串1到8字节用来生成K\_A，9到16字节用来生成K\_B，其余的字节不被使用。** * **调整K\_A和K\_B的奇偶校验位生成正确的DES密钥** |
| **三、求出明文**  **因为所给的消息是base64加密的，所以要先对其base64解码：**    **最后用密钥解密就得到明文啦**    **运行结果是：**    **但令人遗憾的是，当我在MTC3网站输入解得的明文后显示**  **不知道我的问题出现在哪里** |
| **实验总结**  **刚开始做的时候google到了英文版的参考资料，但是没有找到解密的示例。代码慢悠悠写完之后发现结果完全不对，以下是几个我犯错的地方：**  **①把K\_seed和计数器级联之后没有转换成ASCii编码的字符串，在MTC论坛上看到有相关提问于是改了过来**    **②对MRZ\_information选择错了，一开始以为是完整的字符串12345678<8<<<1110182<1111167<<<<<<<<<<<<<<4，后来在论坛看到应该选择护照信息第二行，删除国家的3位数字和性别的1位数字，并且最后一位应该是2**    **结果还是不对，看到同学的中文参考资料才知道应该只用前28位并删除国家的3位数字和性别的1位数字。正确的MRZ\_information是12345678<811101821111167**  **后来为了检查仔细是否还遗漏了信息，再看了一遍英文参考资料，发现其实在说明K——seed如何得到的段落中明确说了MRZ\_information由证件号码，出生日期以及到期日构成。**  **③题目中说了加密的消息包含一个要作为解决方案输入的词。所以应该输入的是单词** **Kryptographie**    **如果根据参考资料步骤进行解题，过程应该是相当清晰的。由于自己的疏忽，在求密钥种子种子那里浪费了相当长时间，以后一定仔细读题和文献！** |
| **参考文献**   * [**https://www.mysterytwisterc3.org/en/mtc3forum/viewtopic.php?f=5&t=217&start=10**](https://www.mysterytwisterc3.org/en/mtc3forum/viewtopic.php?f=5&t=217&start=10) * [**https://www.icao.int/publications/Documents/9303\_p11\_cons\_en.pdf**](https://www.icao.int/publications/Documents/9303_p11_cons_en.pdf) * [**https://www.icao.int/publications/Documents/9303\_p3\_cons\_en.pdf**](https://www.icao.int/publications/Documents/9303_p3_cons_en.pdf) |