

## 第一关：

The image shows a web interface for AES encryption. The title is 'AES加密'. It has three input fields: '请输入加密/解密的内容' with the value '0110000111101111', '请输入密钥' with the value '1111000001011010', and '结果展示' with the value '加密结果: 0011110110100110'. Below these are three radio buttons for '一重加密' (selected), '二重加密', and '三重加密'. At the bottom, there are three buttons: '加密', '解密', and '密钥破解'. Below these buttons are three labels: '字符加密', '字符解密', and 'CBC'. The background is dark with binary code and a padlock icon.

## 第二关： 交叉测试

经过作业表格提供的链接上的部分组进行交叉测试得到的结果与Lucas组等一样，通过检验。

## 第三关：扩展功能：

加密字符串 **Hello, world!** 得到输出，  
而后对输出进行解密得到原字符串。可以正常加密解密。  
此处代码中使用了**UTF-8**编码，解决了乱码无法解密的问题。



## 第四关：多重加密：

### 1.双重加密：



### 2.中间相遇攻击：

两组数据为上一问给出的示例

1100110011001100    1111011000001001  
 1110101011110000    1111011011110001



恰好破解出来只有二个密钥如下，正好有一个密钥与给定密钥相同。



**3.三重加密：48bit密钥输出，加密解密正常。**



