第一章 绪论

1.1 研究背景

这是一个信息时代，信息收发次数频繁，传播途径广，包含内容大。使得信息的地位举足轻重。虽然信息不是看得见摸得着的直接资源，但是它会间接的带来物质和精神上的富足。如果信息不正确，那根据信息做出的决策也一定是错误的。信息和我们的生活息息相关并改变着我们的生活。信息也已步入国家支持发展的行列,所以当今世界发展的必然趋势是信息全球化。而问题也随之而来了，怎么能保证信息的安全性呢？怎么能保证信息的内容不被第三方获取呢？人们对信息安全的认识也从最初的知之甚少变得越来越全面。

1970 年前后是主机时代，信息安全是面向单机的，那个时期最主要的用户是军方，他们要求信息安全就是信息不泄露。

1980 年前后,微机和局城网的兴起带来了不可避免的问题，信息在微机间的传输、用户间的共享问题成为了最有代表性的两个问题。问题的出现却带来了人们对信息安全的进一步认识，通过微机和用户的交互、使人们认识到数据完整性、可用性是多么重要。这个时代信息安全的重要内容就是服务的安全和运行机制的安全。

1990 年前后,因特网的迅速发展把信息传输带入一个新的时代。资源共享、跨越时空、和实时交互是因特网的主要特点。因特网用户成了主角，其中的问题也接踵而至，因特网系统庞大且复杂，该如何保证用户的隐私安全呢？这就成为了该时代的代表性问题。因特网的特点就如同网一样，覆盖广，连接紧密但却有弱点。它也具有普遍性，任何人都可以自由接入，不过接入者的善恶也是个不定因素。恶者会对网络运行环境进行破坏，以达到自己的目的，获取想要得到的信息。信息的攻击也多种多样，无法确定来源、种类、攻击方式。所以想要保证信息安全，首先要了解信息安全的威胁来自哪个方面。

信息安全的威胁很多，种类更是各种各样，攻击为了避免被破解还要保证时刻变化。信息安全的威胁可能来自于磁场干扰，线路老化、断裂，雷电袭击，甚至是微风吹动导致的轻微移动。如何有效的避免这些威胁就成了棘手的问题。这些是通过影响信息传输介质的方式直接威胁信息安全。若是直接对信息本身进行攻击，其可避免的可能性就更加小了。所以信息安全就显得尤为重要了，这也是密码学出现的必不可少的条件之一。

1.2 研究目的及意义

尽管 DES 算法带有过去时代的特征，但它很好地抗住了多年的密码分析，后来，人们发现 DES 在强大攻击下太脆弱，使得其安全性遭到否定，应用机会也越来越少。但是，不代表它就永远地消失了，恰恰相反，它经过改进变成了另外一种算法继续守护信息的安全。

今时今日，DES 在大众的视线里逐渐消失。但是它曾经的辉煌是无法掩盖的，它还在其他的地方发挥着余热，如澳大利亚金融标准，ISO 下属国际销售金融标准组的国际认证标准，密钥管理等。DES 加密算法还是值得我们借鉴学习的，它对算法研究以及对加密算法的改良可以提供思路。

1.3 论文结构介绍

本文主要讲述 DES 加密算法的理论知识以及软件实现方式，但了解一种算法不能仅仅局限于此，要多方面的了解它，其中包括：密码学的简单介绍，加密技术介绍，DES 算法的理论基础，算法的目的、优点等。对于软件方面，我介绍了这次设计要用的硬件描述语言和要用到的软件，以及设计系统的结构组成、代码实现、仿真结果等。

第二章 密码学介绍

2.1 密码学概述

密码学研究的最核心的问题就是信息和信息系统的保密问题。换句话说就是，保证信息内容不外泄，信息所处环境安全。两者缺一不可。

“密码学是关于如何在敌人存在的环境中通讯”，是知名的密码学家 Ron Rivest 对密码学最为生动的描述。由这句话也不难理解出，密码学是研究如何在通信过程中隐秘地传递信息的学科。其首要目的是隐藏传输信息的含义，而不是隐藏其存在，不被人发觉。

密码学的安全目标至少包括三个方面：机密性、完整性、指定性。

（1）机密性：除了授权的人员，其他人无法获取信息，防止信息随意外泄。

（2）完整性：信息的内容不可以被随意改写、删去、添加。防止信息的内容发生变化。

（3）指定性：按照需求对信息进行读取和访问。若信息出现泄露可对应找出泄露者。

随着时代的发展，出现了现代密码学。现代密码学相对密码学来说研究内容更加精细，它保护的不再是信息本身的内容，而是信息所在的环境。其核心是密码编码学和密码分析学。前建立难以破译的安全密码体制和力图破解已有的密码体制，这两个方面就是现代密码学的要义。

由现代密码学的使用环境和传输过程，不难看出这个学科实践起来十分复杂，要想真正的学会密码学就要充分做好知识基础铺垫，如涉及编码的信息论、有关成功率的概率论和涉及移位和异或运算的数字逻辑等。

2.2 密码学发展史

对于信息的保护，密码学是最有效的手段。按照科技的发展程度可以划分成三个阶段。在军事和外交领域的应用是最早的，也是最普遍的，网络的普及和科技的发展使得密码学和我们的日常生活的关系更进一步。

在手工阶段，科技不发达，人们只能通过身边最简单的东西来对想要传递的信息进行加密。密码学的历史悠久，可以追溯到古巴比伦时代。在那个时期，最有代表性的物品就是费斯托斯圆盘，它是一个粘土圆盘，直径约为 6.5 英寸，圆盘的两面刻有象形文字和一些字母字符。