信息安全原理 PJ1-1
6轮DES加密／解密——CBC模式

14307130318
刘超颖

一、开发工具

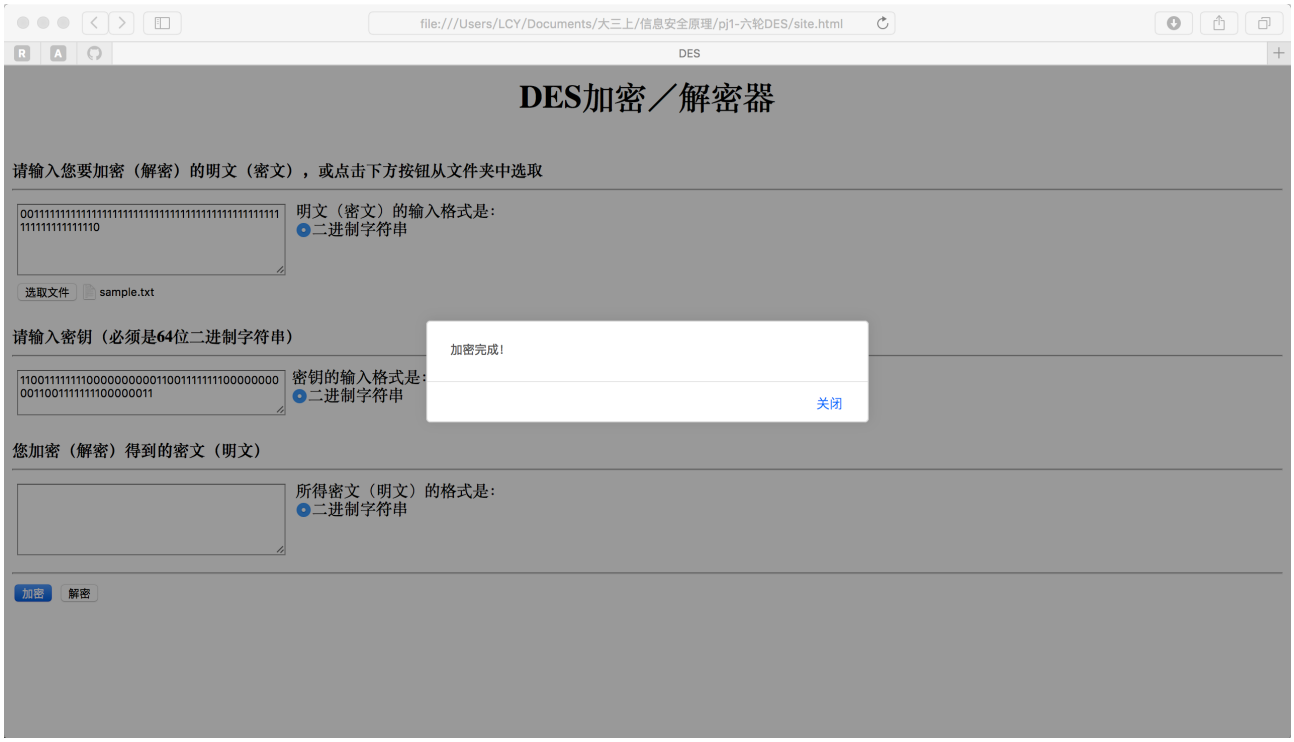
使用HTML和JavaScript实现了CBC模式的6轮DES加密／解密。

二、使用说明

本应用提供根据DES算法CBC模式的六轮加密／解密服务，可通过手动输入／文件导入明文（密文），手动输入密钥，点击加密（解密）按钮，得到对应的密文（明文）。

1. 点击site.html打开应用网页。（注意：网页的编码方式须是GB18030，否则页面上的中文会出现乱码！）

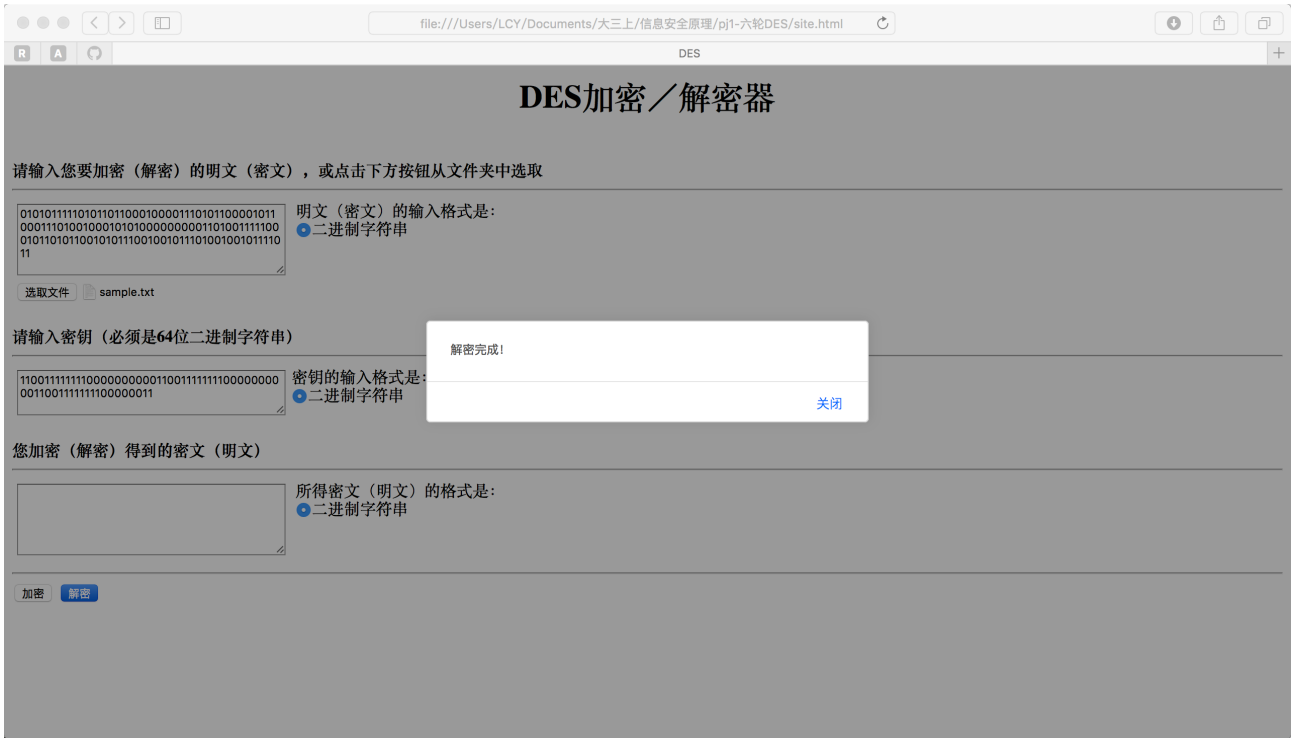
2. 在页面中的第一个文本框中输入明文文本，或点击选取文件选择明文文件，然后输入密钥，点击加密按钮。（可以看到三个文本框右边有输入格式和显示格式的选项按钮，目前不用对这几个按钮作任何勾选，按钮的设定是为了日后加入更多的加／解密模式，如：英文字符串的加／解密、十六进制字符串的加／解密等，目前网页只提供二进制字符串的加／解密）



在点击加密按钮之后，会如上图跳出“加密完成”的弹窗，点击“关闭”弹窗，则能在第三个文本框内看到加密出来的密文结果。

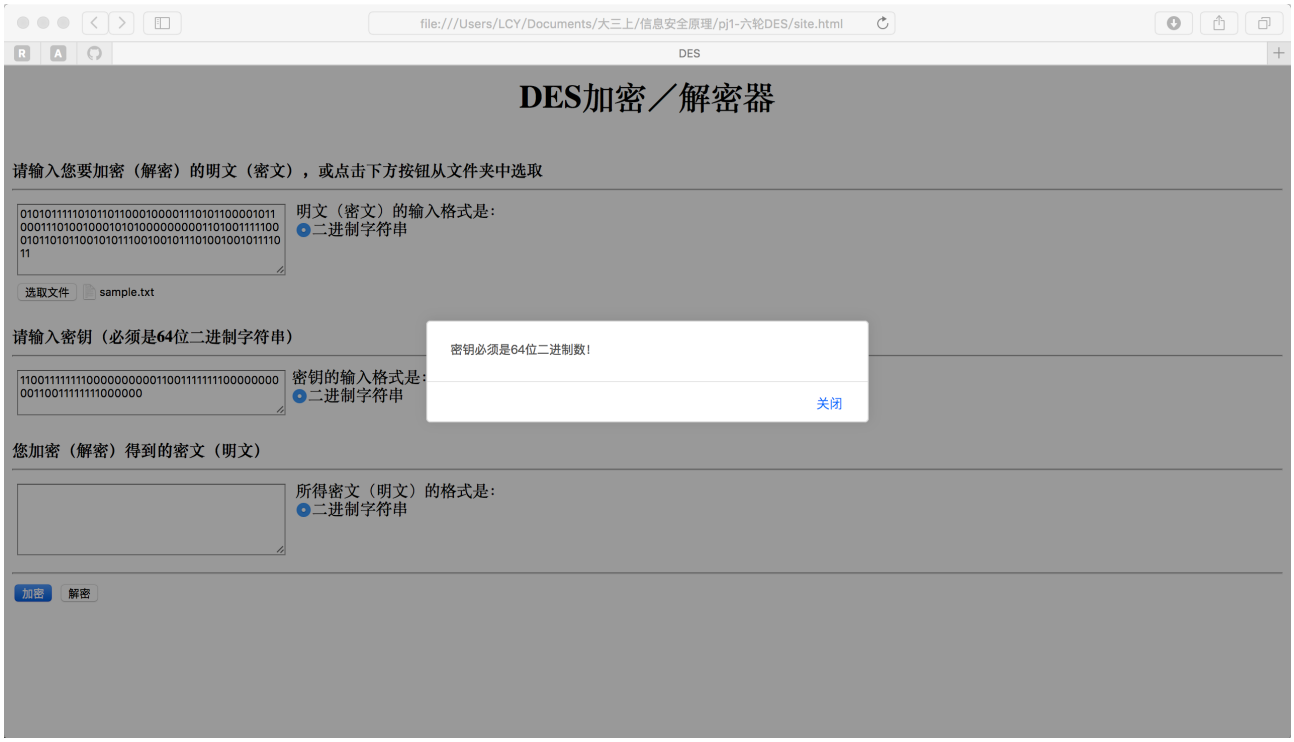
由上图可以看到，输入的明文是一个64位的二进制文本，而输出的密文文本却变成了128位二进制文本，这是因为CBC加密模式的补全系统，这一点会在后文中作出解释。

3. 解密操作同理于加密，在页面中的第一个文本框中输入密文文本，或点击选取文件选择密文文件，然后输入密钥，点击解密按钮。结果如下图：

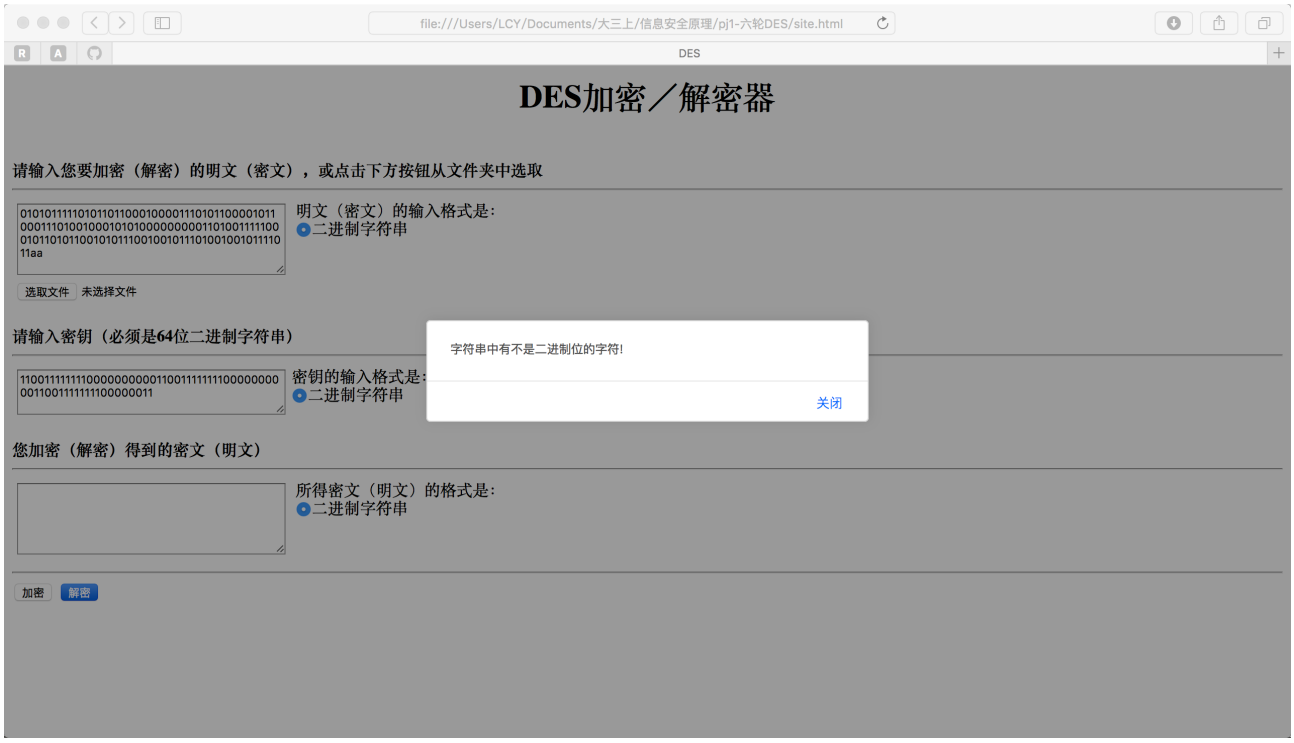


在点击解密按钮之后，会如上图跳出“解密完成”的弹窗，点击“关闭”弹窗，则能在第三个文本框内看到解密出来的明文结果。

4. 需注意，密钥的输入必须是64位二进制字符串，如果输入与64位二进制字符串不符，则会跳出以下弹框提示用户，并无法继续加密。



5. 需注意，密钥和明文（密文）的输入必须是二进制字符串，如果输入字符串中含有非“0”且非“1”的字符，则会跳出以下弹框提示用户，并无法继续加密。



三、设计过程

1. 理解DES加密 / 解密的工作机制，实现基本的64位二进制字符串的DES加密 / 解密。此处需注意的是，DES加密的最后一轮，也即第6轮中，最后L和R不需要进行交换。通过加、解密的对称性，不难推出，在DES解密的第一轮中，一开始L和R也不需要进行交换。
2. 编写DES加密过程的JavaScript代码和网页前端的HTML代码。测试DES加、解密的正确性。将A字符串作为明文，B字符串作为密钥分别输入文本框，点击“加密”按钮，得到加密结果密文C字符串；然后将C字符串作为密文，B字符串作为密钥分别输入文本框，点击“解密”按钮，得到解密结果明文字符串，将其与A对比，验证加、解密的对称性。
3. 在已编写的DES加密算法中加入CBC模式。

1）加入填充机制，支持非64位二进制字符串的加密 / 解密。关于字符串的输入，如果输入明文（密文）的位数不是64的整数倍，则在后面用随机数补全空余位数，最后8位作为填充指示符，表示填充占有的位数（bit数）（注意：此处不表示填充的字节数！）；如果输入明文（密文）的位数是64的整数倍，或不到56位不够留出8位的填充指示符，则在字符串后多连接一个64位的字符串，其中56位是随机填充位，最后8位作为填充指示符，用于表示填充了7个字节。（64位整数倍位数字符串的填充是为了保持填充机制的统一性，保证每个经过填充的字符串的最后8位都是填充指示符，以免造成歧义）。

2）实现CBC模式加 / 解密。在加密过程中，每一组明文要和前一组的加密结果密文进行抑或运算后，形成一个新的明文，再对新的明文进行加密；根据对称性，在解密过程中，每一组密文要先经过解密，将解密所得到的明文再与前一组的密文进行抑或运算后（根据以下公式），得到原本的明文。

$$(A \oplus B) \oplus B = A \oplus B \oplus B = A$$

3）实现解密后结果无效位的去除。在解密过程中，解密后所得的明文的末尾8位表示填充无用数字的字节数，通过这一信息，将末位随机填充的无用数字去除后，再将明文结果输出。

四、其他

1. 在本实验中，将初始向量IV默认设置为“0000000000000000000000000000000000000000000000000000000000000000”，也可通过对代码的修改实现对初始向量IV的修改。见代码：

```
//初始向量值，可修改
var IV = new Array(-1,
    0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
    0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
    0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
    0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0);
```

2. 在代码中，一律不考虑数组X[0]，所有X[0]置-1，从X[1]开始计算。
3. 文件夹中，encryption_sample1对应的加密结果是decryption_sample1，encryption_sample2对应的加密结果是decryption_sample2，且均可逆。密钥为：1100111111110000000000110011111111000000000011001111111100000011。

五、参考资料

1. https://en.wikipedia.org/wiki/DES_supplementary_material
2. https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation#CBC