# 应用密码学

对称加密

姓 名： 陈四贵

学 号： 182210710119

班 级： 1822107101

学 院： 计算机学院

### 一、实验目的

1、理解对称加密算法的原理和特点。

2、理解DES算法以及AES的加密原理

### 二、实验原理

DES是一种分组加密算法，所谓分组加密算法就是对一定大小的明文或密文来做加密或解密动作。而在DES这个加密系统中，每次加密或解密的分组大小均为64位，所以DES没有密文扩充的问题。对大于64位的明文只要按每64位一组进行切割，而对小于64位的明文只要在后面补“0”即可。 另一方面，DES所用的加密或解密密钥也是64位大小，但因其中有8个位是用来作奇偶校验的，所以64位中真正起密钥作用的只有56位，密钥过短也是DES最大的缺点。 DES加密与解密所用的算法除了子密钥的顺序不同外，其他部分完全相同。

AES加密过程是在一个4×4的[字节](https://baike.baidu.com/item/%E5%AD%97%E8%8A%82)矩阵上运作，这个矩阵又称为“体（state）”，其初值就是一个明文区块（矩阵中一个元素大小就是明文区块中的一个Byte）。（Rijndael[加密法](https://baike.baidu.com/item/%E5%8A%A0%E5%AF%86%E6%B3%95)因支持更大的区块，其矩阵行数可视情况增加）加密时，各轮AES加密循环（除最后一轮外）均包含4个步骤：**AddRoundKey****, SubBytes****, ShiftRows****, MixColumns**。

### 三、实验设备

Windows 台式机

### 四、实验步骤

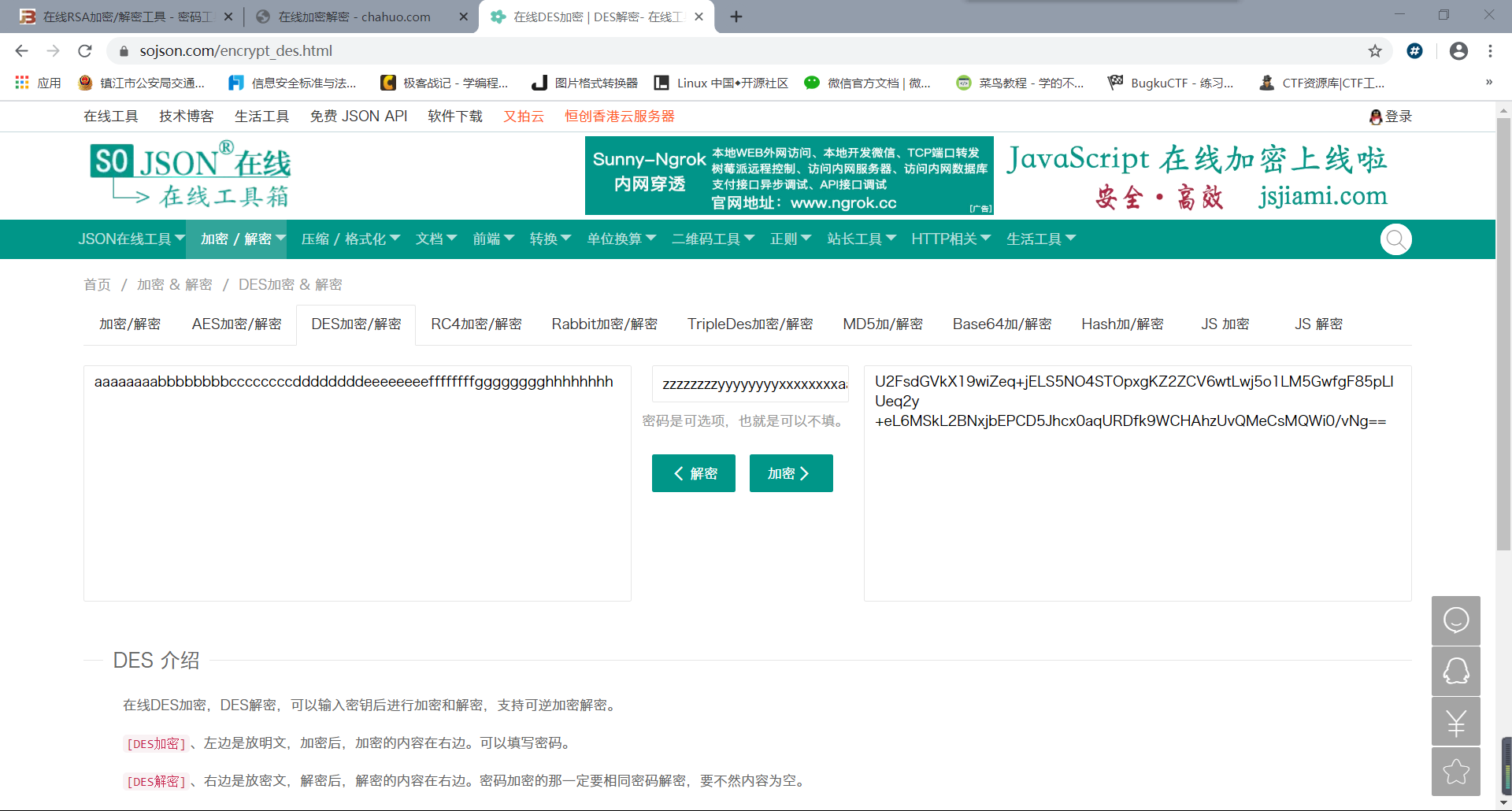
尝试DES与AES的加密与解密过程，并附上程序截图。

1. DES加密与解密过程：

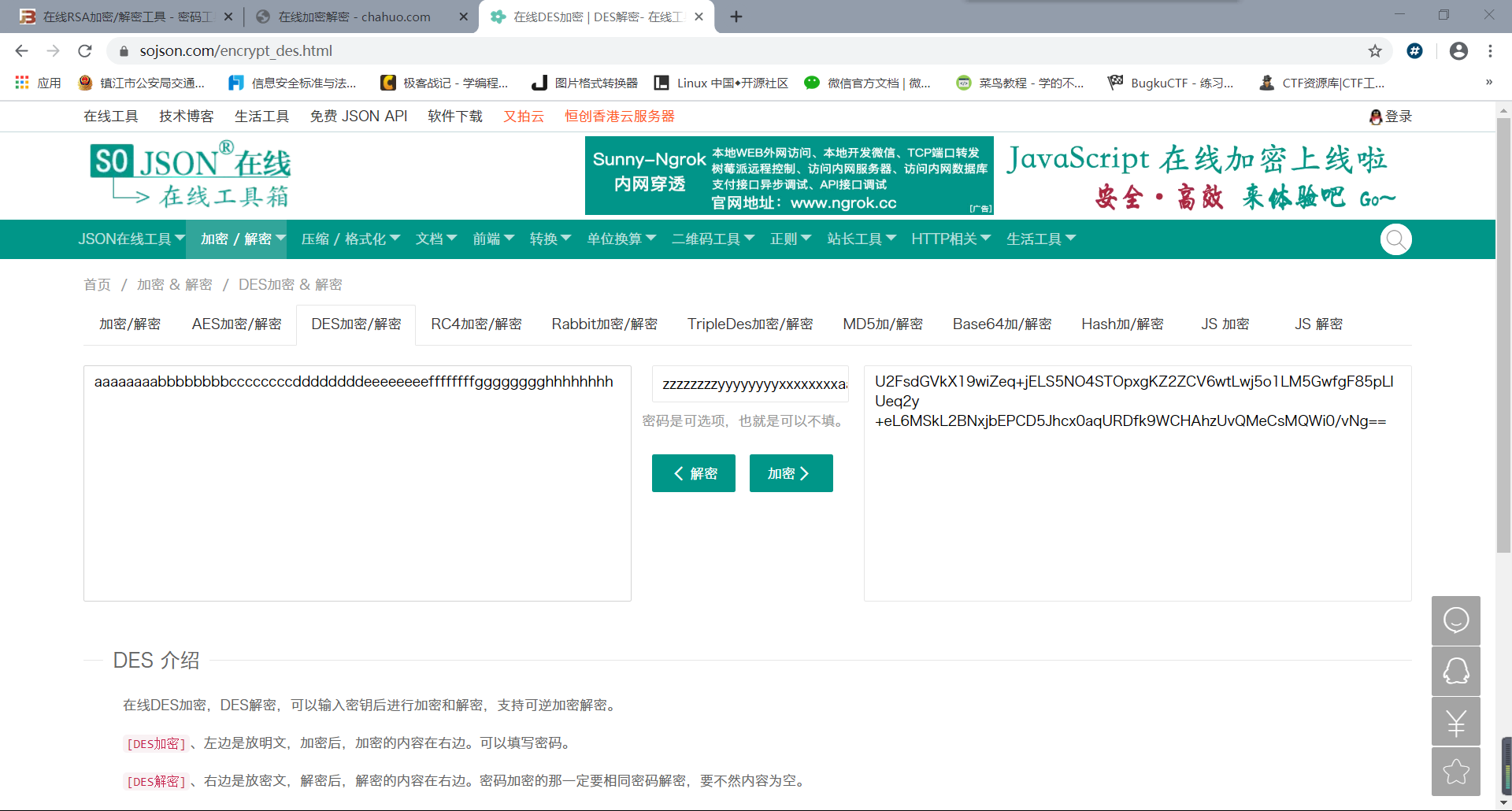
选取明文：aaaaaaaabbbbbbbbccccccccddddddddeeeeeeeeffffffffgggggggghhhhhhhh

密钥：zzzzzzzzyyyyyyyyxxxxxxxxaaaaaaaabbbbbbbbccccccccddddddddeeeeeeee

加密之后的密文截图：



解密截图：

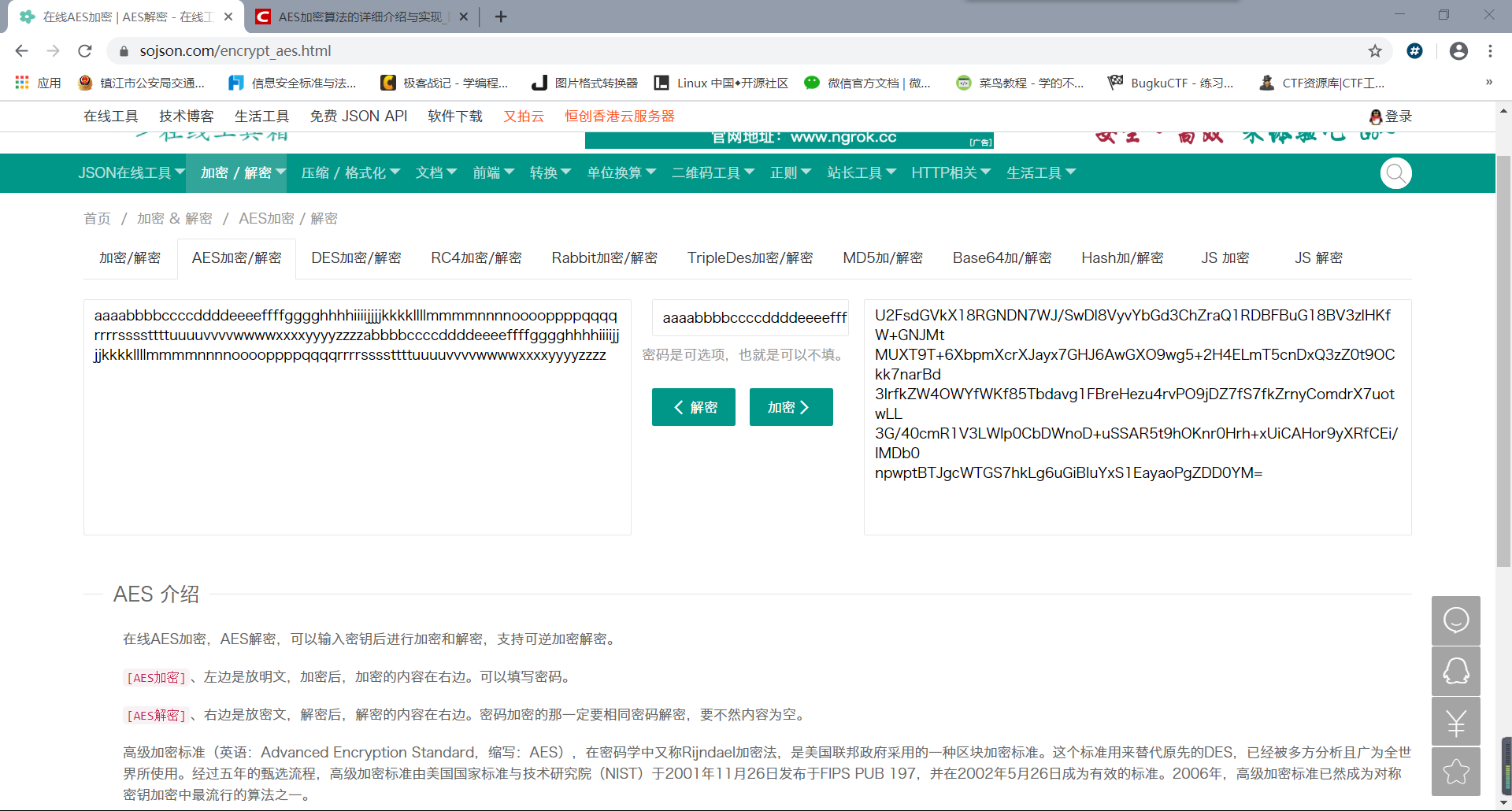


1. AES加密与解密过程：

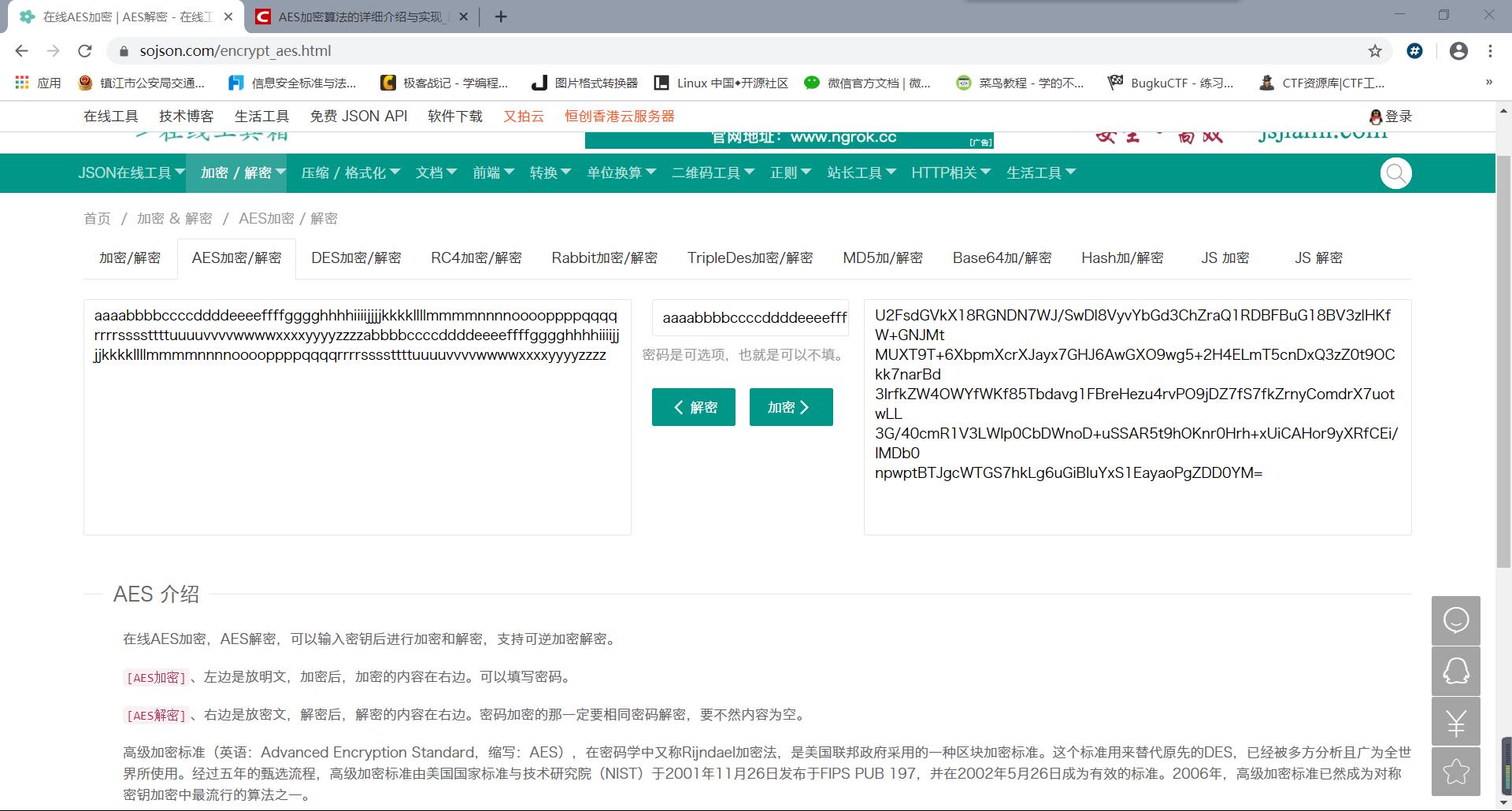
选取明文：aaaabbbbccccddddeeeeffffgggghhhhiiiijjjjkkkkllllmmmmnnnnooooppppqqqqrrrrssssttttuuuuvvvvwwwwxxxxyyyyzzzzabbbbccccddddeeeeffffgggghhhhiiiijjjjkkkkllllmmmmnnnnooooppppqqqqrrrrssssttttuuuuvvvvwwwwxxxxyyyyzzzz

密钥：aaaabbbbccccddddeeeeffffgggghhhhiiiijjjjkkkkllllmmmmnnnnooooppppqqqqrrrrssssttttuuuuvvvvwwwwxxxxyyyyzzzzabbbbccccddddeeeeffffgggghhhhiiiijjjjkkkkllllmmmmnnnnooooppppqqqqrrrrssssttttuuuuvvvvwwwwxxxxyyyyzzzz

加密之后的密文截图：



解密截图：



### 五、实验心得

1.对对称密码而言，只要密钥不变，那么由明文加密得到密文与由密文解密得到明文的过程是可逆的。一旦密钥泄露，密码破译人员便可追本溯源，获取明文。因而密钥至关重要，不可泄露。

2.对某些加密/解密算法而言，即使是同一密文，也可能是不同的明文+不同的密钥组合加密的结果，这个可能的情况往往很多，但是一旦知晓密钥，就很容易破解密文。因而，保证密钥不泄露是很有必要的。