# 综合设计报告

**课程名称： Web前端技术开发**

**设计名称：基于HTML的密码学介绍界面**

**设计组名： 绝不动摇组**

**成员及分工：**

|  |  |  |  |
| --- | --- | --- | --- |
| **班级** | **姓名** | **学号** | **分工及贡献度** |
| **网安201** | **朱传伟** | **2020015540** | **100%** |
|  |  |  |  |
|  |  |  |  |

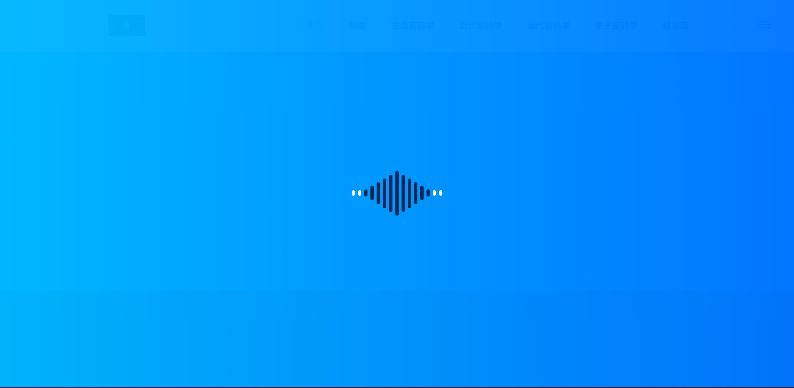
1. **应用意义**

本项目可以对密码学类各类知识进行初步介绍，并对密码学发展的前世今生有了一定的解释，可以让人更好地了解密码学的发展历史和状态。对每一个阶段的密码学的经典算法进行了一定的介绍和讲解。对密码学的各种知识进行汇总和介绍，我觉得是十分有意义的，这可以让我们更加清楚的了解密码学和其发展历程，对密码学有较为全面和总体的了解，可以更加了解密码学为什么要更新和替换所带来的问题等有更加深刻的认识。帮助我们在使用网站和其他工具的时候，借助密码学中的知识来完善我们的密码验证手段，还可以初步查询网站和工具的安全性等等。

1. **功能描述**

本Web大作业是由HTML+CSS+JS编写而成的，由几个不同的HTML界面组成，主要介绍了密码学简介和古典密码学、近代密码学、现代密码学和量子密码学几个部分。古典密码学、近代密码学、现代密码学和量子密码学每个部分简介都在index文件上，可以点击进入对应的HTML界面，每个界面都列举了几种较为经典的密码方案，可以粗略地介绍了几种经典的密码学方案。最后还有发送邮件的界面和说明。

对于界面本身来说，有预加载可以优化观看等待体验；



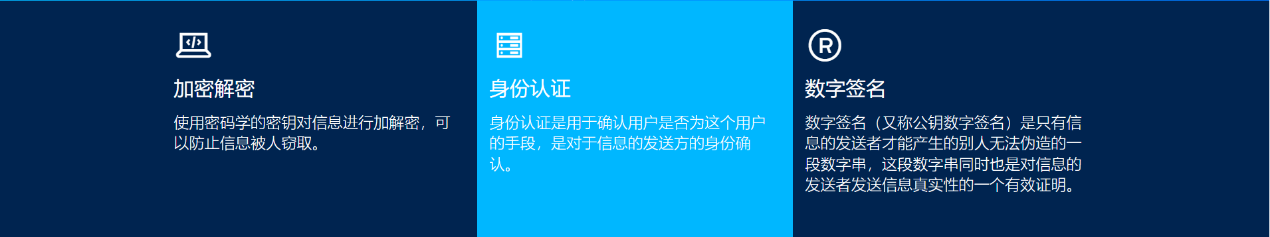
最上方的导航栏和右上角的菜单导航栏是一直存在的，可以更加便捷的访问相映的网页部分；



背景图有JS优化效果，更加美观和富有科技感，左右分栏，图文并茂，看着舒服，等待一定时间后从左右同时划出。文字部分是对密码学的定义简介；



分三栏概述密码学最重要的三个作用，移动上去变色，图片也会变，出现时从左往右依次从小变大出现，更美观和具有互动性；



有视频和文字配合，视频课放大缩小、改变声音、暂停等，文字配备滚轮可适应多文字阅读，出现时两边移动出现，深化对密码学的了解和印象；



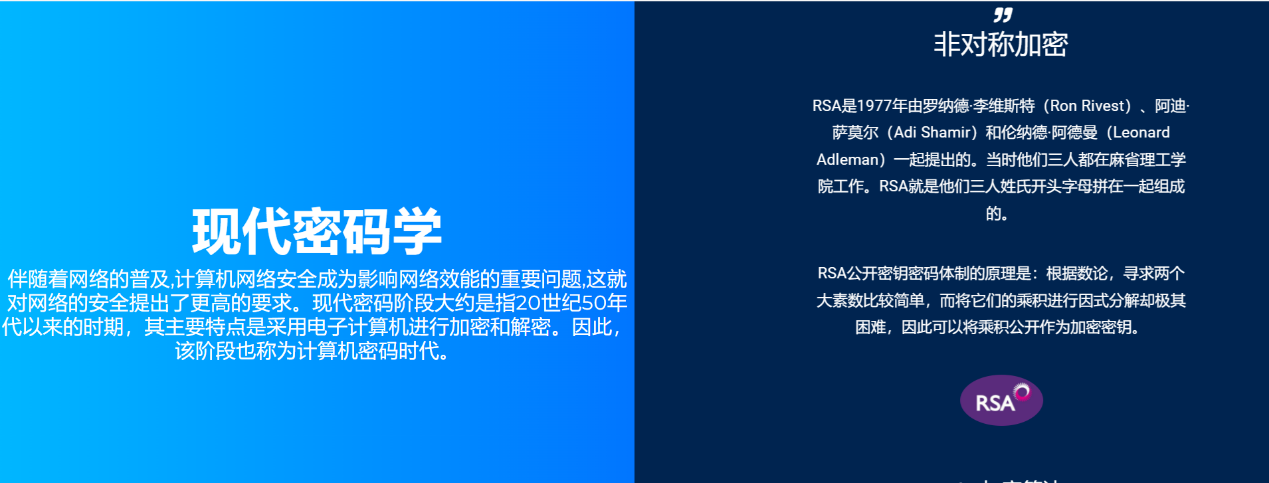
有官方的明确的信息泄露的损失和增长率，出现采用跳动出现（会弹一弹很可爱的感觉），百分比是从0开始到指定值，图文并茂，加深对信息安全的重视；



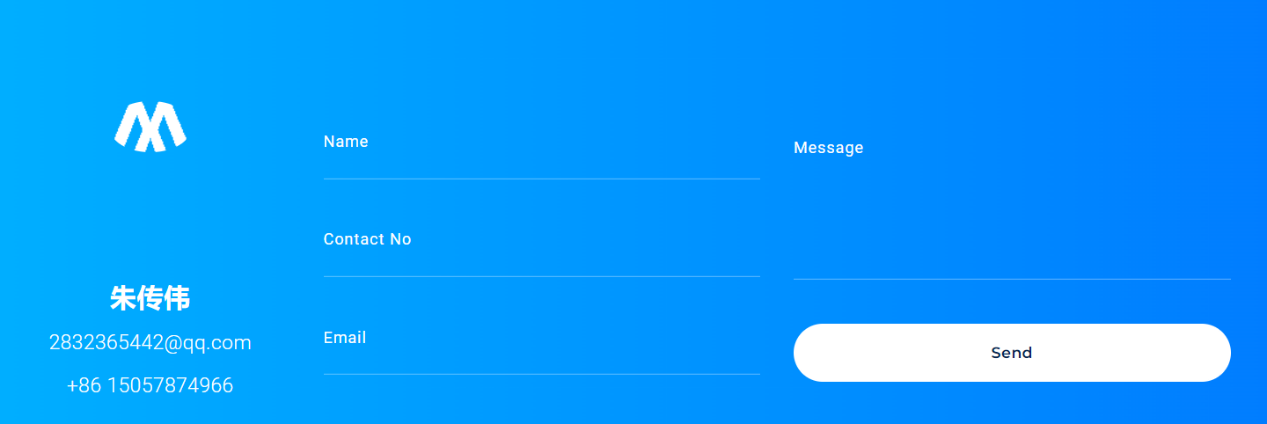
多个链接文件，鼠标移动到上面会变色，出现顺序自上而下是从下到上移动、两边向中间移动，补充密码学知识；



轮播图，加深印象和扩大内容范围等等。



结尾有相关信息和发送界面，点击Send会跳转到微软的发送邮件的功能上



1. **设计方案和结构分析**

**设计方案：**

**设计背景：**随着现代通信技术的发展和迅速普及，特别是随着通信与计算机技术发展而诞生的计算机互联网络全面进入千家万户，信息的共享和应用日益广泛与深入，世界范围的信息革命激发了人类历史上活跃的生产力，但同时也使得信息的安全问题日渐突出而复杂。从大的方面来说，信息安全问题已威胁到的政治、经济军事、文化、意识形态等领域。因此，很时就有人提出了“信息战”的概念并将信息武器列为继原子武器、生物武器、化学武器之后的第四大武器。从小的方面来说，信息安全问题也是人们能否保护自己个人隐私的关键。

当今社会信息泄露和隐私安全问题空前严峻，个人信息安全得不到保障，企业信息安全千疮百孔，甚至是国家的信息安全问题都得不到较好地解决。据官方报道，每年在国内外由于信息泄露所造成的经济损失都高达数千万美元，仅2020年一年全球数据泄露的平均损失成本为1145万美元，2019年数据泄露事件达到7098起，涉及151亿条数据记录，比2018年增幅284%，在明面上的显然是冰山一角，暗地里的信息泄露问题和危害将数倍百倍于统计报告。而且，最大的损失并不是直接经济损失，而是后续的由于信息泄露产生的各种负面效益。

与信息泄露问题不断加深相适应的是，各国都出台了信息安全方面的法规和政策，国内外很多大企业都开始了信息安全产品的开发和研究，我国近几年在不断加强对信息安全的保护和贩卖泄露信息的打击，出台了多项法律法规。作为普通人我们也应该适当学习一些密码学相关知识，以求更好的保护个人信息。

对于个人而言，我们无法解决部分国家和部分组织对我们的信息进行攻击的态度和实际行动。我们能做的只有加强自身信息安全的素养和筛选合适的网站进行使用，其中筛选有无安全的网站是比较困难的，他们会做各种的伪装和欺骗，而我们大部分人一没技术和专业工具去辨别这些网站和其他什么东西，二没精力和时间去一个个辨别，毕竟大部分人都是有需求了才去使用各种网站和工具，所以我们能做的基本上只有加强自身信息安全保护意识，在信息安全的保护中包括合理使用电脑、不访问不良网站和加强个人信息保护等，其中合理使用电脑就是要下载安装杀毒软件，关闭不必要的端口和服务什么的，这些我们只要会用就好也改不来，不良网页上经常会有病毒等东西存在，只有加强信息保护是我们能稍微做一做的。世界上很多的信息泄露都是由于某个公司或者是数据服务被攻破造成的，其中安全的密码学体系可以在一定程度上防止攻击成功的可能性，可以保障在语义上是基本安全的。

密码学是研究如何隐密地传递信息的学科。在现代特别指对信息以及其传输的数学性研究，常被认为是数学和计算机科学的分支，和信息论也密切相关。著名的密码学者Ron Rivest解释道：“密码学是关于如何在敌人存在的环境中通讯”，自工程学的角度，这相当于密码学与纯数学的异同。密码学是信息安全等相关议题，如认证、访问控制的核心。密码学的首要目的是隐藏信息的涵义，并不是隐藏信息的存在。密码学也促进了计算机科学，特别是在于电脑与网络安全所使用的技术，如访问控制与信息的机密性。密码学已被应用在日常生活：包括自动柜员机的芯片卡、电脑使用者存取密码、电子商务等等。

密码是通信双方按约定的法则进行信息特殊变换的一种重要保密手段。依照这些法则，变明文为密文，称为加密变换；变密文为明文，称为脱密变换。密码在早期仅对文字或数码进行加、脱密变换，随着通信技术的发展，对语音、图像、数据等都可实施加、脱密变换。

密码学是在编码与破译的斗争实践中逐步发展起来的，并随着先进科学技术的应用，已成为一门综合性的尖端技术科学。它与语言学、数学、电子学、声学、信息论、计算机科学等有着广泛而密切的联系。它的现实研究成果，特别是各国政府现用的密码编制及破译手段都具有高度的机密性。

在我国，信息网络安全研究历经了通信保密、数据保护两个阶段，正在进入网络信息安全研究阶段，现已开发研制出防火墙、安全路由器、安全网关、黑客入侵检测、系统脆弱性扫描软件等。作为信息安全关键技术的密码学，近年来空前活跃，1976 年美国学者提出的公开密钥密码体制，克服了网络信息系统密钥管理的困难，同时解决了数字签名问题，它是当前研究的热点。而电子商务的安全性已是当前人们普遍关注的焦点，目前正处于研究和发展阶段，量子密码、DNA 密码、混沌理论等密码新技术正处于探索之中。

**设计灵感：**本Web大作业是根据当今社会的信息安全和密码学这两个热点来的灵感，刚好密码学方面没有什么科普性质的或者是总结性质的网站，并且为了加强同学或者普通人对于密码学认识和了解，提升人们对于信息安全问题的重视和寻求一定的方法去更好的保护个人信息。所以，制作了一个覆盖面较为广泛的密码学介绍网站。

**设计思路：①**简介分为两层，上层左侧是密码学的定义，上层右侧是信息安全的图片，下层分左中右三块，重点介绍密码学的三大功能。

 <div class="col-12 col-md-6 col-lg-6 text-md-center text-lg-left wow fadeInLeft content-margin" data-wow-duration="1.5s" data-wow-delay="1.2s">

                    <div class="area-heading text-center text-lg-left">

                        <h1 class="main-font text-white font-weight-bold mb-4">密码学</h1>

                        <p class="text-white alt-font mb-5" style="text-indent:2em;" >密码学是研究如何隐密地传递信息的学科。在现代特别指对信息以及其传输的数学性研究，常被认为是数学和计算机科学的分支，和信息论也密切相关。密码学是信息安全等相关议题，如认证、访问控制的核心。密码学也促进了计算机科学，特别是在于电脑与网络安全所使用的技术，如访问控制与信息的机密性。 </p>

                    </div>

                </div>

                <div class="col-12 col-md-6 col-lg-6 text-right image-order wow fadeInRight" data-wow-duration="1.5s" data-wow-delay="1.2s">

                    <div class="slider-image">

                        <img src="static/picture/R-C.ico" width="400";height="400" alt="Slider-Image">

                    </div>

                </div>

<!-- 第一个作用 -->

                <div class="col-12 col-md-4 about-media wow zoomIn" data-wow-duration="1.5s" data-wow-delay="1.2s">

                    <span class="about-icon"><a href="javascript:void(0);"><i class="la la-laptop-code"></i></a></span>

                    <h4 class="small-heading main-font">加密解密</h4>

                    <p class="small-text alt-font">使用密码学的密钥对信息进行加解密，可以防止信息被人窃取。</p>

                </div>

②摘要分上中下三层，上层左侧是介绍密码学的视频，上层右侧是密码学的一些介绍。中层还是分三个，下层是密码学简介的链接（另一个HTML文件），图形结合强调了损失的重大和增长。

<div class=" col-sm-12 col-md-6 img-sec mt-5 mt-md-0 wow fadeIn order-2 order-md-1" data-wow-duration="1.5s" data-wow-delay=".5s">

                <video width="420" style="margin-top:15px;" controls>

                    <source src="static/vedio/mmx.mp4" type="video/mp4" />

                    <source src="static/vedio/mmx.ogg" type="video/ogg">

                </video>

            </div>

            <!-- 内容 -->

            <div class="col-sm-12 col-md-6 pl-md-5 wow fadeInRight order-1 order-md-1" data-wow-duration="1.5s" data-wow-delay=".5s">

                <div class="about-heading">

                    <h1 class="heading margin\_heading main-font"> 什么是密码学? </h1>

                <div style="width: 500px; height:300px;overflow-x:hidden;">

                    <p class="info"; style="text-indent:2em;">其实在公元前，秘密书信已用于战争之中。西洋“史学之父”希罗多德（Herodotus）的《历史》（The Histories）当中记载了一些最早的秘密书信故事。公元前5世纪，希腊城邦为对抗奴役和侵略，与波斯发生多次冲突和战争。于公元前480年，波斯秘密结了强大的军队，准备对雅典（Athens）和斯巴达（Sparta）发动一次突袭。希腊人狄马拉图斯（Demaratus）在波斯的苏萨城（Susa）里看到了这次集结，便利用了一层蜡把木板上的字遮盖住，送往并告知了希腊人波斯的图谋。最后，波斯海军覆没于雅典附近的沙拉米斯湾（Salamis Bay）。</p>

                    <p class="info"; style="text-indent:2em;">密码是通信双方按约定的法则进行信息特殊变换的一种重要保密手段。依照这些法则，变明文为密文，称为加密变换；变密文为明文，称为脱密变换。密码在早期仅对文字或数码进行加、脱密变换，随着通信技术的发展，对语音、图像、数据等都可实施加、脱密变换。</p>

                    <p class="info"; style="text-indent:2em;"> 密码学是在编码与破译的斗争实践中逐步发展起来的，并随着先进科学技术的应用，已成为一门综合性的尖端技术科学。它与语言学、数学、电子学、声学、信息论、计算机科学等有着广泛而密切的联系。它的现实研究成果，特别是各国政府现用的密码编制及破译手段都具有高度的机密性。</p>

                    <p class="info"; style="text-indent:2em;"> 在通信过程中，待加密的信息称为明文，已被加密的信息称为密文，仅有收、发双方知道的信息称为密钥。在密钥控制下，由明文变到密文的过程叫加密，其逆过程叫脱密或解密。在密码系统中，除合法用户外，还有非法的截收者，他们试图通过各种办法窃取机密（又称为被动攻击)或窜改消息（又称为主动攻击）。</p>

                </div>

                </div>

<!-- 第一个必要性 -->

            <div class="col-12 col-lg-4 wow bounceIn">

                <div id="circle" class="circle" data-value="2.24">

                    <h6 class="counter-num">224%</h6>

                </div>

                <h4 class="stats-heading">年增长率</h4>

                <p class="stats-para">据中国政府报告，网络攻击泄露数据平均年增长高达224%</p>

            </div>

<div class="col-12">

                    <h2 class="heading text-white">如果你想了解更多的密码学相关知识 <span class="d-block"> 请点击下列选项 </span></h2>

                    <a href="mmx.html" class="btn btn-medium btn-rounded btn-blue">学习更多知识</a>

                </div>

③古典密码学介绍大体分为上下两层，上层是简介，下层是典型密码学方案的简介（每个都有HTML链接）

<!--标题-->

        <div class="row text-center">

            <div class="col-12 col-md-10 col-lg-8 offset-md-1 offset-lg-2 wow zoomIn heading-area" data-wow-duration="1s" data-wow-delay=".1s">

                <h3 class="heading text-center">古典密码学</h3>

                <p class="text text-center" ; style="text-indent:2em;">密码(Cryptology)是一种用来混淆的技术,它希望将正常的、可识别的信息转变为无法识别的信息。密码学是一个即古老又新兴的学科,密码学一词源自希腊文“krypto's”及“logos”两字,直译即为“隐藏”及“讯息”之意。古典密码阶段是指从密码的产生到发展成为近代密码之间的这段时期密码的发展历史。</p>

            </div>

        </div>

        <div class="row padding-top-half">

 <!-- 内容一 -->

            <div class="col-12 col-lg-4 wow fadeInLeftBig" data-wow-delay=".4s">

                <div class="price-item text-center">

                    <div class="price\_header">

                        <p class="price\_header\_text"> 换位密码 </p>

                    </div>

                    <ul class="price-list">

                        <li>换位密码，是根据一定的规则重新排列明文，以便打破明文的结构特性。</li>

                        <li>换位密码的特点是 保持明文的所有字符不变 ，只是利用置换打乱了明文字符的 位置和次序 。也就是说，改变了明文的结构，不改变明文的内容。</li>

                    </ul>

                    <a href="gdmmx.html" class="btn btn-medium btn-rounded btn-blue-dark-white mb-5">学习更多知识</a>

                </div>

            </div>

④近代密码学只有一层，左边是近代密码学的简介（有另外的HTML链接），右边是信息安全图片

<div class="container">

        <div class="row align-items-center">

            <div class="col-12 col-md-6 wow fadeInLeftBig" data-wow-delay=".4s">

                <div class="heading-area">

                    <h2 class="heading mb-0">近代密码学</h2>

                    <p class="text" ; style="text-indent:2em;">近代密码学研究信息从发端到收端的安全传输和安全存储，是研究“知己知彼”的一门科学。其核心是密码编码学和密码分析学。前者致力于建立难以被敌方或对手攻破的安全密码体制，即“知己”；后者则力图破译敌方或对手已有的密码体制，即“知彼”。</p>

                    <a href="jdmmx.html" class="btn btn-medium btn-rounded btn-primary">学习更多知识</a>

                </div>

            </div>

            <div class="col-12 col-md-6 wow fadeIn" data-wow-delay="1.2s">

                <div class="img-fluid">

                    <img src="static/picture/R-C.ico" alt="image">

                </div>

            </div>

        </div>

    </div>

⑤现代密码学只有一层，左边是现代密码学的简介，右边是轮播图（播放经典密码学方案，可点击到新的HTML文件）

<div class="col-lg-6 col-md-12 col-sm-12 text-section wow fadeInLeft" data-wow-delay="300ms">

            <div class="text-area testimonial-heading">

                <h2>现代密码学</h2>

                <h4>伴随着网络的普及,计算机网络安全成为影响网络效能的重要问题,这就对网络的安全提出了更高的要求。现代密码阶段大约是指20世纪50年代以来的时期，其主要特点是采用电子计算机进行加密和解密。因此，该阶段也称为计算机密码时代。</h4>

            </div>

        </div>

        <div class="col-lg-6 col-md-12 col-sm-12 carousel-section wow fadeInRight" data-wow-delay="300ms">

            <div class=" text-center testimonial-carousel owl-carousel owl-themes active">

                <!-- 对称加密算法 -->

                <div class="item">

                    <div class="testimonials">

                        <div class="quote">

                            <i class="fas fa-quote-right"></i>

                        </div>

                        <a href="AES.html" class="bs"><h2>对称算法</h4></a>

                        <p class="text subheading">密码学中的高级加密标准（Advanced Encryption Standard，AES），又称Rijndael加密法，是美国联邦政府采用的一种区块加密标准。</p>

                        <p>AES加密过程是在一个4×4的字节矩阵上运作，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</p>

                        <div class="testimonial-image">

                            <img src="static/picture/1111.jpg" alt="image">

                        </div>

                        <h5 class="text">AES加密算法</h5>

                    </div>

                </div>

⑥量子密码学分上下两层，上层是量子密码学简介，下层分三块，每一块代表每一个量子密码学研究方向。

<!--标题-->

        <div class="row text-center padding-bottom-half">

            <div class="col-12 col-md-10 col-lg-8 offset-md-1 offset-lg-2 wow zoomIn heading-area" data-wow-duration="1s" data-wow-delay=".1s">

                <h3 class="heading text-center"> 量子密码学 </h3>

                <p class="text subheading" ; style="text-indent: 2em;">量子密码学（Quantum Cryptography）是一门很有前途的新领域，许多国家的人员都在研究它，而且在一定的范围内进行了试验。离实际应用只有一段不很长的距离。量子密码体系采用量子态作为信息载体，经由量子通道在合法的用户之间传送密钥。</p>

            </div>

        </div>

        <div class="row wow fadeInUp">

            <!--基于格的量子密码-->

            <div class="col-lg-4">

                <div class="news-item">

                    <img alt="image" class="news-img" src="static/picture/11111.png">

                    <div class="news-text-box">

                        <a href="https://zhuanlan.zhihu.com/p/234950092?utm\_source=qq&utm\_medium=social&utm\_oi=1144941642615173120"><h4 class="news-title">基于格的量子密码</h4></a>

                        <p class="para">格 more secure than 整数分解等等，可以抵御量子计算机的攻击。而且，有时候可满足更多功能。格困难问题：给定一点，我们无法知道其是从哪点来的，因为维度可以很高（可沿很多方向移动）。但在实际应用中，这个问题被封装成LWE、SIS等问题。</p>

                        </a>

                    </div>

                </div>

            </div>

⑦末尾是制作者信息和发送消息界面，一层分左中右三块，左边是个人信息、中间和右边是发送邮件及其消息。

<div class="row align-items-center">

            <div class="col-12 col-md-3 text-center">

                <div class="user-img"><img src="static/picture/side-logo.png" class="rounded-circle" alt="img"></div>

                <h4 class="user-name">朱传伟</h4>

                <p class="user-designation">2832365442@qq.com</p>

                <p class="user-designation">+86 15057874966</p>

            </div>

            <div class="col-12 col-md-9">

                <div class="row">

                    <div class="col-12" id="result"></div>

                    <div class="col-12 col-md-6">

                        <form class="row contact-form row-padding" id="contact-form-data">

                            <div class="col-12">

                                <input type="text" name="userName" placeholder="Name" class="form-control">

                                <input type="text" name="userPhone" placeholder="Contact No" class="form-control">

                                <input type="email" name="userEmail" placeholder="Email" class="form-control">

                            </div>

                        </form>

                    </div>

                    <div class="col-12 col-md-6 contact-form">

                        <textarea class="form-control" name="userMessage" rows="6" placeholder="Message"></textarea>

                        <a href="mailto:2832365442@qq.com" class="btn btn-medium btn-rounded btn-trans-white rounded-pill w-100 contact\_btn main-font">Send</a>

                    </div>

                </div>

            </div>

        </div>

**设计目标：**计划做一个可粗略介绍密码学的前世今生和部分密码学方案介绍的多页面HTML网页界面。

**主要工作：**学习HTML语言和CSS以及JavaScript，使用HTML和CSS以及JavaScript结合网络上的部分资源库制作出框架，然后再向框架中不断加入密码学相关内容。

**结构分析：**项目是总分结构， 总体分为两级，index.html是第一级，AES.html、RSA.html等是第二级，index.html概括性的介绍了密码学的作用、发展历程等信息，其他界面是用来补充说明index.html文件的。主要工作就是理清楚密码学的关系和分支等组成框架，然后去寻找各种密码学知识来填充进框架内，并处理好密码学关系和文件关系等各种关系。

1. **源代码**

两级目录，index.html是根目录，其他文件是枝目录。

**Index.html:**

<!DOCTYPE html>

<html lang="zh">

<head>

    <!-- 元标签 -->

    <meta charset="utf-8">

    <!-- 作者 -->

    <meta name="name" content="朱传伟">

    <!-- 描述 -->

    <meta name="description" content="密码学资料">

    <!-- 页面标题 -->

    <title>密码学资料</title>

    <!-- 网站图标 -->

    <link href="static/image/favicon.ico" rel="icon">

    <link href="static/css/bundle.min.css" rel="stylesheet">

    <!-- 插件 CSS -->

    <link href="static/css/owl.carousel.min.css" rel="stylesheet">

    <!-- <link href="static/css/LineIcons.min.css" rel="stylesheet"> -->

    <!-- <link href="static/css/jquery.fancybox.min.css" rel="stylesheet"> -->

    <!-- 样式表 -->

    <link href="static/css/line-awesome.min.css" rel="stylesheet">

    <link href="static/css/style.css" rel="stylesheet">

</head>

<body data-spy="scroll" data-target=".navbar" data-offset="90">

<style type="text/css">

.bs:hover{

    color: pink;

}

</style>

<!-- 预加载开始 -->

<div class="loader-bg">

    <div class="loader">

        <span></span>

        <span></span>

        <span></span>

        <span></span>

        <span></span>

        <span></span>

        <span></span>

        <span></span>

        <span></span>

        <span></span>

        <span></span>

        <span></span>

        <span></span>

        <span></span>

        <span></span>

    </div>

</div>

<!-- 预加载结束 -->

<!-- 标题开始 -->

<header>

    <!--导航栏-->

    <nav class="navbar navbar-top-default navbar-expand-lg navbar-simple nav-line">

        <div class="container">

            <a href="#slider-area" title="Logo" class="logo scroll">

                <!--logo-->

                <img src="static/image/favicon.ico" title="logo" alt="logo" class="logo-default">

            </a>

            <!--顶部导航栏链接-->

            <div class="collapse navbar-collapse" id="megaone">

                <div class="navbar-nav ml-auto">

                    <a class="nav-link scroll line active" href="#slider-area">简介</a>

                    <a class="nav-link scroll line" href="#about">摘要</a>

                    <a class="nav-link scroll line" href="#prices">古典密码学</a>

                    <a class="nav-link scroll line" href="#hosting">近代密码学</a>

                    <a class="nav-link scroll line" href="#testimonials">现代密码学</a>

                    <a class="nav-link scroll line" href="#blog">量子密码学</a>

                    <a class="nav-link scroll line" href="#contact">联系我</a>

                </div>

            </div>

        </div>

        <!--侧面菜单按钮-->

        <div>

            <ul>

                <li>

                    <a href="javascript:void(0);" class="sidemenu\_btn" id="sidemenu\_toggle">

                        <span></span>

                        <span></span>

                        <span></span>

                    </a>

                </li>

            </ul>

        </div>

    </nav>

    <!--侧面导航栏-->

    <div class="side-menu hidden">

        <div class="inner-wrapper">

            <span class="btn-close" id="btn\_sideNavClose"><i></i><i></i></span>

            <a href="" title="Logo" class="logo side-logo">

                <!--Logo-->

                <img src="static/image/favicon.ico" alt="logo">

            </a>

            <nav class="side-nav w-100">

                <ul class="navbar-nav side-navbar">

                    <li class="nav-item">

                        <a class="nav-link scroll" href="#slider-area">简介</a>

                    </li>

                    <li class="nav-item">

                        <a class="nav-link scroll" href="#about">摘要</a>

                    </li>

                    <li class="nav-item">

                        <a class="nav-link scroll" href="#prices">古典密码学</a>

                    </li>

                    <li class="nav-item">

                        <a class="nav-link scroll" href="#hosting">近代密码学</a>

                    </li>

                    <li class="nav-item">

                        <a class="nav-link scroll" href="#testimonials">现代密码学</a>

                    </li>

                    <li class="nav-item">

                        <a class="nav-link scroll" href="#blog">量子密码学</a>

                    </li>

                    <li class="nav-item">

                        <a class="nav-link scroll" href="#contact">联系我</a>

                    </li>

                </ul>

            </nav>

            <div class="side-footer w-100">

                <ul class="social-icons-simple">

                    <li><a class="social-icon" href="https://connect.facebook.com"><i class="fab fa-facebook-f"></i> </a> </li>

                    <li><a class="social-icon" href="www.twitters.com"><i class="fab fa-twitter"></i> </a> </li>

                    <li><a class="social-icon" href="https://cn.linkedin.com"><i class="fab fa-linkedin-in"></i> </a> </li>

                    <li><a class="social-icon" href="www.sinoclick.com"><i class="fab fa-instagram"></i> </a> </li>

                </ul>

            </div>

        </div>

    </div>

    <a id="close\_side\_menu" href="javascript:void(0);"></a>

</header>

<!-- 标题结束 -->

<!-- 简介开始 -->

<section id="particles-js" class="p-0 position-relative">

    <div class="slider-area" id="slider-area">

        <div class="container">

            <div class="row align-items-center">

                <div class="col-12 col-md-6 col-lg-6 text-md-center text-lg-left wow fadeInLeft content-margin" data-wow-duration="1.5s" data-wow-delay="1.2s">

                    <div class="area-heading text-center text-lg-left">

                        <h1 class="main-font text-white font-weight-bold mb-4">密码学</h1>

                        <p class="text-white alt-font mb-5" style="text-indent:2em;" >密码学是研究如何隐密地传递信息的学科。在现代特别指对信息以及其传输的数学性研究，常被认为是数学和计算机科学的分支，和信息论也密切相关。密码学是信息安全等相关议题，如认证、访问控制的核心。密码学也促进了计算机科学，特别是在于电脑与网络安全所使用的技术，如访问控制与信息的机密性。 </p>

                    </div>

                </div>

                <div class="col-12 col-md-6 col-lg-6 text-right image-order wow fadeInRight" data-wow-duration="1.5s" data-wow-delay="1.2s">

                    <div class="slider-image">

                        <img src="static/picture/R-C.ico" width="400";height="400" alt="Slider-Image">

                    </div>

                </div>

            </div>

        </div>

    </div>

    <!-- 三大作用 -->

    <div class="author-skills bg-blue">

        <div class="container">

            <div class="row text-center text-lg-left">

                <!-- 第一个作用 -->

                <div class="col-12 col-md-4 about-media wow zoomIn" data-wow-duration="1.5s" data-wow-delay="1.2s">

                    <span class="about-icon"><a href="javascript:void(0);"><i class="la la-laptop-code"></i></a></span>

                    <h4 class="small-heading main-font">加密解密</h4>

                    <p class="small-text alt-font">使用密码学的密钥对信息进行加解密，可以防止信息被人窃取。</p>

                </div>

                <!-- 第二个作用 -->

                <div class="col-12 col-md-4 about-media wow zoomIn" data-wow-duration="1.5s" data-wow-delay="1.5s">

                    <span class="about-icon"><a href="javascript:void(0);"><i class="las la-server"></i></a></span>

                    <h4 class="small-heading main-font">身份认证</h4>

                    <p class="small-text alt-font">身份认证是用于确认用户是否为这个用户的手段，是对于信息的发送方的身份确认。</p>

                </div>

                <!-- 第三个作用 -->

                <div class="col-12 col-md-4 about-media wow zoomIn" data-wow-duration="1.5s" data-wow-delay="1.8s">

                    <span class="about-icon"><a href="javascript:void(0);"><i class="las la-registered"></i></a></span>

                    <h4 class="small-heading main-font">数字签名</h4>

                    <p class="small-text alt-font">数字签名（又称公钥数字签名）是只有信息的发送者才能产生的别人无法伪造的一段数字串，这段数字串同时也是对信息的发送者发送信息真实性的一个有效证明。</p>

                </div>

            </div>

        </div>

    </div>

</section>

<!-- 简介结束 -->

<!-- 摘要开始 -->

<section id="about">

    <div class="container">

        <div class="row align-items-center">

            <!-- 视频 -->

            <div class=" col-sm-12 col-md-6 img-sec mt-5 mt-md-0 wow fadeIn order-2 order-md-1" data-wow-duration="1.5s" data-wow-delay=".5s">

                <video width="420" style="margin-top:15px;" controls>

                    <source src="static/vedio/mmx.mp4" type="video/mp4" />

                    <source src="static/vedio/mmx.ogg" type="video/ogg">

                </video>

            </div>

            <!-- 内容 -->

            <div class="col-sm-12 col-md-6 pl-md-5 wow fadeInRight order-1 order-md-1" data-wow-duration="1.5s" data-wow-delay=".5s">

                <div class="about-heading">

                    <h1 class="heading margin\_heading main-font"> 什么是密码学? </h1>

                <div style="width: 500px; height:300px;overflow-x:hidden;">

                    <p class="info"; style="text-indent:2em;">其实在公元前，秘密书信已用于战争之中。西洋“史学之父”希罗多德（Herodotus）的《历史》（The Histories）当中记载了一些最早的秘密书信故事。公元前5世纪，希腊城邦为对抗奴役和侵略，与波斯发生多次冲突和战争。于公元前480年，波斯秘密结了强大的军队，准备对雅典（Athens）和斯巴达（Sparta）发动一次突袭。希腊人狄马拉图斯（Demaratus）在波斯的苏萨城（Susa）里看到了这次集结，便利用了一层蜡把木板上的字遮盖住，送往并告知了希腊人波斯的图谋。最后，波斯海军覆没于雅典附近的沙拉米斯湾（Salamis Bay）。</p>

                    <p class="info"; style="text-indent:2em;">密码是通信双方按约定的法则进行信息特殊变换的一种重要保密手段。依照这些法则，变明文为密文，称为加密变换；变密文为明文，称为脱密变换。密码在早期仅对文字或数码进行加、脱密变换，随着通信技术的发展，对语音、图像、数据等都可实施加、脱密变换。</p>

                    <p class="info"; style="text-indent:2em;"> 密码学是在编码与破译的斗争实践中逐步发展起来的，并随着先进科学技术的应用，已成为一门综合性的尖端技术科学。它与语言学、数学、电子学、声学、信息论、计算机科学等有着广泛而密切的联系。它的现实研究成果，特别是各国政府现用的密码编制及破译手段都具有高度的机密性。</p>

                    <p class="info"; style="text-indent:2em;"> 在通信过程中，待加密的信息称为明文，已被加密的信息称为密文，仅有收、发双方知道的信息称为密钥。在密钥控制下，由明文变到密文的过程叫加密，其逆过程叫脱密或解密。在密码系统中，除合法用户外，还有非法的截收者，他们试图通过各种办法窃取机密（又称为被动攻击)或窜改消息（又称为主动攻击）。</p>

                </div>

                </div>

            </div>

        </div>

    </div>

</section>

<!-- 必要性开始 -->

<section class="stats-sec pt-0" id="stats-sec">

    <div class="container">

        <div class="row circular-wrap text-center">

            <!-- 第一个必要性 -->

            <div class="col-12 col-lg-4 wow bounceIn">

                <div id="circle" class="circle" data-value="2.24">

                    <h6 class="counter-num">224%</h6>

                </div>

                <h4 class="stats-heading">年增长率</h4>

                <p class="stats-para">据中国政府报告，网络攻击泄露数据平均年增长高达224%</p>

            </div>

            <!-- 第二个必要性 -->

            <div class="col-12 col-lg-4 wow bounceIn wrap-2">

                <div id="circletwo" class="circle" data-value="0.70">

                    <h6 class="counter-num">70%</h6>

                </div>

                <h4 class="stats-heading">信息泄露占比</h4>

                <p class="stats-para">据中国政府报告，2021年有70%的中国公民信息被泄露</p>

            </div>

            <!-- 第三个必要性 -->

            <div class="col-12 col-lg-4 wow bounceIn">

                <div id="circlethree" class="circle" data-value="0.75">

                    <h6 class="counter-num">805亿元</h6>

                </div>

                <h4 class="stats-heading">信息泄露损失</h4>

                <p class="stats-para">据中国政府报告，2021年中国信息泄露损失高达805亿元</p>

            </div>

        </div>

    </div>

</section>

<!-- 必要性结束 -->

<!-- 摘要结束 -->

<!-- 学习更多开始 -->

<section class="learn-more-section">

    <div class="container">

        <div class="text-area wow fadeInUpBig heading-area" data-wow-delay=".5s">

            <div class="row">

                <div class="col-12">

                    <h2 class="heading text-white">如果你想了解更多的密码学相关知识 <span class="d-block"> 请点击下列选项 </span></h2>

                    <a href="mmx.html" class="btn btn-medium btn-rounded btn-blue">学习更多知识</a>

                </div>

            </div>

        </div>

    </div>

</section>

<!-- 学习更多结束 -->

<!-- 古典密码学开始 -->

<section id="prices" class="prices padding-up">

    <div class="container">

        <!--标题-->

        <div class="row text-center">

            <div class="col-12 col-md-10 col-lg-8 offset-md-1 offset-lg-2 wow zoomIn heading-area" data-wow-duration="1s" data-wow-delay=".1s">

                <h3 class="heading text-center">古典密码学</h3>

                <p class="text text-center" ; style="text-indent:2em;">密码(Cryptology)是一种用来混淆的技术,它希望将正常的、可识别的信息转变为无法识别的信息。密码学是一个即古老又新兴的学科,密码学一词源自希腊文“krypto's”及“logos”两字,直译即为“隐藏”及“讯息”之意。古典密码阶段是指从密码的产生到发展成为近代密码之间的这段时期密码的发展历史。</p>

            </div>

        </div>

        <div class="row padding-top-half">

            <!-- 内容一 -->

            <div class="col-12 col-lg-4 wow fadeInLeftBig" data-wow-delay=".4s">

                <div class="price-item text-center">

                    <div class="price\_header">

                        <p class="price\_header\_text"> 换位密码 </p>

                    </div>

                    <ul class="price-list">

                        <li>换位密码，是根据一定的规则重新排列明文，以便打破明文的结构特性。</li>

                        <li>换位密码的特点是 保持明文的所有字符不变 ，只是利用置换打乱了明文字符的 位置和次序 。也就是说，改变了明文的结构，不改变明文的内容。</li>

                    </ul>

                    <a href="gdmmx.html" class="btn btn-medium btn-rounded btn-blue-dark-white mb-5">学习更多知识</a>

                </div>

            </div>

            <!-- 内容二 -->

            <div class="col-12 col-lg-4 wow fadeIn" data-wow-delay=".8s">

                <div class="price-item-center text-center">

                    <div class="price\_header-center">

                        <p class="price\_header\_text"> 替换密码 </p>

                    </div>

                    <ul class="price-list">

                        <li>置换密码的特点是 保持明文的所有字符不变 ，只是利用置换打乱了明文字符的 位置和次序 。也就是说，改变了明文的结构，不改变明文的内容。</li>

                        <li>根据密码加/解密时使用的替换表的多少，替换密码又可分为单表替换密码和多表替换密码。</li>

                    </ul>

                    <a href="gdmmx.html" class="btn btn-medium btn-rounded btn-primary mb-5"> 学习更多知识 </a>

                </div>

            </div>

            <!-- 内容三 -->

            <div class="col-12 col-lg-4 wow fadeInRightBig" data-wow-delay=".4s">

                <div class="price-item text-center">

                    <div class="price\_header">

                        <p class="price\_header\_text"> 分组密码 </p>

                    </div>

                    <ul class="price-list">

                        <li>分组密码是一种拆解字母的方法，以便一个字母能被两个或多个符号表示。例如：a可以用01代替、b可以用02代替，依次类推我们得到加密表。</li>

                        <li>虽然分组密码有这些缺陷，但它可以使其他密码更加安全。如将分组与列换位密码结合。</li>

                    </ul>

                    <a href="gdmmx.html" class="btn btn-medium btn-rounded btn-blue-dark-white mb-5">学习更多知识</a>

                </div>

            </div>

        </div>

    </div>

</section>

<!-- 古典密码学结束 -->

<!-- 近代密码学开始 -->

<section class="hosting bg-light-white" id="hosting">

    <div class="container">

        <div class="row align-items-center">

            <div class="col-12 col-md-6 wow fadeInLeftBig" data-wow-delay=".4s">

                <div class="heading-area">

                    <h2 class="heading mb-0">近代密码学</h2>

                    <p class="text" ; style="text-indent:2em;">近代密码学研究信息从发端到收端的安全传输和安全存储，是研究“知己知彼”的一门科学。其核心是密码编码学和密码分析学。前者致力于建立难以被敌方或对手攻破的安全密码体制，即“知己”；后者则力图破译敌方或对手已有的密码体制，即“知彼”。</p>

                    <a href="jdmmx.html" class="btn btn-medium btn-rounded btn-primary">学习更多知识</a>

                </div>

            </div>

            <div class="col-12 col-md-6 wow fadeIn" data-wow-delay="1.2s">

                <div class="img-fluid">

                    <img src="static/picture/R-C.ico" alt="image">

                </div>

            </div>

        </div>

    </div>

</section>

<!-- 近代密码学结束 -->

<!-- 现代密码学开始 -->

<section class="testimonial-section py-0" id="testimonials">

    <div class="row no-gutters">

        <div class="col-lg-6 col-md-12 col-sm-12 text-section wow fadeInLeft" data-wow-delay="300ms">

            <div class="text-area testimonial-heading">

                <h2>现代密码学</h2>

                <h4>伴随着网络的普及,计算机网络安全成为影响网络效能的重要问题,这就对网络的安全提出了更高的要求。现代密码阶段大约是指20世纪50年代以来的时期，其主要特点是采用电子计算机进行加密和解密。因此，该阶段也称为计算机密码时代。</h4>

            </div>

        </div>

        <div class="col-lg-6 col-md-12 col-sm-12 carousel-section wow fadeInRight" data-wow-delay="300ms">

            <div class=" text-center testimonial-carousel owl-carousel owl-themes active">

                <!-- 对称加密算法 -->

                <div class="item">

                    <div class="testimonials">

                        <div class="quote">

                            <i class="fas fa-quote-right"></i>

                        </div>

                        <a href="AES.html" class="bs"><h2>对称算法</h4></a>

                        <p class="text subheading">密码学中的高级加密标准（Advanced Encryption Standard，AES），又称Rijndael加密法，是美国联邦政府采用的一种区块加密标准。</p>

                        <p>AES加密过程是在一个4×4的字节矩阵上运作，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</p>

                        <div class="testimonial-image">

                            <img src="static/picture/1111.jpg" alt="image">

                        </div>

                        <h5 class="text">AES加密算法</h5>

                    </div>

                </div>

                <!-- 非对称加密算法 -->

                <div class="item active">

                    <div class="testimonials">

                        <div class="quote">

                            <i class="fas fa-quote-right"></i>

                        </div>

                        <a href="RSA.html" class="bs"><h2>非对称加密</h2></a>

                        <p class="text subheading">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。</p>

                        <p class="text subheading">RSA公开密钥密码体制的原理是：根据数论，寻求两个大素数比较简单，而将它们的乘积进行因式分解却极其困难，因此可以将乘积公开作为加密密钥。</p>

                        <div class="testimonial-image">

                            <img src="static/picture/2222.jpg" alt="image">

                        </div>

                        <h5 class="text">RSA加密算法</h5>

                    </div>

                </div>

                <!-- 摘要算法 -->

                <div class="item">

                    <div class="testimonials">

                        <div class="quote">

                            <i class="fas fa-quote-right"></i>

                        </div>

                        <a href="SHA256.html" class="bs"><h2>摘要算法</h2></a>

                        <p class="text subheading">SHA-2，名称来自于安全散列算法2（英语：Secure Hash Algorithm 2）的缩写，一种密码散列函数算法标准，由美国国家安全局研发，属于SHA算法之一，是SHA-1的后继者。</p>

                        <p class="text subheading">哈希函数，又称散列算法，是一种从任何一种数据中创建小的数字“指纹”的方法。散列函数把消息或数据压缩成摘要，使得数据量变小，将数据的格式固定下来。该函数将数据打乱混合，重新创建一个叫做散列值（或哈希值）的指纹。散列值通常用一个短的随机字母和数字组成的字符串来代表。</p>

                        <div class="testimonial-image">

                            <img src="static/picture/3333.jpg" alt="image">

                        </div>

                        <h5 class="text">SHA256算法</h5>

                    </div>

                </div>

            </div>

        </div>

    </div>

</section>

<!-- 现代密码学结束 -->

<!-- 量子密码学开始 -->

<section class="blog-sec" id="blog">

    <div class="container">

        <!--标题-->

        <div class="row text-center padding-bottom-half">

            <div class="col-12 col-md-10 col-lg-8 offset-md-1 offset-lg-2 wow zoomIn heading-area" data-wow-duration="1s" data-wow-delay=".1s">

                <h3 class="heading text-center"> 量子密码学 </h3>

                <p class="text subheading" ; style="text-indent: 2em;">量子密码学（Quantum Cryptography）是一门很有前途的新领域，许多国家的人员都在研究它，而且在一定的范围内进行了试验。离实际应用只有一段不很长的距离。量子密码体系采用量子态作为信息载体，经由量子通道在合法的用户之间传送密钥。</p>

            </div>

        </div>

        <div class="row wow fadeInUp">

            <!--基于格的量子密码-->

            <div class="col-lg-4">

                <div class="news-item">

                    <img alt="image" class="news-img" src="static/picture/11111.png">

                    <div class="news-text-box">

                        <a href="https://zhuanlan.zhihu.com/p/234950092?utm\_source=qq&utm\_medium=social&utm\_oi=1144941642615173120"><h4 class="news-title">基于格的量子密码</h4></a>

                        <p class="para">格 more secure than 整数分解等等，可以抵御量子计算机的攻击。而且，有时候可满足更多功能。格困难问题：给定一点，我们无法知道其是从哪点来的，因为维度可以很高（可沿很多方向移动）。但在实际应用中，这个问题被封装成LWE、SIS等问题。</p>

                        </a>

                    </div>

                </div>

            </div>

            <!--基于编码的量子密码-->

            <div class="col-lg-4">

                <div class="news-item">

                    <img alt="image" class="news-img" src="static/picture/22222.jpg">

                    <div class="news-text-box">

                        <a href="https://zhuanlan.zhihu.com/p/379001794?utm\_source=qq&utm\_medium=social&utm\_oi=1144941642615173120

                        "><h4 class="news-title">基于编码的量子密码</h4></a>

                        <p class="para">基于编码的公钥密码由于能抵抗量子攻击和美国 NIST 后量子公钥密码算法的征集而受到越来越多的关注。基于编码的 NIST 抗量子攻击公钥密码征集算法, 梳理基于编码的公钥方案具有的特点, 即三种加密方式, 三种重要的参与码类, 三种安全性基于的困难问题,。</p>

                        </a>

                    </div>

                </div>

            </div>

            <!--基于梅森数的量子密码-->

            <div class="col-lg-4">

                <div class="news-item">

                    <img alt="image" class="news-img" src="static/picture/33333.jpg">

                    <div class="news-text-box">

                        <a href="https://zhuanlan.zhihu.com/p/500382331?utm\_source=qq&utm\_medium=social&utm\_oi=1144941642615173120"><h4 class="news-title">基于梅森数的量子密码</h4></a>

                        <p class="para">基于梅森素数的抗量子密码体系是最近新出的抗量子密码系统，它依靠梅森素数的困难问题和低汉明bit的困难问题来实现抗量子特性。并出现了多篇针对性的论文，在各种理论上论证了其安全性和对其进行了理论攻击，目前理论上并未攻破。</p>

                        </a>

                    </div>

                </div>

            </div>

        </div>

    </div>

</section>

<!-- 量子密码学结束 -->

<!-- 联系我开始 -->

<section class="contact-sec" id="contact">

    <div class="container">

        <div class="row align-items-center">

            <div class="col-12 col-md-3 text-center">

                <div class="user-img"><img src="static/picture/side-logo.png" class="rounded-circle" alt="img"></div>

                <h4 class="user-name">朱传伟</h4>

                <p class="user-designation">2832365442@qq.com</p>

                <p class="user-designation">+86 15057874966</p>

            </div>

            <div class="col-12 col-md-9">

                <div class="row">

                    <div class="col-12" id="result"></div>

                    <div class="col-12 col-md-6">

                        <form class="row contact-form row-padding" id="contact-form-data">

                            <div class="col-12">

                                <input type="text" name="userName" placeholder="Name" class="form-control">

                                <input type="text" name="userPhone" placeholder="Contact No" class="form-control">

                                <input type="email" name="userEmail" placeholder="Email" class="form-control">

                            </div>

                        </form>

                    </div>

                    <div class="col-12 col-md-6 contact-form">

                        <textarea class="form-control" name="userMessage" rows="6" placeholder="Message"></textarea>

                        <a href="mailto:2832365442@qq.com" class="btn btn-medium btn-rounded btn-trans-white rounded-pill w-100 contact\_btn main-font">Send</a>

                    </div>

                </div>

            </div>

        </div>

    </div>

</section>

<!-- 联系我结束 -->

<!-- 底部栏开始 -->

<footer class="footer">

    <div class="container">

        <div class="row align-items-center">

            <!--超链接-->

            <div class="col-12">

                <div class="footer-social text-center">

                    <ul class="list-unstyled">

                        <li><a class="wow fadeInUp" href="https://connect.facebook.com"><i aria-hidden="true" class="fab fa-facebook-f"></i><span></span></a></li>

                        <li><a class="wow fadeInDown" href="www.twitters.com"><i aria-hidden="true" class="fab fa-twitter"></i><span></span></a></li>

                        <li><a class="wow fadeInUp" href="https://google.cn/webhp?source=g\_cn"><i aria-hidden="true" class="fab fa-google-plus-g"></i><span></span></a></li>

                        <li><a class="wow fadeInDown" href="https://cn.linkedin.com"><i aria-hidden="true" class="fab fa-linkedin-in"></i><span></span></a></li>

                        <li><a class="wow fadeInUp" href="www.sinoclick.com"><i aria-hidden="true" class="fab fa-instagram"></i><span></span></a></li>

                        <li><a class="wow fadeInDown" href="www.sinoclick.com"><i aria-hidden="true" class="fab fa-pinterest-p"></i><span></span></a></li>

                    </ul>

                </div>

            </div>

            <!-- 底部行 -->

            <div class="col-12 text-center mt-3">

                <p class="company-about fadeIn">Copyright &copy; 2022.5.23 朱传伟

                </p>

            </div>

        </div>

    </div>

</footer>

<!-- 底部栏结束 -->

</body>

<!-- JavaScript -->

<script src="static/js/bundle.min.js"></script>

<script src="static/js/jquery.appear.js"></script>

<script src="static/js/owl.carousel.min.js"></script>

<script src="static/js/wow.min.js"></script>

<script src="static/js/jquery.fancybox.min.js"></script>

<script src="static/js/particles.min.js"></script>

<script src="static/js/contact\_us.js"></script>

<script src="static/js/circle-progress.min.js"></script>

<script src="static/js/script.js"></script>

</html>

**gdmmx.html:**

<!DOCTYPE html>

<html lang="zh">

<head>

    <!-- 元标签 -->

    <meta charset="utf-8">

    <meta content="width=device-width, initial-scale=1, shrink-to-fit=no" name="viewport">

    <!-- 作者 -->

    <meta name="author" content="朱传伟">

    <!-- 描述 -->

    <meta name="description" content="古典密码学">

    <!-- 页面标题 -->

    <title>密码学介绍</title>

    <!-- 网站图标 -->

    <link href="static/image/favicon.ico" rel="icon">

    <link href="static/css/bundle.min.css" rel="stylesheet">

    <!-- 插件 CSS -->

    <link href="static/css/owl.carousel.min.css" rel="stylesheet">

    <link rel="stylesheet" href="static/css/LineIcons.min.css">

    <link rel="stylesheet" href="static/css/jquery.fancybox.min.css">

    <!-- 样式表 -->

    <link href="static/css/line-awesome.min.css" rel="stylesheet">

    <link href="static/css/style.css" rel="stylesheet">

    <link href="static/css/custom.css" rel="stylesheet">

</head>

<body>

<!-- 预加载开始 -->

<div class="loader-bg">

    <div class="loader">

        <span></span>

        <span></span>

        <span></span>

        <span></span>

        <span></span>

        <span></span>

        <span></span>

        <span></span>

        <span></span>

        <span></span>

        <span></span>

        <span></span>

        <span></span>

        <span></span>

        <span></span>

    </div>

</div>

<!-- 预加载结束 -->

<!-- 标题开始 -->

<header>

    <!--导航栏-->

    <nav class="navbar navbar-top-default navbar-expand-lg navbar-simple nav-line">

        <div class="container">

            <a href="index.html#slider-area" title="Logo" class="logo scroll">

                <!--Logo-->

                <img src="static/image/favicon.ico" title="logo" alt="logo" class="logo-default">

            </a>

            <!--菜单-->

            <div class="collapse navbar-collapse" id="megaone">

                <div class="navbar-nav ml-auto">

                    <a class="nav-link" href="index.html">简介</a>

                    <a class="nav-link" href="index.html#about">摘要</a>

                    <a class="nav-link" href="index.html#prices">古典密码学</a>

                    <a class="nav-link" href="index.html#hosting">近代密码学</a>

                    <a class="nav-link" href="index.html#testimonials">现代密码学</a>

                    <a class="nav-link" href="index.html#blog">量子密码学</a>

                    <a class="nav-link" href="index.html#contact">联系我</a>

                </div>

            </div>

        </div>

        <div class="navigation-toggle">

            <ul class="slider-social toggle-btn my-0">

                <li>

                    <a href="javascript:void(0);" class="sidemenu\_btn" id="sidemenu\_toggle">

                        <span></span>

                        <span></span>

                        <span></span>

                    </a>

                </li>

            </ul>

        </div>

    </nav>

    <!--侧边导航栏-->

    <div class="side-menu hidden">

        <div class="inner-wrapper">

            <span class="btn-close" id="btn\_sideNavClose"><i></i><i></i></span>

            <a href="index.html" title="Logo" class="logo side-logo">

                <!--Logo-->

                <img src="static/image/favicon.ico" alt="logo">

            </a>

            <nav class="side-nav w-100">

                <ul class="navbar-nav side-navbar">

                    <li class="nav-item">

                        <a class="nav-link" href="index.html">密码学资料</a>

                    </li>

                    <li class="nav-item">

                        <a class="nav-link" href="index.html#about">摘要</a>

                    </li>

                    <li class="nav-item">

                        <a class="nav-link" href="index.html#prices">古典密码学</a>

                    </li>

                    <li class="nav-item">

                        <a class="nav-link" href="index.html#hosting">近代密码学</a>

                    </li>

                    <li class="nav-item">

                        <a class="nav-link" href="index.html#testimonials">现代密码学</a>

                    </li>

                    <li class="nav-item">

                        <a class="nav-link" href="index.html#blog">量子密码学</a>

                    </li>

                    <li class="nav-item">

                        <a class="nav-link" href="index.html#contact">联系我</a>

                    </li>

                </ul>

            </nav>

            <div class="side-footer w-100">

                <ul class="social-icons-simple">

                    <li><a class="social-icon" href="https://connect.facebook.com"><i class="fab fa-facebook-f"></i> </a> </li>

                    <li><a class="social-icon" href="https://www.twitters.com"><i class="fab fa-twitter"></i> </a> </li>

                    <li><a class="social-icon" href="https://cn.linkedin.com"><i class="fab fa-linkedin-in"></i> </a> </li>

                    <li><a class="social-icon" href="https://apps.apple.com/ca/app/instagram/id389801252"><i class="fab fa-instagram"></i> </a> </li>

                </ul>

            </div>

        </div>

    </div>

    <a id="close\_side\_menu" href="javascript:void(0);"></a>

</header>

<!-- 标题结束 -->

<!-- 首页开始 -->

<section class="page-title stand-banner">

    <div class="container">

        <div class="row justify-content-center">

            <div class="col-12 col-lg-10">

                <div class="box-content">

                    <h2 class="hide-cursor wow fadeInUp" data-wow-delay="1.2s">古典密码学</h2>

                    <ul class="page-breadcrumb link wow fadeInUp" data-wow-delay="1.6s">

                        <li><a href="index.html"><span class="icon fas fa-home"></span>密码学资料</a></li>

                        <li>古典密码学</li>

                    </ul>

                </div>

            </div>

        </div>

    </div>

</section>

<!-- 首页结束 -->

<!-- 内容开始 -->

<section class="main" id="main">

    <div class="blog-content">

        <div class="container">

            <div class="row no-gutters">

                <div class="col-12">

                    <!-- 概括内容 -->

                    <div class="standalone-detail">

                        <div class="row no-gutters">

                            <div class="col-12 col-md-10 offset-md-1 col-lg-8 offset-lg-2  text-center wow slideInUp" data-wow-duration="2s">

                                <h1 class="heading">古典密码学</h1>

                                <p class="para\_text m-auto">古典密码学是密码学中的一个类型，其大部分加密方式都是利用置换式密码或代换式密码，有时则是两者的混合。古典密码在历史中经常使用，但现代已经很少使用，大部分的已经不再安全了。一般而言，古典密码是基于一个拼音字母（像是 A-Z）、动手操作或是简单的设备。</p>

                            </div>

                        </div>

                    </div>

                    <div class="standalone-area">

                        <!-- 栅栏密码 -->

                        <div class="row standalone-row align-items-center">

                            <div class="col-lg-6 px-md-0">

                                <div class="blog-image wow hover-effect fadeInLeftBig text-center text-lg-left">

                                    <div class="box">

                                        <img src="static/picture/1.png" alt="image">

                                        <div class="box-content">

                                            <h3 class="name">栅栏密码</h3>

                                        </div>

                                    </div>

                                </div>

                            </div>

                            <div class="col-lg-6 stand-img-des">

                                <div class="d-inline-block wow fadeIn" data-wow-delay=".5s">

                                    <h2 class="heading-text">栅栏密码</h2>

                                    <p class="para\_text" style="text-indent: 2em;">栅栏密码是经典的换位密码，就是把要加密的明文分成N个一组，然后把每组的第1个字连起来，形成一段无规律的话。 不过栅栏密码本身有一个潜规则，就是组成栅栏的字母一般不会太多。 </p>

                                    <p class="para\_text" style="text-indent: 2em;">栅栏密码的安全性较低，我们可以对其进行扩展。在选择行数时可以使多行，这样对于加密强度有所提高。可以在加密之后在使用其他密码进行加密，增加强度</p>

                                </div>

                            </div>

                        </div>

                        <!-- 凯撒密码 -->

                        <div class="row standalone-row align-items-center">

                            <div class="col-lg-6 order-lg-2 px-md-0">

                                <div class="blog-image wow hover-effect fadeInRightBig text-center text-lg-right">

                                    <div class="box">

                                        <img src="static/picture/111.jpg" alt="image">

                                        <div class="box-content">

                                            <h3 class="name">凯撒密码</h3>

                                        </div>

                                    </div>

                                </div>

                            </div>

                            <div class="col-lg-6 stand-img-des">

                                <div class="d-inline-block wow fadeIn" data-wow-delay=".5s">

                                    <h2 class="heading-text">凯撒密码</h2>

                                    <p class="para\_text" style="text-indent: 2em;">在密码学中，恺撒密码（英语：Caesar cipher），或称恺撒加密、恺撒变换、变换加密，是一种最简单且最广为人知的加密技术。它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。 </p>

                                    <p class="para\_text" style="text-indent: 2em;">​凯撒密码是典型的替换密码。加密原理是把明文中所有的英文字母都在字母表中向后（或向前）按照一个固定 数目进行移位后替换成密文，而数字和非字母字符则保持不变。凯撒密码只有25种可能的密钥。</p>

                                </div>

                            </div>

                        </div>

                        <!-- 维吉尼亚密码 -->

                        <div class="row standalone-row align-items-center">

                            <div class="col-lg-6 px-md-0">

                                <div class="blog-image wow hover-effect fadeInLeftBig text-center text-lg-left">

                                    <div class="box">

                                        <img src="static/picture/2.jpg" alt="image">

                                        <div class="box-content">

                                            <h3 class="name">维吉尼亚密码</h3>

                                        </div>

                                    </div>

                                </div>

                            </div>

                            <div class="col-lg-6 stand-img-des">

                                <div class="d-inline-block wow fadeIn" data-wow-delay=".5s">

                                    <h2 class="heading-text">维吉尼亚密码</h2>

                                    <p class="para\_text" style="text-indent: 2em;">维吉尼亚密码（又译维热纳尔密码）是使用一系列凯撒密码组成密码字母表的加密算法，属于多表密码的一种简单形式。 </p>

                                    <p class="para\_text" style="text-indent: 2em;">维吉尼亚密码以其简单易用而著称，同时初学者通常难以破解，因而又被称为“不可破译的密码”（法语：le chiffre indéchiffrable）。这也让很多人使用维吉尼亚密码来加密的目的就是为了将其破解。 </p>

                                </div>

                            </div>

                        </div>

                    </div>

                </div>

            </div>

        </div>

    </div>

</section>

<!-- 内容结束 -->

<!-- 底部栏 -->

<footer class="footer standalone-footer">

    <div class="container">

        <div class="row align-items-center">

            <!--内容-->

            <div class="col-12">

                <div class="footer-social text-center">

                    <ul class="list-unstyled">

                        <li><a class="wow fadeInUp" href="https://connect.facebook.com"><i aria-hidden="true" class="fab fa-facebook-f"></i><span></span></a></li>

                        <li><a class="wow fadeInDown" href="https://www.twitters.com"><i aria-hidden="true" class="fab fa-twitter"></i><span></span></a></li>

                        <li><a class="wow fadeInUp" href="https://google.cn/"><i aria-hidden="true" class="fab fa-google-plus-g"></i><span></span></a></li>

                        <li><a class="wow fadeInDown" href="https://cn.linkedin.com"><i aria-hidden="true" class="fab fa-linkedin-in"></i><span></span></a></li>

                        <li><a class="wow fadeInUp" href="https://apps.apple.com/ca/app/instagram/id389801252"><i aria-hidden="true" class="fab fa-instagram"></i><span></span></a></li>

                        <li><a class="wow fadeInDown" href="https://www.pinterest.es"><i aria-hidden="true" class="fab fa-pinterest-p"></i><span></span></a></li>

                    </ul>

                </div>

            </div>

            <!--版权-->

            <div class="col-12 text-center mt-3">

                <p class="company-about fadeIn">Copyright &copy; 2022.5.23 朱传伟<a target="\_blank" ></a>

                </p>

            </div>

        </div>

    </div>

</footer>

<!-- 底部栏 -->

<!-- JavaScript -->

<script src="static/js/bundle.min.js"></script>

<script src="static/js/jquery.appear.js"></script>

<script src="static/js/owl.carousel.min.js"></script>

<script src="static/js/wow.min.js"></script>

<script src="static/js/jquery.fancybox.min.js"></script>

<script src="static/js/particles.min.js"></script>

<script src="static/js/contact\_us.js"></script>

<script src="static/js/circle-progress.min.js"></script>

<script src="static/js/script.js"></script>

</body>

</html>

**Jdmmx.html:**

<!DOCTYPE html>

<html lang="zh">

<head>

    <!-- 元标签 -->

    <meta charset="utf-8">

    <meta content="width=device-width, initial-scale=1, shrink-to-fit=no" name="viewport">

    <!-- 作者 -->

    <meta name="author" content="朱传伟">

    <!-- 描述 -->

    <meta name="description" content="古典密码学">

    <!-- 页面标题 -->

    <title>密码学介绍</title>

    <!-- 网站图标 -->

    <link href="static/image/favicon.ico" rel="icon">

    <link href="static/css/bundle.min.css" rel="stylesheet">

    <!-- 插件 CSS -->

    <link href="static/css/owl.carousel.min.css" rel="stylesheet">

    <link rel="stylesheet" href="static/css/LineIcons.min.css">

    <link rel="stylesheet" href="static/css/jquery.fancybox.min.css">

    <!-- 样式表 -->

    <link href="static/css/line-awesome.min.css" rel="stylesheet">

    <link href="static/css/style.css" rel="stylesheet">

    <link href="static/css/custom.css" rel="stylesheet">

</head>

<body>

<!-- 预加载开始 -->

<div class="loader-bg">

    <div class="loader">

        <span></span>

        <span></span>

        <span></span>

        <span></span>

        <span></span>

        <span></span>

        <span></span>

        <span></span>

        <span></span>

        <span></span>

        <span></span>

        <span></span>

        <span></span>

        <span></span>

        <span></span>

    </div>

</div>

<!-- 预加载结束 -->

<!-- 标题开始 -->

<header>

    <!--导航栏-->

    <nav class="navbar navbar-top-default navbar-expand-lg navbar-simple nav-line">

        <div class="container">

            <a href="index.html#slider-area" title="Logo" class="logo scroll">

                <!--Logo-->

                <img src="static/image/favicon.ico" title="logo" alt="logo" class="logo-default">

            </a>

            <!--菜单-->

            <div class="collapse navbar-collapse" id="megaone">

                <div class="navbar-nav ml-auto">

                    <a class="nav-link" href="index.html">简介</a>

                    <a class="nav-link" href="index.html#about">摘要</a>

                    <a class="nav-link" href="index.html#prices">古典密码学</a>

                    <a class="nav-link" href="index.html#hosting">近代密码学</a>

                    <a class="nav-link" href="index.html#testimonials">现代密码学</a>

                    <a class="nav-link" href="index.html#blog">量子密码学</a>

                    <a class="nav-link" href="index.html#contact">联系我</a>

                </div>

            </div>

        </div>

        <div class="navigation-toggle">

            <ul class="slider-social toggle-btn my-0">

                <li>

                    <a href="javascript:void(0);" class="sidemenu\_btn" id="sidemenu\_toggle">

                        <span></span>

                        <span></span>

                        <span></span>

                    </a>

                </li>

            </ul>

        </div>

    </nav>

    <!--侧边导航栏-->

    <div class="side-menu hidden">

        <div class="inner-wrapper">

            <span class="btn-close" id="btn\_sideNavClose"><i></i><i></i></span>

            <a href="index.html" title="Logo" class="logo side-logo">

                <!--Logo-->

                <img src="static/image/favicon.ico" alt="logo">

            </a>

            <nav class="side-nav w-100">

                <ul class="navbar-nav side-navbar">

                    <li class="nav-item">

                        <a class="nav-link" href="index.html">密码学资料</a>

                    </li>

                    <li class="nav-item">

                        <a class="nav-link" href="index.html#about">摘要</a>

                    </li>

                    <li class="nav-item">

                        <a class="nav-link" href="index.html#prices">古典密码学</a>

                    </li>

                    <li class="nav-item">

                        <a class="nav-link" href="index.html#hosting">近代密码学</a>

                    </li>

                    <li class="nav-item">

                        <a class="nav-link" href="index.html#testimonials">现代密码学</a>

                    </li>

                    <li class="nav-item">

                        <a class="nav-link" href="index.html#blog">量子密码学</a>

                    </li>

                    <li class="nav-item">

                        <a class="nav-link" href="index.html#contact">联系我</a>

                    </li>

                </ul>

            </nav>

            <div class="side-footer w-100">

                <ul class="social-icons-simple">

                    <li><a class="social-icon" href="https://connect.facebook.com"><i class="fab fa-facebook-f"></i> </a> </li>

                    <li><a class="social-icon" href="https://www.twitters.com"><i class="fab fa-twitter"></i> </a> </li>

                    <li><a class="social-icon" href="https://cn.linkedin.com"><i class="fab fa-linkedin-in"></i> </a> </li>

                    <li><a class="social-icon" href="https://apps.apple.com/ca/app/instagram/id389801252"><i class="fab fa-instagram"></i> </a> </li>

                </ul>

            </div>

        </div>

    </div>

    <a id="close\_side\_menu" href="javascript:void(0);"></a>

</header>

<!-- 标题结束 -->

<!-- 首页开始 -->

<section class="page-title stand-banner">

    <div class="container">

        <div class="row justify-content-center">

            <div class="col-12 col-lg-10">

                <div class="box-content">

                    <h2 class="hide-cursor wow fadeInUp" data-wow-delay="1.2s">近代密码学</h2>

                    <ul class="page-breadcrumb link wow fadeInUp" data-wow-delay="1.6s">

                        <li><a href="index.html"><span class="icon fas fa-home"></span>密码学资料</a></li>

                        <li>近代密码学</li>

                    </ul>

                </div>

            </div>

        </div>

    </div>

</section>

<!-- 首页结束 -->

<!-- 内容开始 -->

<section class="main" id="main">

    <div class="blog-content">

        <div class="container">

            <div class="row no-gutters">

                <div class="col-12">

                    <!-- 概括内容 -->

                    <div class="standalone-detail">

                        <div class="row no-gutters">

                            <div class="col-12 col-md-10 offset-md-1 col-lg-8 offset-lg-2  text-center wow slideInUp" data-wow-duration="2s">

                                <h1 class="heading">近代密码学</h1>

                                <p class="para\_text m-auto">近代密码学研究信息从发端到收端的安全传输和安全存储，是研究“知己知彼”的一门科学。其核心是密码编码学和密码分析学。前者致力于建立难以被敌方或对手攻破的安全密码体制，即“知己”；后者则力图破译敌方或对手已有的密码体制，即“知彼”。</p>

                            </div>

                        </div>

                    </div>

                    <div class="standalone-area">

                        <!-- 恩尼格玛密码机 -->

                        <div class="row standalone-row align-items-center">

                            <div class="col-lg-6 px-md-0">

                                <div class="blog-image wow hover-effect fadeInLeftBig text-center text-lg-left">

                                    <div class="box">

                                        <img src="static/picture/11.jpg" alt="image">

                                        <div class="box-content">

                                            <h3 class="name">恩尼格玛密码机</h3>

                                        </div>

                                    </div>

                                </div>

                            </div>

                            <div class="col-lg-6 stand-img-des">

                                <div class="d-inline-block wow fadeIn" data-wow-delay=".5s">

                                    <h2 class="heading-text">恩尼格玛密码机</h2>

                                    <p class="para\_text" style="text-indent: 2em;">在密码学史中，恩尼格玛密码机（德语：Enigma，又译哑谜机，或“谜”式密码机）是一种用于加密与解密文件的密码机。确切地说，恩尼格玛是对二战时期纳粹德国使用的一系列相似的转子机械加解密机器的统称，它包括了许多不同的型号，为密码学对称加密算法的流加密。 </p>

                                    <p class="para\_text" style="text-indent: 2em;">栅栏密码的安全性较低，我们可以对其进行扩展。在选择行数时可以使多行，这样对于加密强度有所提高。可以在加密之后在使用其他密码进行加密，增加强度</p>

                                </div>

                            </div>

                        </div>

                        <!-- 希尔密码 -->

                        <div class="row standalone-row align-items-center">

                            <div class="col-lg-6 order-lg-2 px-md-0">

                                <div class="blog-image wow hover-effect fadeInRightBig text-center text-lg-right">

                                    <div class="box">

                                        <img src="static/picture/22.jpg" alt="image">

                                        <div class="box-content">

                                            <h3 class="name">希尔密码</h3>

                                        </div>

                                    </div>

                                </div>

                            </div>

                            <div class="col-lg-6 stand-img-des">

                                <div class="d-inline-block wow fadeIn" data-wow-delay=".5s">

                                    <h2 class="heading-text">希尔密码</h2>

                                    <p class="para\_text" style="text-indent: 2em;">希尔密码（Hill Cipher）是运用基本矩阵论原理的替换密码，由Lester S. Hill在1929年发明。每个字母当作26进制数字：A=0, B=1, C=2... 一串字母当成n维向量，跟一个n×n的矩阵相乘，再将得出的结果MOD26。 </p>

                                    <p class="para\_text" style="text-indent: 2em;">​希尔加密算法的基本思想是，将d个明文字母通过线性变换将它们转换为d个密文字母。解密只要作一次逆变换就可以了，密钥就是变换矩阵本身。</p>

                                </div>

                            </div>

                        </div>

                        <!-- 流密码 -->

                        <div class="row standalone-row align-items-center">

                            <div class="col-lg-6 px-md-0">

                                <div class="blog-image wow hover-effect fadeInLeftBig text-center text-lg-left">

                                    <div class="box">

                                        <img src="static/picture/33.jpg" alt="image">

                                        <div class="box-content">

                                            <h3 class="name">流密码</h3>

                                        </div>

                                    </div>

                                </div>

                            </div>

                            <div class="col-lg-6 stand-img-des">

                                <div class="d-inline-block wow fadeIn" data-wow-delay=".5s">

                                    <h2 class="heading-text">流密码</h2>

                                    <p class="para\_text" style="text-indent: 2em;">流密码(streamcipher)也称为序列密码，每次加密处理数据流的一位或一个字节，加解密使用相同的密钥，是对称密码算法的一种。1949年Shannon证明只有一次一密密码体制是绝对安全的，为流密码技术的研究提供了强大的支持，一次一密的密码方案是流密码的雏形。 </p>

                                    <p class="para\_text" style="text-indent: 2em;">流密码分为同步流密码和自同步流密码两种。同步流密码的密钥流的产生独立于明文和密文；自同步流密码的密钥流的产生与密钥和已经产生的固定数量的密文字符有关，即是一种有记忆变换的序列密码。 </p>

                                </div>

                            </div>

                        </div>

                    </div>

                </div>

            </div>

        </div>

    </div>

</section>

<!-- 内容结束 -->

<!-- 底部栏 -->

<footer class="footer standalone-footer">

    <div class="container">

        <div class="row align-items-center">

            <!--内容-->

            <div class="col-12">

                <div class="footer-social text-center">

                    <ul class="list-unstyled">

                        <li><a class="wow fadeInUp" href="https://connect.facebook.com"><i aria-hidden="true" class="fab fa-facebook-f"></i><span></span></a></li>

                        <li><a class="wow fadeInDown" href="https://www.twitters.com"><i aria-hidden="true" class="fab fa-twitter"></i><span></span></a></li>

                        <li><a class="wow fadeInUp" href="https://google.cn/"><i aria-hidden="true" class="fab fa-google-plus-g"></i><span></span></a></li>

                        <li><a class="wow fadeInDown" href="https://cn.linkedin.com"><i aria-hidden="true" class="fab fa-linkedin-in"></i><span></span></a></li>

                        <li><a class="wow fadeInUp" href="https://apps.apple.com/ca/app/instagram/id389801252"><i aria-hidden="true" class="fab fa-instagram"></i><span></span></a></li>

                        <li><a class="wow fadeInDown" href="https://www.pinterest.es"><i aria-hidden="true" class="fab fa-pinterest-p"></i><span></span></a></li>

                    </ul>

                </div>

            </div>

            <!--版权-->

            <div class="col-12 text-center mt-3">

                <p class="company-about fadeIn">Copyright &copy; 2022.5.23 朱传伟<a target="\_blank" ></a>

                </p>

            </div>

        </div>

    </div>

</footer>

<!-- 底部栏 -->

<!-- JavaScript -->

<script src="static/js/bundle.min.js"></script>

<script src="static/js/jquery.appear.js"></script>

<script src="static/js/owl.carousel.min.js"></script>

<script src="static/js/wow.min.js"></script>

<script src="static/js/jquery.fancybox.min.js"></script>

<script src="static/js/particles.min.js"></script>

<script src="static/js/contact\_us.js"></script>

<script src="static/js/circle-progress.min.js"></script>

<script src="static/js/script.js"></script>

</body>

</html>

**Xdmmx.html:**

<!DOCTYPE html>

<html lang="zh">

<head>

    <!-- 元标签 -->

    <meta charset="utf-8">

    <!-- 作者 -->

    <meta name="author" content="朱传伟">

    <!-- 描述 -->

    <meta name="description" content="现代密码学">

    <!-- 页面标题 -->

    <title>密码学介绍</title>

    <!-- 网站图标 -->

    <link href="static/image/favicon.ico" rel="icon">

    <link href="static/css/bundle.min.css" rel="stylesheet">

    <!-- 插件 CSS -->

    <link href="static/css/owl.carousel.min.css" rel="stylesheet">

    <link rel="stylesheet" href="static/css/LineIcons.min.css">

    <link rel="stylesheet" href="static/css/jquery.fancybox.min.css">

    <!-- 样式表 -->

    <link href="static/css/line-awesome.min.css" rel="stylesheet">

    <link href="static/css/style.css" rel="stylesheet">

    <link href="static/css/custom.css" rel="stylesheet">

</head>

<body>

<!-- 预加载开始 -->

<div class="loader-bg">

    <div class="loader">

        <span></span>

        <span></span>

        <span></span>

        <span></span>

        <span></span>

        <span></span>

        <span></span>

        <span></span>

        <span></span>

        <span></span>

        <span></span>

        <span></span>

        <span></span>

        <span></span>

        <span></span>

    </div>

</div>

<!-- 预加载结束 -->

<!-- 标题开始 -->

<header>

    <!--导航栏-->

    <nav class="navbar navbar-top-default navbar-expand-lg navbar-simple nav-line">

        <div class="container">

            <a href="index.html#slider-area" title="Logo" class="logo scroll">

                <!--Logo-->

                <img src="static/image/favicon.ico" title="logo" alt="logo" class="logo-default">

            </a>

            <!--菜单-->

            <div class="collapse navbar-collapse" id="megaone">

                <div class="navbar-nav ml-auto">

                    <a class="nav-link" href="index.html">简介</a>

                    <a class="nav-link" href="index.html#about">摘要</a>

                    <a class="nav-link" href="index.html#prices">古典密码学</a>

                    <a class="nav-link" href="index.html#hosting">近代密码学</a>

                    <a class="nav-link" href="index.html#testimonials">现代密码学</a>

                    <a class="nav-link" href="index.html#blog">量子密码学</a>

                    <a class="nav-link" href="index.html#contact">联系我</a>

                </div>

            </div>

        </div>

        <div class="navigation-toggle">

            <ul class="slider-social toggle-btn my-0">

                <li>

                    <a href="javascript:void(0);" class="sidemenu\_btn" id="sidemenu\_toggle">

                        <span></span>

                        <span></span>

                        <span></span>

                    </a>

                </li>

            </ul>

        </div>

    </nav>

    <!--侧边导航栏-->

    <div class="side-menu hidden">

        <div class="inner-wrapper">

            <span class="btn-close" id="btn\_sideNavClose"><i></i><i></i></span>

            <a href="index.html" title="Logo" class="logo side-logo">

                <!--Logo-->

                <img src="static/image/favicon.ico" alt="logo">

            </a>

            <nav class="side-nav w-100">

                <ul class="navbar-nav side-navbar">

                    <li class="nav-item">

                        <a class="nav-link" href="index.html">密码学资料</a>

                    </li>

                    <li class="nav-item">

                        <a class="nav-link" href="index.html#about">摘要</a>

                    </li>

                    <li class="nav-item">

                        <a class="nav-link" href="index.html#prices">古典密码学</a>

                    </li>

                    <li class="nav-item">

                        <a class="nav-link" href="index.html#hosting">近代密码学</a>

                    </li>

                    <li class="nav-item">

                        <a class="nav-link" href="index.html#testimonials">现代密码学</a>

                    </li>

                    <li class="nav-item">

                        <a class="nav-link" href="index.html#blog">量子密码学</a>

                    </li>

                    <li class="nav-item">

                        <a class="nav-link" href="index.html#contact">联系我</a>

                    </li>

                </ul>

            </nav>

            <div class="side-footer w-100">

                <ul class="social-icons-simple">

                    <li><a class="social-icon" href="https://connect.facebook.com"><i class="fab fa-facebook-f"></i> </a> </li>

                    <li><a class="social-icon" href="https://www.twitters.com"><i class="fab fa-twitter"></i> </a> </li>

                    <li><a class="social-icon" href="https://cn.linkedin.com"><i class="fab fa-linkedin-in"></i> </a> </li>

                    <li><a class="social-icon" href="https://apps.apple.com/ca/app/instagram/id389801252"><i class="fab fa-instagram"></i> </a> </li>

                </ul>

            </div>

        </div>

    </div>

    <a id="close\_side\_menu" href="javascript:void(0);"></a>

</header>

<!-- 标题结束 -->

<!-- 首页开始 -->

<section class="page-title stand-banner">

    <div class="container">

        <div class="row justify-content-center">

            <div class="col-12 col-lg-10">

                <div class="box-content">

                    <h2 class="hide-cursor wow fadeInUp" data-wow-delay="1.2s">现代密码学</h2>

                    <ul class="page-breadcrumb link wow fadeInUp" data-wow-delay="1.6s">

                        <li><a href="index.html"><span class="icon fas fa-home"></span>密码学资料</a></li>

                        <li>现代密码学</li>

                    </ul>

                </div>

            </div>

        </div>

    </div>

</section>

<!-- 首页结束 -->

<!-- 内容开始 -->

<section class="main" id="main">

    <div class="blog-content">

        <div class="container">

            <div class="row no-gutters">

                <div class="col-12">

                    <!-- 概括内容 -->

                    <div class="standalone-detail">

                        <div class="row no-gutters">

                            <div class="col-12 col-md-10 offset-md-1 col-lg-8 offset-lg-2  text-center wow slideInUp" data-wow-duration="2s">

                                <h1 class="heading">现代密码学</h1>

                                <p class="para\_text m-auto">古典密码学是密码学中的一个类型，其大部分加密方式都是利用置换式密码或代换式密码，有时则是两者的混合。古典密码在历史中经常使用，但现代已经很少使用，大部分的已经不再安全了。一般而言，古典密码是基于一个拼音字母（像是 A-Z）、动手操作或是简单的设备。</p>

                            </div>

                        </div>

                    </div>

                    <div class="standalone-area">

                        <!-- 栅栏密码 -->

                        <div class="row standalone-row align-items-center">

                            <div class="col-lg-6 px-md-0">

                                <div class="blog-image wow hover-effect fadeInLeftBig text-center text-lg-left">

                                    <div class="box">

                                        <img src="static/picture/1.png" alt="image">

                                        <div class="box-content">

                                            <h3 class="name">栅栏密码</h3>

                                        </div>

                                    </div>

                                </div>

                            </div>

                            <div class="col-lg-6 stand-img-des">

                                <div class="d-inline-block wow fadeIn" data-wow-delay=".5s">

                                    <h2 class="heading-text">栅栏密码</h2>

                                    <p class="para\_text" style="text-indent: 2em;">栅栏密码是经典的换位密码，就是把要加密的明文分成N个一组，然后把每组的第1个字连起来，形成一段无规律的话。 不过栅栏密码本身有一个潜规则，就是组成栅栏的字母一般不会太多。 </p>

                                    <p class="para\_text" style="text-indent: 2em;">栅栏密码的安全性较低，我们可以对其进行扩展。在选择行数时可以使多行，这样对于加密强度有所提高。可以在加密之后在使用其他密码进行加密，增加强度</p>

                                </div>

                            </div>

                        </div>

                        <!-- 凯撒密码 -->

                        <div class="row standalone-row align-items-center">

                            <div class="col-lg-6 order-lg-2 px-md-0">

                                <div class="blog-image wow hover-effect fadeInRightBig text-center text-lg-right">

                                    <div class="box">

                                        <img src="static/picture/111.jpg" alt="image">

                                        <div class="box-content">

                                            <h3 class="name">凯撒密码</h3>

                                        </div>

                                    </div>

                                </div>

                            </div>

                            <div class="col-lg-6 stand-img-des">

                                <div class="d-inline-block wow fadeIn" data-wow-delay=".5s">

                                    <h2 class="heading-text">凯撒密码</h2>

                                    <p class="para\_text" style="text-indent: 2em;">在密码学中，恺撒密码（英语：Caesar cipher），或称恺撒加密、恺撒变换、变换加密，是一种最简单且最广为人知的加密技术。它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。 </p>

                                    <p class="para\_text" style="text-indent: 2em;">​凯撒密码是典型的替换密码。加密原理是把明文中所有的英文字母都在字母表中向后（或向前）按照一个固定 数目进行移位后替换成密文，而数字和非字母字符则保持不变。凯撒密码只有25种可能的密钥。</p>

                                </div>

                            </div>

                        </div>

                        <!-- 维吉尼亚密码 -->

                        <div class="row standalone-row align-items-center">

                            <div class="col-lg-6 px-md-0">

                                <div class="blog-image wow hover-effect fadeInLeftBig text-center text-lg-left">

                                    <div class="box">

                                        <img src="static/picture/2.jpg" alt="image">

                                        <div class="box-content">

                                            <h3 class="name">维吉尼亚密码</h3>

                                        </div>

                                    </div>

                                </div>

                            </div>

                            <div class="col-lg-6 stand-img-des">

                                <div class="d-inline-block wow fadeIn" data-wow-delay=".5s">

                                    <h2 class="heading-text">维吉尼亚密码</h2>

                                    <p class="para\_text" style="text-indent: 2em;">维吉尼亚密码（又译维热纳尔密码）是使用一系列凯撒密码组成密码字母表的加密算法，属于多表密码的一种简单形式。 </p>

                                    <p class="para\_text" style="text-indent: 2em;">维吉尼亚密码以其简单易用而著称，同时初学者通常难以破解，因而又被称为“不可破译的密码”（法语：le chiffre indéchiffrable）。这也让很多人使用维吉尼亚密码来加密的目的就是为了将其破解。 </p>

                                </div>

                            </div>

                        </div>

                    </div>

                </div>

            </div>

        </div>

    </div>

</section>

<!-- 内容结束 -->

<!-- 底部栏 -->

<footer class="footer standalone-footer">

    <div class="container">

        <div class="row align-items-center">

            <!--内容-->

            <div class="col-12">

                <div class="footer-social text-center">

                    <ul class="list-unstyled">

                        <li><a class="wow fadeInUp" href="https://connect.facebook.com"><i aria-hidden="true" class="fab fa-facebook-f"></i><span></span></a></li>

                        <li><a class="wow fadeInDown" href="https://www.twitters.com"><i aria-hidden="true" class="fab fa-twitter"></i><span></span></a></li>

                        <li><a class="wow fadeInUp" href="https://google.cn/"><i aria-hidden="true" class="fab fa-google-plus-g"></i><span></span></a></li>

                        <li><a class="wow fadeInDown" href="https://cn.linkedin.com"><i aria-hidden="true" class="fab fa-linkedin-in"></i><span></span></a></li>

                        <li><a class="wow fadeInUp" href="https://apps.apple.com/ca/app/instagram/id389801252"><i aria-hidden="true" class="fab fa-instagram"></i><span></span></a></li>

                        <li><a class="wow fadeInDown" href="https://www.pinterest.es"><i aria-hidden="true" class="fab fa-pinterest-p"></i><span></span></a></li>

                    </ul>

                </div>

            </div>

            <!--版权-->

            <div class="col-12 text-center mt-3">

                <p class="company-about fadeIn">Copyright &copy; 2022.5.23 朱传伟<a target="\_blank" ></a>

                </p>

            </div>

        </div>

    </div>

</footer>

<!-- 底部栏 -->

<!-- JavaScript -->

<script src="static/js/bundle.min.js"></script>

<script src="static/js/jquery.appear.js"></script>

<script src="static/js/owl.carousel.min.js"></script>

<script src="static/js/wow.min.js"></script>

<script src="static/js/jquery.fancybox.min.js"></script>

<script src="static/js/particles.min.js"></script>

<script src="static/js/contact\_us.js"></script>

<script src="static/js/circle-progress.min.js"></script>

<script src="static/js/script.js"></script>

</body>

</html>

**AES.html:**

<!DOCTYPE html>

<html lang="zh">

<head>

    <!-- 元标签 -->

    <meta charset="utf-8">

    <!-- 作者 -->

    <meta name="author" content="朱传伟">

    <!-- 描述 -->

    <meta name="description" content="现代密码学">

    <!-- 页面标题 -->

    <title>密码学介绍</title>

    <!-- 网站图标 -->

    <link href="static/image/favicon.ico" rel="icon">

    <link href="static/css/bundle.min.css" rel="stylesheet">

    <!-- 插件 CSS -->

    <link href="static/css/owl.carousel.min.css" rel="stylesheet">

    <link rel="stylesheet" href="static/css/LineIcons.min.css">

    <link rel="stylesheet" href="static/css/jquery.fancybox.min.css">

    <!-- 样式表 -->

    <link href="static/css/line-awesome.min.css" rel="stylesheet">

    <link href="static/css/style.css" rel="stylesheet">

    <link href="static/css/custom.css" rel="stylesheet">

</head>

<body>

<!-- 预加载开始 -->

<div class="loader-bg">

    <div class="loader">

        <span></span>

        <span></span>

        <span></span>

        <span></span>

        <span></span>

        <span></span>

        <span></span>

        <span></span>

        <span></span>

        <span></span>

        <span></span>

        <span></span>

        <span></span>

        <span></span>

        <span></span>

    </div>

</div>

<!-- 预加载结束 -->

<!-- 标题开始 -->

<header>

    <!--导航栏-->

    <nav class="navbar navbar-top-default navbar-expand-lg navbar-simple nav-line">

        <div class="container">

            <a href="index.html#slider-area" title="Logo" class="logo scroll">

                <!--Logo-->

                <img src="static/image/favicon.ico" title="logo" alt="logo" class="logo-default">

            </a>

            <!--菜单-->

            <div class="collapse navbar-collapse" id="megaone">

                <div class="navbar-nav ml-auto">

                    <a class="nav-link" href="index.html">简介</a>

                    <a class="nav-link" href="index.html#about">摘要</a>

                    <a class="nav-link" href="index.html#prices">古典密码学</a>

                    <a class="nav-link" href="index.html#hosting">近代密码学</a>

                    <a class="nav-link" href="index.html#testimonials">现代密码学</a>

                    <a class="nav-link" href="index.html#blog">量子密码学</a>

                    <a class="nav-link" href="index.html#contact">联系我</a>

                </div>

            </div>

        </div>

        <div class="navigation-toggle">

            <ul class="slider-social toggle-btn my-0">

                <li>

                    <a href="javascript:void(0);" class="sidemenu\_btn" id="sidemenu\_toggle">

                        <span></span>

                        <span></span>

                        <span></span>

                    </a>

                </li>

            </ul>

        </div>

    </nav>

    <!--侧边导航栏-->

    <div class="side-menu hidden">

        <div class="inner-wrapper">

            <span class="btn-close" id="btn\_sideNavClose"><i></i><i></i></span>

            <a href="index.html" title="Logo" class="logo side-logo">

                <!--Logo-->

                <img src="static/image/favicon.ico" alt="logo">

            </a>

            <nav class="side-nav w-100">

                <ul class="navbar-nav side-navbar">

                    <li class="nav-item">

                        <a class="nav-link" href="index.html">密码学资料</a>

                    </li>

                    <li class="nav-item">

                        <a class="nav-link" href="index.html#about">摘要</a>

                    </li>

                    <li class="nav-item">

                        <a class="nav-link" href="index.html#prices">古典密码学</a>

                    </li>

                    <li class="nav-item">

                        <a class="nav-link" href="index.html#hosting">近代密码学</a>

                    </li>

                    <li class="nav-item">

                        <a class="nav-link" href="index.html#testimonials">现代密码学</a>

                    </li>

                    <li class="nav-item">

                        <a class="nav-link" href="index.html#blog">量子密码学</a>

                    </li>

                    <li class="nav-item">

                        <a class="nav-link" href="index.html#contact">联系我</a>

                    </li>

                </ul>

            </nav>

            <div class="side-footer w-100">

                <ul class="social-icons-simple">

                    <li><a class="social-icon" href="https://connect.facebook.com"><i class="fab fa-facebook-f"></i> </a> </li>

                    <li><a class="social-icon" href="https://www.twitters.com"><i class="fab fa-twitter"></i> </a> </li>

                    <li><a class="social-icon" href="https://cn.linkedin.com"><i class="fab fa-linkedin-in"></i> </a> </li>

                    <li><a class="social-icon" href="https://apps.apple.com/ca/app/instagram/id389801252"><i class="fab fa-instagram"></i> </a> </li>

                </ul>

            </div>

        </div>

    </div>

</header>

<!-- 标题结束 -->

<!-- 首页开始 -->

<section class="page-title stand-banner">

    <div class="container">

        <div class="row justify-content-center">

            <div class="col-12 col-lg-10">

                <div class="box-content">

                    <h2 class="hide-cursor wow fadeInUp" data-wow-delay="1.2s">AES加密算法</h2>

                    <ul class="page-breadcrumb link wow fadeInUp" data-wow-delay="1.6s">

                        <li><a href="index.html"><span class="icon fas fa-home"></span>密码学资料</a></li>

                        <li>AES加密算法</li>

                    </ul>

                </div>

            </div>

        </div>

    </div>

</section>

<!-- 首页结束 -->

<!-- 内容开始 -->

<section class="main" id="main">

    <div class="blog-content">

        <div class="container">

            <div class="row no-gutters">

                <div class="col-12">

                    <!-- 概括内容 -->

                    <div class="standalone-detail">

                        <div class="row no-gutters">

                            <div class="col-12 col-md-10 offset-md-1 col-lg-8 offset-lg-2  text-center wow slideInUp" data-wow-duration="2s">

                                <h1 class="heading">AES加密算法</h1>

                                <p class="para\_text m-auto";style="text-indent:2em;">密码学中的高级加密标准（Advanced Encryption Standard，AES），又称Rijndael加密法，是美国联邦政府采用的一种区块加密标准。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。</p>

                            </div>

                        </div>

                    </div>

                    <div class="standalone-area">

                        <!-- 加密流程 -->

                        <div class="row standalone-row align-items-center">

                            <div class="col-lg-6 px-md-0">

                                <div class="blog-image wow hover-effect fadeInLeftBig text-center text-lg-left">

                                    <div class="box">

                                        <img src="static/picture/qqq.png" alt="image">

                                        <div class="box-content">

                                            <h3 class="name">加密流程</h3>

                                        </div>

                                    </div>

                                </div>

                            </div>

                            <div class="col-lg-6 stand-img-des">

                                <div class="d-inline-block wow fadeIn" data-wow-delay=".5s">

                                    <h2 class="heading-text">加密流程</h2>

                                    <p class="para\_text" style="text-indent: 2em;">1. 严格地说，AES和Rijndael加密法并不完全一样（虽然在实际应用中二者可以互换），因为Rijndael加密法可以支持更大范围的区块和密钥长度：AES的区块长度固定为128位，密钥长度则可以是128，192或256位；而Rijndael使用的密钥和区块长度可以是32位的整数倍，以128位为下限，256位为上限。加密过程中使用的密钥是由Rijndael密钥生成方案产生。 </p>

                                    <p class="para\_text" style="text-indent: 2em;">2. AES加密过程是在一个4×4的字节矩阵上运作，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，AddRoundKey，ShiftRows，MixColumns。</p>

                                </div>

                            </div>

                        </div>

                        <!-- AES加密模式 -->

                        <div class="row standalone-row align-items-center">

                            <div class="col-lg-6 order-lg-2 px-md-0">

                                <div class="blog-image wow hover-effect fadeInRightBig text-center text-lg-right">

                                    <div class="box">

                                        <img src="static/picture/eee.jpg" alt="image">

                                        <div class="box-content">

                                            <h3 class="name">AES加密模式</h3>

                                        </div>

                                    </div>

                                </div>

                            </div>

                            <div class="col-lg-6 stand-img-des">

                                <div class="d-inline-block wow fadeIn" data-wow-delay=".5s">

                                    <h2 class="heading-text">AES加密模式</h2>

                                    <p class="para\_text" style="text-indent: 2em;">1. 对称/分组密码一般分为流加密(如OFB、CFB等)和块加密(如ECB、CBC等)。对于流加密，需要将分组密码转化为流模式工作。对于块加密(或称分组加密)，如果要加密超过块大小的数据，就需要涉及填充和链加密模式。 </p>

                                    <p class="para\_text" style="text-indent: 2em;">2. ​ECB模式是最早采用和最简单的模式，它将加密的数据分成若干组，每组的大小跟加密密钥长度相同，然后每组都用相同的密钥进行加密</p>

                                </div>

                            </div>

                        </div>

                        <!-- 攻击方法 -->

                        <div class="row standalone-row align-items-center">

                            <div class="col-lg-6 px-md-0">

                                <div class="blog-image wow hover-effect fadeInLeftBig text-center text-lg-left">

                                    <div class="box">

                                        <img src="static/picture/www.jpg" alt="image">

                                        <div class="box-content">

                                            <h3 class="name">攻击方法</h3>

                                        </div>

                                    </div>

                                </div>

                            </div>

                            <div class="col-lg-6 stand-img-des">

                                <div class="d-inline-block wow fadeIn" data-wow-delay=".5s">

                                    <h2 class="heading-text">攻击方法</h2>

                                    <p class="para\_text" style="text-indent: 2em;">1. 2005年4月，D.J. Bernstein公布了一种缓存时序攻击法，他以此破解了一个装载OpenSSL AES加密系统的客户服务器。为了设计使该服务器公布所有的时序信息，攻击算法使用了2亿多条筛选过的明码。有人认为，对于需要多个跳跃的国际互联网而言，这样的攻击方法并不实用。 </p>

                                    <p class="para\_text" style="text-indent: 2em;">2. 2005年10月，Eran Tromer和另外两个研究员发表了一篇论文，展示了数种针对AES的缓存时序攻击法[8]。其中一种攻击法只需要800个写入动作，费时65毫秒，就能得到一把完整的AES密钥。但攻击者必须在运行加密的系统上拥有运行程序的权限，方能以此法破解该密码系统。 </p>

                                </div>

                            </div>

                        </div>

                    </div>

                </div>

            </div>

        </div>

    </div>

</section>

<!-- 内容结束 -->

<!-- 底部栏 -->

<footer class="footer standalone-footer">

    <div class="container">

        <div class="row align-items-center">

            <!--内容-->

            <div class="col-12">

                <div class="footer-social text-center">

                    <ul class="list-unstyled">

                        <li><a class="wow fadeInUp" href="https://connect.facebook.com"><i aria-hidden="true" class="fab fa-facebook-f"></i><span></span></a></li>

                        <li><a class="wow fadeInDown" href="https://www.twitters.com"><i aria-hidden="true" class="fab fa-twitter"></i><span></span></a></li>

                        <li><a class="wow fadeInUp" href="https://google.cn/"><i aria-hidden="true" class="fab fa-google-plus-g"></i><span></span></a></li>

                        <li><a class="wow fadeInDown" href="https://cn.linkedin.com"><i aria-hidden="true" class="fab fa-linkedin-in"></i><span></span></a></li>

                        <li><a class="wow fadeInUp" href="https://apps.apple.com/ca/app/instagram/id389801252"><i aria-hidden="true" class="fab fa-instagram"></i><span></span></a></li>

                        <li><a class="wow fadeInDown" href="https://www.pinterest.es"><i aria-hidden="true" class="fab fa-pinterest-p"></i><span></span></a></li>

                    </ul>

                </div>

            </div>

            <!--版权-->

            <div class="col-12 text-center mt-3">

                <p class="company-about fadeIn">Copyright &copy; 2022.5.23 朱传伟<a target="\_blank" ></a>

                </p>

            </div>

        </div>

    </div>

</footer>

<!-- 底部栏 -->

<!-- JavaScript -->

<script src="static/js/bundle.min.js"></script>

<script src="static/js/jquery.appear.js"></script>

<script src="static/js/owl.carousel.min.js"></script>

<script src="static/js/wow.min.js"></script>

<script src="static/js/jquery.fancybox.min.js"></script>

<script src="static/js/particles.min.js"></script>

<script src="static/js/contact\_us.js"></script>

<script src="static/js/circle-progress.min.js"></script>

<script src="static/js/script.js"></script>

</body>

</html>

**RSA.html:**

<!DOCTYPE html>

<html lang="zh">

<head>

    <!-- 元标签 -->

    <meta charset="utf-8">

    <!-- 作者 -->

    <meta name="author" content="朱传伟">

    <!-- 描述 -->

    <meta name="description" content="现代密码学">

    <!-- 页面标题 -->

    <title>密码学介绍</title>

    <!-- 网站图标 -->

    <link href="static/image/favicon.ico" rel="icon">

    <link href="static/css/bundle.min.css" rel="stylesheet">

    <!-- 插件 CSS -->

    <link href="static/css/owl.carousel.min.css" rel="stylesheet">

    <link rel="stylesheet" href="static/css/LineIcons.min.css">

    <link rel="stylesheet" href="static/css/jquery.fancybox.min.css">

    <!-- 样式表 -->

    <link href="static/css/line-awesome.min.css" rel="stylesheet">

    <link href="static/css/style.css" rel="stylesheet">

    <link href="static/css/custom.css" rel="stylesheet">

</head>

<body>

<!-- 预加载开始 -->

<div class="loader-bg">

    <div class="loader">

        <span></span>

        <span></span>

        <span></span>

        <span></span>

        <span></span>

        <span></span>

        <span></span>

        <span></span>

        <span></span>

        <span></span>

        <span></span>

        <span></span>

        <span></span>

        <span></span>

        <span></span>

    </div>

</div>

<!-- 预加载结束 -->

<!-- 标题开始 -->

<header>

    <!--导航栏-->

    <nav class="navbar navbar-top-default navbar-expand-lg navbar-simple nav-line">

        <div class="container">

            <a href="index.html#slider-area" title="Logo" class="logo scroll">

                <!--Logo-->

                <img src="static/image/favicon.ico" title="logo" alt="logo" class="logo-default">

            </a>

            <!--菜单-->

            <div class="collapse navbar-collapse" id="megaone">

                <div class="navbar-nav ml-auto">

                    <a class="nav-link" href="index.html">简介</a>

                    <a class="nav-link" href="index.html#about">摘要</a>

                    <a class="nav-link" href="index.html#prices">古典密码学</a>

                    <a class="nav-link" href="index.html#hosting">近代密码学</a>

                    <a class="nav-link" href="index.html#testimonials">现代密码学</a>

                    <a class="nav-link" href="index.html#blog">量子密码学</a>

                    <a class="nav-link" href="index.html#contact">联系我</a>

                </div>

            </div>

        </div>

        <div class="navigation-toggle">

            <ul class="slider-social toggle-btn my-0">

                <li>

                    <a href="javascript:void(0);" class="sidemenu\_btn" id="sidemenu\_toggle">

                        <span></span>

                        <span></span>

                        <span></span>

                    </a>

                </li>

            </ul>

        </div>

    </nav>

    <!--侧边导航栏-->

    <div class="side-menu hidden">

        <div class="inner-wrapper">

            <span class="btn-close" id="btn\_sideNavClose"><i></i><i></i></span>

            <a href="index.html" title="Logo" class="logo side-logo">

                <!--Logo-->

                <img src="static/image/favicon.ico" alt="logo">

            </a>

            <nav class="side-nav w-100">

                <ul class="navbar-nav side-navbar">

                    <li class="nav-item">

                        <a class="nav-link" href="index.html">密码学资料</a>

                    </li>

                    <li class="nav-item">

                        <a class="nav-link" href="index.html#about">摘要</a>

                    </li>

                    <li class="nav-item">

                        <a class="nav-link" href="index.html#prices">古典密码学</a>

                    </li>

                    <li class="nav-item">

                        <a class="nav-link" href="index.html#hosting">近代密码学</a>

                    </li>

                    <li class="nav-item">

                        <a class="nav-link" href="index.html#testimonials">现代密码学</a>

                    </li>

                    <li class="nav-item">

                        <a class="nav-link" href="index.html#blog">量子密码学</a>

                    </li>

                    <li class="nav-item">

                        <a class="nav-link" href="index.html#contact">联系我</a>

                    </li>

                </ul>

            </nav>

            <div class="side-footer w-100">

                <ul class="social-icons-simple">

                    <li><a class="social-icon" href="https://connect.facebook.com"><i class="fab fa-facebook-f"></i> </a> </li>

                    <li><a class="social-icon" href="https://www.twitters.com"><i class="fab fa-twitter"></i> </a> </li>

                    <li><a class="social-icon" href="https://cn.linkedin.com"><i class="fab fa-linkedin-in"></i> </a> </li>

                    <li><a class="social-icon" href="https://apps.apple.com/ca/app/instagram/id389801252"><i class="fab fa-instagram"></i> </a> </li>

                </ul>

            </div>

        </div>

    </div>

    <a id="close\_side\_menu" href="javascript:void(0);"></a>

</header>

<!-- 标题结束 -->

<!-- 首页开始 -->

<section class="page-title stand-banner">

    <div class="container">

        <div class="row justify-content-center">

            <div class="col-12 col-lg-10">

                <div class="box-content">

                    <h2 class="hide-cursor wow fadeInUp" data-wow-delay="1.2s">RSA加密算法</h2>

                    <ul class="page-breadcrumb link wow fadeInUp" data-wow-delay="1.6s">

                        <li><a href="index.html"><span class="icon fas fa-home"></span>密码学资料</a></li>

                        <li>RSA加密算法</li>

                    </ul>

                </div>

            </div>

        </div>

    </div>

</section>

<!-- 首页结束 -->

<!-- 内容开始 -->

<section class="main" id="main">

    <div class="blog-content">

        <div class="container">

            <div class="row no-gutters">

                <div class="col-12">

                    <!-- 概括内容 -->

                    <div class="standalone-detail">

                        <div class="row no-gutters">

                            <div class="col-12 col-md-10 offset-md-1 col-lg-8 offset-lg-2  text-center wow slideInUp" data-wow-duration="2s">

                                <h1 class="heading">RSA加密算法</h1>

                                <p class="para\_text m-auto">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。</p>

                            </div>

                        </div>

                    </div>

                    <div class="standalone-area">

                        <!-- RSA算法描述 -->

                        <div class="row standalone-row align-items-center">

                            <div class="col-lg-6 px-md-0">

                                <div class="blog-image wow hover-effect fadeInLeftBig text-center text-lg-left">

                                    <div class="box">

                                        <img src="static/picture/qwe.jpg" alt="image">

                                        <div class="box-content">

                                            <h3 class="name">RSA算法描述</h3>

                                        </div>

                                    </div>

                                </div>

                            </div>

                            <div class="col-lg-6 stand-img-des">

                                <div class="d-inline-block wow fadeIn" data-wow-delay=".5s">

                                    <h2 class="heading-text">RSA算法描述</h2>

                                    <p class="para\_text" style="text-indent: 2em;">（1）任意选取两个不同的大素数p和q计算乘积 ；  </p>

                                    <p class="para\_text" style="text-indent: 2em;">（2）任意选取一个大整数e，满足 ，整数e用做加密钥（注意：e的选取是很容易的，例如，所有大于p和q的素数都可用）；</p>

                                    <p class="para\_text" style="text-indent: 2em;">（3）确定的解密钥d，满足 ，即 是一个任意的整数；所以，若知道e和，则很容易计算出d；</p>

                                    <p class="para\_text" style="text-indent: 2em;">（4）公开整数n和e，秘密保存d；</p>

                                    <p class="para\_text" style="text-indent: 2em;">（5）将明文m加密成密文c ；</p>

                                    <p class="para\_text" style="text-indent: 2em;">（6）将密文c解密为明文m，解密算法为；</p>

                                </div>

                            </div>

                        </div>

                        <!-- RSA安全性 -->

                        <div class="row standalone-row align-items-center">

                            <div class="col-lg-6 order-lg-2 px-md-0">

                                <div class="blog-image wow hover-effect fadeInRightBig text-center text-lg-right">

                                    <div class="box">

                                        <img src="static/picture/wqe.png" alt="image">

                                        <div class="box-content">

                                            <h3 class="name">RSA安全性</h3>

                                        </div>

                                    </div>

                                </div>

                            </div>

                            <div class="col-lg-6 stand-img-des">

                                <div class="d-inline-block wow fadeIn" data-wow-delay=".5s">

                                    <h2 class="heading-text">RSA安全性</h2>

                                    <p class="para\_text" style="text-indent: 2em;">1. RSA的安全性依赖于大数分解，但是否等同于大数分解一直未能得到理论上的证明，也并没有从理论上证明破译。RSA的难度与大数分解难度等价。因为没有证明破解RSA就一定需要做大数分解。假设存在一种无须分解大数的算法，那它肯定可以修改成为大数分解算法，即RSA的重大缺陷是无法从理论上把握它的保密性能如何，而且密码学界多数人士倾向于因子分解不是NPC问题。 </p>

                                    <p class="para\_text" style="text-indent: 2em;">​2. RSA算法的保密强度随其密钥的长度增加而增强。但是，密钥越长，其加解密所耗用的时间也越长。因此，要根据所保护信息的敏感程度与攻击者破解所要花费的代价值不值得以及系统所要求的反应时间来综合考虑，尤其对于商业信息领域更是如此。</p>

                                </div>

                            </div>

                        </div>

                        <!-- 攻击方法 -->

                        <div class="row standalone-row align-items-center">

                            <div class="col-lg-6 px-md-0">

                                <div class="blog-image wow hover-effect fadeInLeftBig text-center text-lg-left">

                                    <div class="box">

                                        <img src="static/picture/ewq.png" alt="image">

                                        <div class="box-content">

                                            <h3 class="name">攻击方法</h3>

                                        </div>

                                    </div>

                                </div>

                            </div>

                            <div class="col-lg-6 stand-img-des">

                                <div class="d-inline-block wow fadeIn" data-wow-delay=".5s">

                                    <h2 class="heading-text">攻击方法</h2>

                                    <p class="para\_text" style="text-indent: 2em;">1. RSA在选择密码攻击面前显得很脆弱。一般攻击者是将某一信息进行下伪装，让拥有私钥的实体签名；然后，经过计算就可得到它所想要的信息。实际上，攻击利用的都是同一个弱点，即存在这样一个事实：乘幂保留了输入的乘法结构。前面已经提到，这个固有的问题来自于公钥密码系统的最基本的特征，即每个人都能使用公钥加密信息。 </p>

                                    <p class="para\_text" style="text-indent: 2em;">2. 当公钥e取较小的值，虽然会使加密变得易于实现，速度有所提高，但这样做也是不安全的。最简单的办法就是e和d都取较大的值。 </p>

                                </div>

                            </div>

                        </div>

                    </div>

                </div>

            </div>

        </div>

    </div>

</section>

<!-- 内容结束 -->

<!-- 底部栏 -->

<footer class="footer standalone-footer">

    <div class="container">

        <div class="row align-items-center">

            <!--内容-->

            <div class="col-12">

                <div class="footer-social text-center">

                    <ul class="list-unstyled">

                        <li><a class="wow fadeInUp" href="https://connect.facebook.com"><i aria-hidden="true" class="fab fa-facebook-f"></i><span></span></a></li>

                        <li><a class="wow fadeInDown" href="https://www.twitters.com"><i aria-hidden="true" class="fab fa-twitter"></i><span></span></a></li>

                        <li><a class="wow fadeInUp" href="https://google.cn/"><i aria-hidden="true" class="fab fa-google-plus-g"></i><span></span></a></li>

                        <li><a class="wow fadeInDown" href="https://cn.linkedin.com"><i aria-hidden="true" class="fab fa-linkedin-in"></i><span></span></a></li>

                        <li><a class="wow fadeInUp" href="https://apps.apple.com/ca/app/instagram/id389801252"><i aria-hidden="true" class="fab fa-instagram"></i><span></span></a></li>

                        <li><a class="wow fadeInDown" href="https://www.pinterest.es"><i aria-hidden="true" class="fab fa-pinterest-p"></i><span></span></a></li>

                    </ul>

                </div>

            </div>

            <!--版权-->

            <div class="col-12 text-center mt-3">

                <p class="company-about fadeIn">Copyright &copy; 2022.5.23 朱传伟<a target="\_blank" ></a>

                </p>

            </div>

        </div>

    </div>

</footer>

<!-- 底部栏 -->

<!-- JavaScript -->

<script src="static/js/bundle.min.js"></script>

<script src="static/js/jquery.appear.js"></script>

<script src="static/js/owl.carousel.min.js"></script>

<script src="static/js/wow.min.js"></script>

<script src="static/js/jquery.fancybox.min.js"></script>

<script src="static/js/particles.min.js"></script>

<script src="static/js/contact\_us.js"></script>

<script src="static/js/circle-progress.min.js"></script>

<script src="static/js/script.js"></script>

</body>

</html>

**SHA256.html:**

<!DOCTYPE html>

<html lang="zh">

<head>

    <!-- 元标签 -->

    <meta charset="utf-8">

    <!-- 作者 -->

    <meta name="author" content="朱传伟">

    <!-- 描述 -->

    <meta name="description" content="现代密码学">

    <!-- 页面标题 -->

    <title>密码学介绍</title>

    <!-- 网站图标 -->

    <link href="static/image/favicon.ico" rel="icon">

    <link href="static/css/bundle.min.css" rel="stylesheet">

    <!-- 插件 CSS -->

    <link href="static/css/owl.carousel.min.css" rel="stylesheet">

    <link rel="stylesheet" href="static/css/LineIcons.min.css">

    <link rel="stylesheet" href="static/css/jquery.fancybox.min.css">

    <!-- 样式表 -->

    <link href="static/css/line-awesome.min.css" rel="stylesheet">

    <link href="static/css/style.css" rel="stylesheet">

    <link href="static/css/custom.css" rel="stylesheet">

</head>

<body>

<!-- 预加载开始 -->

<div class="loader-bg">

    <div class="loader">

        <span></span>

        <span></span>

        <span></span>

        <span></span>

        <span></span>

        <span></span>

        <span></span>

        <span></span>

        <span></span>

        <span></span>

        <span></span>

        <span></span>

        <span></span>

        <span></span>

        <span></span>

    </div>

</div>

<!-- 预加载结束 -->

<!-- 标题开始 -->

<header>

    <!--导航栏-->

    <nav class="navbar navbar-top-default navbar-expand-lg navbar-simple nav-line">

        <div class="container">

            <a href="index.html#slider-area" title="Logo" class="logo scroll">

                <!--Logo-->

                <img src="static/image/favicon.ico" title="logo" alt="logo" class="logo-default">

            </a>

            <!--菜单-->

            <div class="collapse navbar-collapse" id="megaone">

                <div class="navbar-nav ml-auto">

                    <a class="nav-link" href="index.html">简介</a>

                    <a class="nav-link" href="index.html#about">摘要</a>

                    <a class="nav-link" href="index.html#prices">古典密码学</a>

                    <a class="nav-link" href="index.html#hosting">近代密码学</a>

                    <a class="nav-link" href="index.html#testimonials">现代密码学</a>

                    <a class="nav-link" href="index.html#blog">量子密码学</a>

                    <a class="nav-link" href="index.html#contact">联系我</a>

                </div>

            </div>

        </div>

        <div class="navigation-toggle">

            <ul class="slider-social toggle-btn my-0">

                <li>

                    <a href="javascript:void(0);" class="sidemenu\_btn" id="sidemenu\_toggle">

                        <span></span>

                        <span></span>

                        <span></span>

                    </a>

                </li>

            </ul>

        </div>

    </nav>

    <!--侧边导航栏-->

    <div class="side-menu hidden">

        <div class="inner-wrapper">

            <span class="btn-close" id="btn\_sideNavClose"><i></i><i></i></span>

            <a href="index.html" title="Logo" class="logo side-logo">

                <!--Logo-->

                <img src="static/image/favicon.ico" alt="logo">

            </a>

            <nav class="side-nav w-100">

                <ul class="navbar-nav side-navbar">

                    <li class="nav-item">

                        <a class="nav-link" href="index.html">密码学资料</a>

                    </li>

                    <li class="nav-item">

                        <a class="nav-link" href="index.html#about">摘要</a>

                    </li>

                    <li class="nav-item">

                        <a class="nav-link" href="index.html#prices">古典密码学</a>

                    </li>

                    <li class="nav-item">

                        <a class="nav-link" href="index.html#hosting">近代密码学</a>

                    </li>

                    <li class="nav-item">

                        <a class="nav-link" href="index.html#testimonials">现代密码学</a>

                    </li>

                    <li class="nav-item">

                        <a class="nav-link" href="index.html#blog">量子密码学</a>

                    </li>

                    <li class="nav-item">

                        <a class="nav-link" href="index.html#contact">联系我</a>

                    </li>

                </ul>

            </nav>

            <div class="side-footer w-100">

                <ul class="social-icons-simple">

                    <li><a class="social-icon" href="https://connect.facebook.com"><i class="fab fa-facebook-f"></i> </a> </li>

                    <li><a class="social-icon" href="https://www.twitters.com"><i class="fab fa-twitter"></i> </a> </li>

                    <li><a class="social-icon" href="https://cn.linkedin.com"><i class="fab fa-linkedin-in"></i> </a> </li>

                    <li><a class="social-icon" href="https://apps.apple.com/ca/app/instagram/id389801252"><i class="fab fa-instagram"></i> </a> </li>

                </ul>

            </div>

        </div>

    </div>

    <a id="close\_side\_menu" href="javascript:void(0);"></a>

</header>

<!-- 标题结束 -->

<!-- 首页开始 -->

<section class="page-title stand-banner">

    <div class="container">

        <div class="row justify-content-center">

            <div class="col-12 col-lg-10">

                <div class="box-content">

                    <h2 class="hide-cursor wow fadeInUp" data-wow-delay="1.2s">SHA256算法</h2>

                    <ul class="page-breadcrumb link wow fadeInUp" data-wow-delay="1.6s">

                        <li><a href="index.html"><span class="icon fas fa-home"></span>密码学资料</a></li>

                        <li>SHA256算法</li>

                    </ul>

                </div>

            </div>

        </div>

    </div>

</section>

<!-- 首页结束 -->

<!-- 内容开始 -->

<section class="main" id="main">

    <div class="blog-content">

        <div class="container">

            <div class="row no-gutters">

                <div class="col-12">

                    <!-- 概括内容 -->

                    <div class="standalone-detail">

                        <div class="row no-gutters">

                            <div class="col-12 col-md-10 offset-md-1 col-lg-8 offset-lg-2  text-center wow slideInUp" data-wow-duration="2s">

                                <h1 class="heading">SHA256算法</h1>

                                <p class="para\_text m-auto">安全散列算法（英语：Secure Hash Algorithm，缩写为SHA）是一个密码散列函数家族，是FIPS所认证的安全散列算法。能计算出一个数字消息所对应到的，长度固定的字符串（又称消息摘要）的算法。且若输入的消息不同，它们对应到不同字符串的机率很高。</p>

                            </div>

                        </div>

                    </div>

                    <div class="standalone-area">

                        <!-- 算法分析 -->

                        <div class="row standalone-row align-items-center">

                            <div class="col-lg-6 px-md-0">

                                <div class="blog-image wow hover-effect fadeInLeftBig text-center text-lg-left">

                                    <div class="box">

                                        <img src="static/picture/asd.png" alt="image">

                                        <div class="box-content">

                                            <h3 class="name">算法分析</h3>

                                        </div>

                                    </div>

                                </div>

                            </div>

                            <div class="col-lg-6 stand-img-des">

                                <div class="d-inline-block wow fadeIn" data-wow-delay=".5s">

                                    <h2 class="heading-text">算法分析</h2>

                                    <p class="para\_text" style="text-indent: 2em;">1. SHA-256和SHA-512是很新的杂凑函数，前者以定义一个word为32位元，后者则定义一个word为64位元。它们分别使用了不同的偏移量，或用不同的常数，然而，实际上二者结构是相同的，只在循环执行的次数上有所差异。SHA-224以及SHA-384则是前述二种杂凑函数的截短版，利用不同的初始值做计算。 </p>

                                    <p class="para\_text" style="text-indent: 2em;">2. 这些新的杂凑函数并没有接受像SHA-1一样的公众密码社群做详细的检验，所以它们的密码安全性还不被大家广泛的信任。Gilbert和Handschuh在2003年曾对这些新变种作过一些研究，声称他们没有找到弱点。</p>

                                </div>

                            </div>

                        </div>

                        <!-- SHA256应用 -->

                        <div class="row standalone-row align-items-center">

                            <div class="col-lg-6 order-lg-2 px-md-0">

                                <div class="blog-image wow hover-effect fadeInRightBig text-center text-lg-right">

                                    <div class="box">

                                        <img src="static/picture/sad.jpg" alt="image">

                                        <div class="box-content">

                                            <h3 class="name">SHA256应用</h3>

                                        </div>

                                    </div>

                                </div>

                            </div>

                            <div class="col-lg-6 stand-img-des">

                                <div class="d-inline-block wow fadeIn" data-wow-delay=".5s">

                                    <h2 class="heading-text">SHA256应用</h2>

                                    <p class="para\_text" style="text-indent: 2em;">1. SHA-1, SHA-224, SHA-256, SHA-384 和 SHA-512 都被需要安全杂凑算法的美国联邦政府所应用，他们也使用其他的密码算法和协定来保护敏感的未保密资料。FIPS PUB 180-1也鼓励私人或商业组织使用 SHA-1 加密。Fritz-chip 将很可能使用 SHA-1 杂凑函数来实现个人电脑上的数位版权管理。 </p>

                                    <p class="para\_text" style="text-indent: 2em;">​2. 首先推动安全杂凑算法出版的是已合并的数位签章标准。SHA 杂凑函数已被做为 SHACAL 分组密码算法的基础。</p>

                                </div>

                            </div>

                        </div>

                        <!-- 攻击方法 -->

                        <div class="row standalone-row align-items-center">

                            <div class="col-lg-6 px-md-0">

                                <div class="blog-image wow hover-effect fadeInLeftBig text-center text-lg-left">

                                    <div class="box">

                                        <img src="static/picture/dsa.png" alt="image">

                                        <div class="box-content">

                                            <h3 class="name">攻击方法</h3>

                                        </div>

                                    </div>

                                </div>

                            </div>

                            <div class="col-lg-6 stand-img-des">

                                <div class="d-inline-block wow fadeIn" data-wow-delay=".5s">

                                    <h2 class="heading-text">攻击方法</h2>

                                    <p class="para\_text" style="text-indent: 2em;">1. Hash函数是将任意长度的消息压缩到某一固定长度的消息摘要。所以是有可能使得不同消息的Hash摘要是一样的，这就是Hash碰撞攻击。</p>

                                    <p class="para\_text" style="text-indent: 2em;">2. 证据表明，攻击者必须在拥有原始文件和已知哈希的情况下才能完成碰撞攻击，另外，由于攻击利用了定向编辑，不是每次编辑都会有效。换句话说，即使是破解了SSH或TLS的认证证书，也都不可能实现，需要对原始文件进行一些非常细微的定向更改才能保证碰撞攻击成功。 </p>

                                    <p class="para\_text" style="text-indent: 2em;">3. 在经过两年的联合研究和花费了巨大的计算机时间之后，研究人员在他们的研究网站 SHAttered 上给出了两个内容不同，但是具有相同 SHA-1 消息摘要的 PDF 文件（PDF 1、 PDF 2），这就意味着在理论研究长期以来警示 SHA-1 算法存在风险之后，SHA-1 算法的实际攻击案例也浮出水面，同时也标志着 SHA-1 算法终于走向了生命的末期。</p>

                                </div>

                            </div>

                        </div>

                    </div>

                </div>

            </div>

        </div>

    </div>

</section>

<!-- 内容结束 -->

<!-- 底部栏 -->

<footer class="footer standalone-footer">

    <div class="container">

        <div class="row align-items-center">

            <!--内容-->

            <div class="col-12">

                <div class="footer-social text-center">

                    <ul class="list-unstyled">

                        <li><a class="wow fadeInUp" href="https://connect.facebook.com"><i aria-hidden="true" class="fab fa-facebook-f"></i><span></span></a></li>

                        <li><a class="wow fadeInDown" href="https://www.twitters.com"><i aria-hidden="true" class="fab fa-twitter"></i><span></span></a></li>

                        <li><a class="wow fadeInUp" href="https://google.cn/"><i aria-hidden="true" class="fab fa-google-plus-g"></i><span></span></a></li>

                        <li><a class="wow fadeInDown" href="https://cn.linkedin.com"><i aria-hidden="true" class="fab fa-linkedin-in"></i><span></span></a></li>

                        <li><a class="wow fadeInUp" href="https://apps.apple.com/ca/app/instagram/id389801252"><i aria-hidden="true" class="fab fa-instagram"></i><span></span></a></li>

                        <li><a class="wow fadeInDown" href="https://www.pinterest.es"><i aria-hidden="true" class="fab fa-pinterest-p"></i><span></span></a></li>

                    </ul>

                </div>

            </div>

            <!--版权-->

            <div class="col-12 text-center mt-3">

                <p class="company-about fadeIn">Copyright &copy; 2022.5.23 朱传伟<a target="\_blank" ></a>

                </p>

            </div>

        </div>

    </div>

</footer>

<!-- 底部栏 -->

<!-- JavaScript -->

<script src="static/js/bundle.min.js"></script>

<script src="static/js/jquery.appear.js"></script>

<script src="static/js/owl.carousel.min.js"></script>

<script src="static/js/wow.min.js"></script>

<script src="static/js/jquery.fancybox.min.js"></script>

<script src="static/js/particles.min.js"></script>

<script src="static/js/contact\_us.js"></script>

<script src="static/js/circle-progress.min.js"></script>

<script src="static/js/script.js"></script>

</body>

</html>