软件设计报告

李嘉博

目录

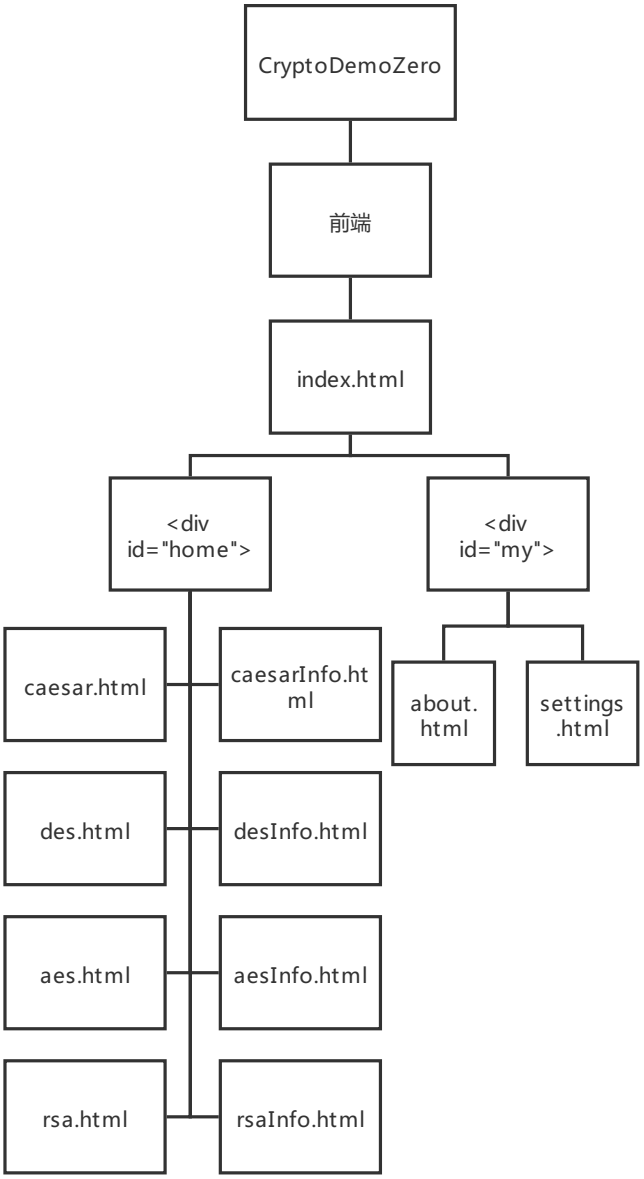
1 设计目的

本系统旨在展示多种加密算法的细节及其具体原理，方便密码学相关的教学、学习工作。

2 使用技术

本项目为HTML5+ App，界面使用MUI开发，其他部分使用HTML+CSS+JS实现，主要算法采用JavaScript结合第三方JS库实现。 由于本程序不涉及用户注册登录，唯一的需要进行数据存储的壁纸更换采用了JavaScript的localStorage实现。

3　系统总体设计


CryptoDemoZero
前端
index.html

caesar.html
caesarInfo.html
about.html
settings.html
des.html
desInfo.html
aes.html
aesInfo.html
rsa.html
rsaInfo.html

4 模块设计

4.1 index.html

index.html分为2个页面，通过MUI的div方式来区分，分别是 和 。

4.1.1 “首页”div

“首页”div提供各种加密算法演示页面的入口，通过二级列表的方式来展示各种概念之间的层次结构。

4.1.2 “我的”div

“我的”div中，具有关于页面的入口和设置页面的入口，同样通过列表的方式展示。

4.2 简单替换密码

本部分只有1种加密算法，即凯撒密码。在凯撒密码中，只支持26个英文字母的加密，加密过程也仅仅是将其以统一的偏移量进行偏移， 因此界面比较简单。

4.3 对称密码

本部分有2种加密算法，DES（Data Encryption Standard）和AES（Advanced Encryption Standard）。这两种都是对称加密算法， 因此界面也比较简单，仅有设置密钥、加密、解密功能。

4.4 公钥密码

本部分虽然只有1种加密算法：RSA算法，但由于是非对称加密，因此涉及的功能非常多，总体分为发送者、数字证书、接受者3大部分。 发送者、接受者可以生成其密钥对、选择摘要算法、生成各种摘要、加密、解密、签名、验签（其中验签部分暂未实现）。 数字证书部分模拟了只有1层证书的情况，没有模拟实际算法中多层证书的情况，但也具有生成CA（证书颁发机构）密钥对、签名、验签、摘要等功能。

4.5 壁纸替换

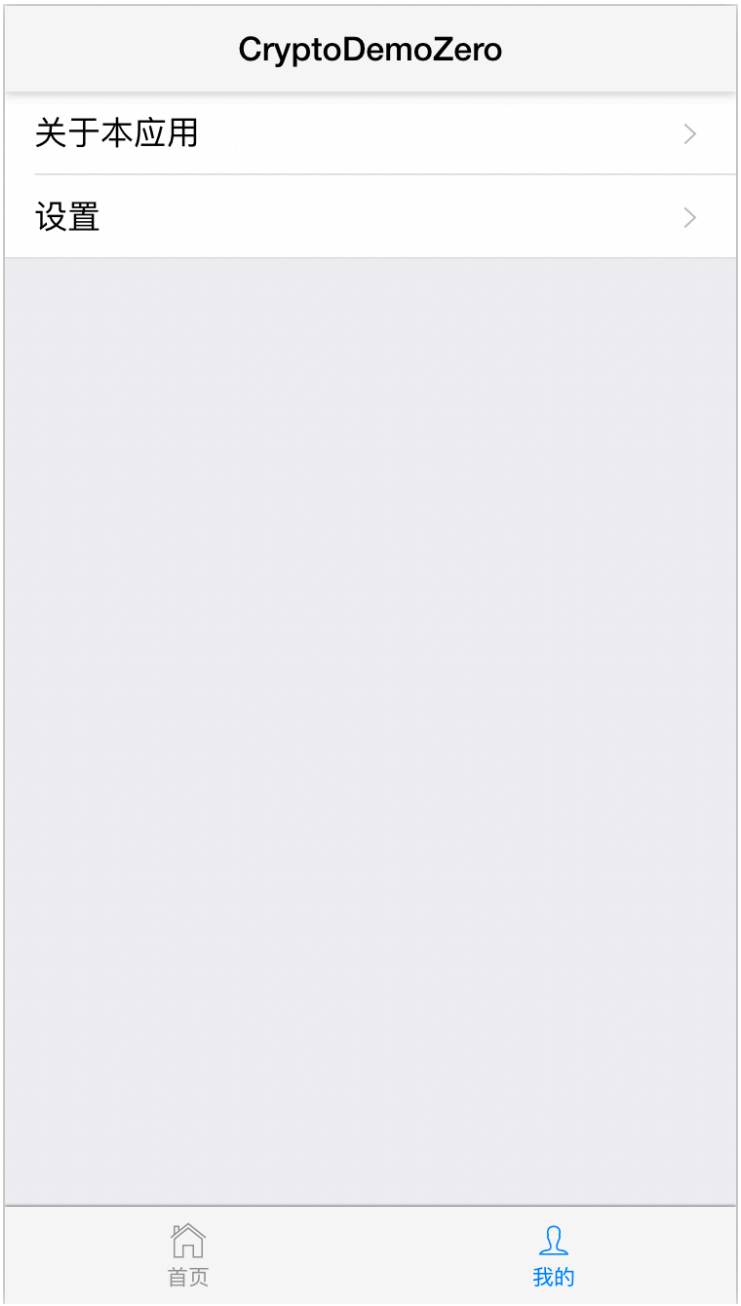
本部分对应源文件中的settings.html，暂时只有更换壁纸的功能。

5　界面设计

5.1　index.html

5.1.1　“首页”div

5.1.2 “我的”div



5.2　凯撒密码


凯撒密码介绍
在密码学中，恺撒密码（英语：Caesar cipher），是一种替换加密的技术，明文中的所有字母都在字母表上向后（或向前）按 照一个固定数目进行偏移后被替换成密文。例如，当偏移量是3的时候， 所有的字母A将被替换成D，B变成E，以此类推。这个加密方法是以罗 马共和时期恺撒的名字命名的，当年恺撒曾用此方法与其将军们进行联系。 （摘自百度百科，有改动）

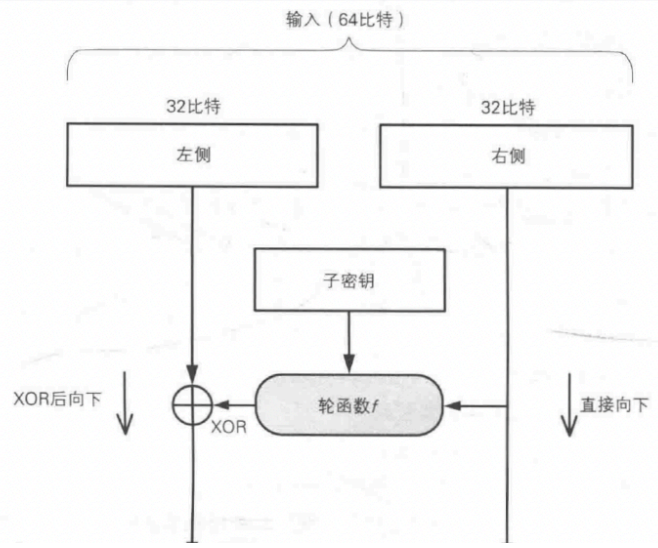
5.3 DES

DES算法介绍

DES（Data Encryption Standard，数据加密标准），是一种使用密钥加密的块算法，分组加密算法，1977年被美国联邦政府的国家标准局确定为联邦资料处理标准（FIPS），并授权在非密级政府通信中使用，随后该算法在国际上广泛 流传开来。需要注意的是，在某些文献中，作为算法的DES 称为数据加密算法（Data Encryption Algorithm,DEA），已与作为标准的DES区分开来。（摘自百度百科，有改动）

算法原理：

将数据分为64比特的组，每组单独加密。如果 要加密的明文较长，就要对DES加密进行迭代，而迭代的具 体方式称为模式。DES的基本结构称为Feistel网络，在Feistel网络 中，加密是多轮的循环。DES是一种16轮循环的Feistel网络。



5.4 AES


AES算法介绍
AES（Advanced Encryption Standard，高级加密标准）， 又称Rijndael加密法，是美国联邦政府采用的一种区块加密标准。
这个标准用来替代原先的DES（Data Encryption Standard）， 已经被多方分析且广为全世界所使用。经过五年的甄选流程， 高级加密标准由美国国家标准与技术研究院 （NIST）于2001年 11月26日发布于FIPS PUB 197，并在2002年5月26日成为有效 的标准。2006年，高级加密标准已然成为对称密钥加密中最流行 的算法之一。
该算法为比利时密码学家Joan Daemen和Vincent Rijmen所设计， 结合两位作者的名字，以Rijdael之名命之，投稿高级加密标准的 甄选流程。（Rijdael的发音近于 "Rhine doll"。） （摘自百度百科，有改动）

5.5 RSA

RSA算法介绍

RSA是1977年由罗纳德·李维斯特（Ron Rivest）、阿迪·萨莫尔（Adi Shamir）和伦纳德·阿德曼（Leonard Adleman）一起提出的。当时他们三人都在麻省理工学院工作。RSA就是他们三人姓氏开头字母拼在一起组成的。（摘自百度百科，有改动）

算法原理：

1.简介

RSA是一种非对称加密算法，发送方（A）、接收方（B）都有自己的公钥和私钥。

2.加密解密

A给B发送时，A使用B的公钥加密，B收到后使用自己的私钥解密。

3.数字签名

为了保证发送者确实是A，A需要用自己的私钥进行签名。签名的过程实际上就是用私钥对原文的摘要进行加密（不对原文进行签名是为了防止被公钥直接解密）。B收到后，用A的公钥进行验签，与自己解密出的原文计算出的摘要进行对比。

4.数字证书

在此过程中，A需要将自己的公钥分发给B，为了防止它被篡改，需要有一个证书颁发机构（CA）对其进行签名，这就是数字证书。而CA的公钥也要进行这一过程，所以通常证书有一个分层结构，上级CA又对这个证书进行签名。而最高一级的证书就是根证书，它的颁发机构就是根证书颁发机构（Root CA），通常是由操作系统内置的，不能随意修改。

5.6 settings.html