**“密码学”学习心得**

密码可破!人类的智慧不可能造成这样的密码，使得人类本身的才智即使运用得当也无法破开它!

**———爱伦·坡所**

在我们的生活中有许多的秘密和隐私，我们不想让其他人知道，更不想让他们去广泛传播或者使用。对于我们来说，这些私密是至关重要的，它记载了我们个人的重要信息，其他人不需要知道，也没有必要知道。为了防止秘密泄露，我们当然就会设置密码，保护我们的信息安全。更有甚者去设置密保，以防密码丢失后能够及时找回。密码”一词对人们来说并不陌生，人们可以举出许多有关使用密码的例子。现代的密码已经比古代有了长远的发展，并逐渐形成一门科学，吸引着越来越多的人们为之奋斗。

1. **密码学的定义**

密码学是研究信息加密、解密和破密的科学，含密码编码学和密码分析学。

密码技术是信息安全的核心技术。随着现代计算机技术的飞速发展，密码技术正在不断向更多其他领域渗透。它是集数学、计算机科学、电子与通信等诸多学科于一身的交叉学科。使用密码技术不仅可以保证信息的机密性，而且可以保证信息的完整性和确证性，防止信息被篡改、伪造和假冒。目前密码的核心课题主要是在结合具体的网络环境、提高运算效率的基础上，针对各种主动攻击行为，研究各种可证安全体制。

密码学的加密技术使得即使敏感信息被窃取，窃取者也无法获取信息的内容；认证性可以实体身份的验证。以上思想是密码技术在信息安全方面所起作用的具体表现。密码学是保障信息安全的核心；密码技术是保护信息安全的主要手段。

本文主要讲述了密码的基本原理，设计思路，分析方法以及密码学的最新研究进展等内容

密码学主要包括两个分支，即密码编码学和密码分析学。密码编码学对信息进行编码以实现信息隐藏，其主要目的是寻求保护信息保密性和认证性的方法;密码分析学是研究分析破译密码的学科，其主要目的是研究加密消息的破译和消息的伪造。密码技术的基本思想是对消息做秘密变换，变换的算法即称为密码算法。密码编码学主要研究对信息进行变换，以保护信息在传递过程中不被敌方窃取、解读和利用的方法，而密码分析学则于密码编码学相反，它主要研究如何分析和破译密码。这两者之间既相互对立又相互促进。密码的基本思想是对机密信息进行伪装。

**二、密码学的发展历程**

密码学的发展历程大致经历了三个阶段：古代加密方法、古典密码和近代密码。

1.古代加密方法（手工阶段）

源于应用的无穷需求总是推动技术发明和进步的直接动力。存于石刻或史书中的记载表明，许多古代文明，包括埃及人、希伯来人、亚述人都在实践中逐步发明了密码系统。从某种意义上说，战争是科学技术进步的催化剂。人类自从有了战争，就面临着通信安全的需求，密码技术源远流长。

古代加密方法大约起源于公元前440年出现在古希腊战争中的隐写术。当时为了安全传送军事情报，奴隶主剃光奴隶的头发，将情报写在奴隶的光头上，待头发长长后将奴隶送到另一个部落，再次剃光头发，原有的信息复现出来，从而实现这两个部落之间的秘密通信。

我国古代也早有以藏头诗、藏尾诗、漏格诗及绘画等形式，将要表达的真正意思或“密语”隐藏在诗文或画卷中特定位置的记载，一般人只注意诗或画的表面意境，而不会去注意或很难发现隐藏其中的“话外之音”。

比如：我画蓝江水悠悠，爱晚亭枫叶愁。秋月溶溶照佛寺，香烟袅袅绕轻楼

2.古典密码（机械阶段）

古典密码的加密方法一般是文字置换，使用手工或机械变换的方式实现。古典密码系统已经初步体现出近代密码系统的雏形，它比古代加密方法复杂，其变化较小。古典密码的代表密码体制主要有：单表代替密码、多表代替密码及转轮密码。

3.近代密码（计算机阶段）

密码形成一门新的学科是在20世纪70年代，这是受计算机科学蓬勃发展刺激和推动的结果。快速电子计算机和现代数学方法一方面为加密技术提供了新的概念和工具，另一方面也给破译者提供了有力武器。计算机和电子学时代的到来给密码设计者带来了前所未有的自由，他们可以轻易地摆脱原先用铅笔和纸进行手工设计时易犯的错误，也不用再面对用电子机械方式实现的密码机的高额费用。总之，利用电子计算机可以设计出更为复杂的密码系统

20世纪中叶以前, 由于条件所限, 密码技术的保密性基于加密算法的秘密, 因此称之为古典密码体制或受限的密码算法。尽管古典密码体制受到当时历史条件的限制, 没有涉及非常高深或者复杂的理论, 但在其漫长的发展演化过程中, 已经充分表现出了现代密码学的两大基本思想一“ 代替” 和“换位” , 而且还将数学的方法引人到密码分析和研究中。这为后来密码学成为系统的学科以及相关学科的发展莫定了坚实的基础。

密码学真正成为科学是在19世纪末和20世纪初期，由于军事、数学、通讯等相关技术的发展，特别是两次世界大战中对军事信息保密传递和破获敌方信息的需求，密码学得到了空前的发展，并广泛的用于军事情报部门的决策.

**小结**

从以上密码学的发展历史可以看出，整个密码学的发展过程是从简单到复杂，从不完美到完美，从具有单一功能到具有多种功能的过程。这是符合历史发展规律和人类对客观事物的认识规律的。而且也可以看出密码学的发展受到其它学科如数学、计算机科学的极大促动。这说明，在科学的发展进程中，各个学科互相推动，互相联系，乃至互相渗透，其结果是不断涌现出新的交叉学科，从而达到人类对事物更深的认识。从密码学的发展中还可以看出，任何一门学科如果具有广泛的应用基础，那么这个学科就能从中汲取发展动力，就会有进一步发展的基础。

我们这个社会已进入了信息时代，随着数据库技术和计算机网络应用的不断深入，信息的安全传输也有着广阔的应用前景。虽然密码可以追溯到古代，但密码作为一门学科还非常年轻，还有着更进一步的发展要求。

**三、密码学的基础知识**

密码学(Cryptogra phy)，现代准确的术语为“密码编制学”，简称“编密学”，与之相对的专门研究如何破解密码的学问称之为“密码分析学”。密码学是主要研究通信安全和保密的学科，密码编码学主要研究对信息进行变换，以保护信息在传递过程中不被敌方窃取、解读和利用的方法，而密码分析学则于密码编码学相反，它主要研究如何分析和破译密码。这两者之间既相互对立又相互促进。密码的基本思想是对机密信息进行伪装。一个密码系统完成如下伪装：加密者对需要进行伪装机密信息（明文）进行伪装进行变换（加密变换），得到另外一种看起来似乎与原有信息不相关的表示（密文），如果合法者（接收者）获得了伪装后的信息，那么他可以通过事先约定的密钥，从得到的信息中分析得到原有的机密信息（解密变换），而如果不合法的用户（密码分析者）试图从这种伪装后信息中分析得到原有的机密信息，那么，要么这种分析过程根本是不可能的，要么代价过于巨大，以至于无法进行。

在计算机出现以前，密码学的算法主要是通过字符之间代替或易位实现的，我们称这些密码体制为古典密码。其中包括：易位密码、代替密码（单表代替密码、多表代替密码等）。这些密码算法大都十分简单，现在已经很少在实际应用中使用了。由于密码学是涉及数学、通讯、计算机等相关学科的知识，就我们现有的知识水平而言，只能初步研究古典密码学的基本原理和方法。但是对古典密码学的研究，对于理解、构造和分析现代实用的密码都是很有帮助。以下介绍我们所研究的古典密码学。

**小结**

像绝大多数领域的科学知识一样，密码学在完整的科学体系建立起来之前，古典密码学仅限于一些简单代替和置换算法，当然，这代替和置换如果经过了几次算法的加密就会一样复杂多变，而现代的算法经过科学体系的整理与发展，更加的完善一些复杂算法的应用和各种应用协议的产生。而由于网络的出现以及发展，未来的密码学也必定向这个方向发展。例如网络签名，网上银行的安全，个人邮件信息的保护，都很迫切需要密码学的支持，推动密码学的发展.

**四、密码学的作用**

现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”。 人类有记载的通信密码始于公元前400年。古希腊人是置换密码的发明者。1881年世界上的第一个电话保密专利出现。电报、无线电的发明使密码学成为通信领域中不可回避的研究课题。

1.用来加密保护信息

利用密码变换将明文变换成只有合法者才能恢复的密文，这是密码的最基本功能。信息的加密保护包括传输信息和存储信息两方面，后者解决起来难度更大。

2.采用数字证书来进行身份鉴别

数字证书就是网络通讯中标志通讯各方身份信息的一系列数据，是网络正常运行所必须的。现在一般采用交互式询问回答，在询问和回答过程中采用密码加密，特别是采用密码技术的带CPU的职能卡，安全性好，在电子商务系统中，所有参与活动的实体都需要用数字证书来表明自己的身份，数字证书从某种角度上说就是“电子身份证”。

3.数字指纹

在数字签名中有重要作用的“报文摘要”算法，即生成报文“数字指纹”的方法，近年来备受关注，构成了现代密码学的一个重要侧面。

4.采用密码技术对发送信息进行验证

为防止传输和存储的消息被有意或无意的篡改，采用密码技术对消息进行运算生成消息的验证码，附在消息之后发出或信息一起存储，对信息进行验证，它在票房防伪中有重要作用。

5.利用数字签名来完成最终协议

在信息时代，电子数据的收发使我们过去所依赖的个人特征都将被数字代替，数字签名的作用有两点，一是因为自己的签名难以否认，从而确定了文件已签署这一事实；二是因为签名不易仿冒，从而确定了文件时真的这一事实。

**五、密码学的前景**

**量子密码学**

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。量子密码的安全性由量子力学原理所保证。所谓绝对安全性是指：即使在窃听者可能拥有极高的智商、可能采用最高明的窃听措施、可能使用最先进的测量手段，密钥的传送仍然是安全的。通常，窃听者采用截获密钥的方法有两类：一种方法是通过对携带信息的量子态进行测量，从其测量的结果来提取密钥的信息。但是，量子力学的基本原理告诉我们，对量子态的测量会引起波函数塌缩，本质上改变量子态的性质，发送者和接受者通过信息校验就会发现他们的通讯被窃听，因为这种窃听方式必然会留下具有明显量子测量特征的痕迹，合法用户之间便因此终止正在进行的通讯。第二种方法则是避开直接的量子测量，采用具有复制功能的装置，先截获和复制传送信息的量子态。然后，窃听者再将原来的量子态传送给要接受密钥的合法用户，留下复制的量子态可供窃听者测量分析，以窃取信息。这样，窃听原则上不会留下任何痕迹。但是，由量子相干性决定的量子不可克隆定理告诉人们，任何物理上允许的量子复制装置都不可能克隆出与输入态完全一样的量子态来。这一重要的量子物理效应，确保了窃听者不会完整地复制出传送信息的量子态。因而，第二种窃听方法也无法成功。量子密码术原则上提供了不可破译、不可窃听和大容量的保密通讯体系。

现代密码学与计算机技术、电子通信技术紧密相关。在这一阶段，密码理论蓬勃发展，密码算法设计与分析互相促进，出现了大量的密码算法和各种攻击方法。而且如今“密码学”不仅用于国家军事安全上，而且更多的集中在实际生活中。如在生活中，为防止别人查阅你的文件，可将文件加密；为防止窃取你的钱财，可在银行账户上设置密码等。随着科学技术的发展和信息保密的需求，密码学的应用将融人到人们的日常生活中。基于密码学有着坚实的应用基础，可以相信，密码学一定能不断地发展，不断地完善，从而会给全人类提供更加安全的各种服务，让我们祝福这一天的到来吧！

随着科学技术的迅猛发展，人们对信息安全和保密的重要性认识不断提高，在信息安全中起着举足轻重作用的密码学也就成为信息安全中不可或缺的重要部分。在今天，密码学仍然是信息技术非常重要的组成部分，它还在多个方面发挥着重要作用。比如对于用户的认证，对于信息的认证，信息的安全以及存储的安全等，但这些对于密码学而言，它需要同其他组件配合，比如管理软件等。密码学是和技术相关。作为一项技术本身有演进的需要，同时还要适应跟它相配合的技术组件发展的需要，要适应用户的新需求以及其他的新应用。密码学同信息技术所包括的组件一样，一直在发展变化中，这就需要我们要不断地发展密码学，使密码学能够适应其他应用的需求，同其他技术的进步齐头并进。信息安全有着众多基础研究的领域，这些基础研究构成了密码学的基础，也构成了通信、安全软件等系统的基础。当我们在实施一个工程项目的时候，不能仅靠一个细分领域技术就能把这个项目完成。

**六、学习密码学的感悟**

**1.密码学家的人生价值**

密码学家，也许不为人知。但他们的工作却在我们的生活中发挥

着巨大的作用。他们在现代社会中有着不可替代的作用。有人认为密码学家就像一个黑客，但他们有着本质的不同。黑客是盗取密码保护的信息以获取利益，而密码学家从事的是基础理论研究，是为了评估密码算法的安全性，找到其漏洞，以设计出更安全的密码算法。

我觉得，对于密码学家来说，其实有两重意义上的生命：一是生物意义上的生命，二是学术意义上的生命。两种生命往往并不同步。有的人，生物意义上的生命还活着，学术意义上的生命已经死了。这种情况在我们周围越来越常见。目前充斥着大量名为成果，实为名利敲门砖的所谓学术，没有任何新意和创见，前脚迈出印刷厂，后脚就进造纸厂，白耗费了财力，还增加了环境污染。有的人，生物意义上的生命死了，学术意义上的生命还活着。我想，密码学家就是这样的一类人，他们的研究成果，大到保卫国家，小到维护个人的利益，我想这是他们人生价值的最好体现。

**2.总结与体会**

密码学充满了神秘性，让我对她产生了浓厚的兴趣和好奇。最近的这次人类战争中，即二战，认识到密码和情报是一件事情。而在当代密码学跟数学，计算机只是一个大背景，因为信息将会以网络为媒介，所以现代密码学更多的是以数字化的信息而非纸质为研究对象。所以密码学归根结底是数学问题，计算能力是数学的一个方面，高性能的计算机可以成为国力的象征，分析情报就是一方面。数学研究等一些自然基础学科的研究才是国家实力的坚定的基石，才是一个自然科学的学生的理想所在。数学研究很广泛，而密码学涉及很有限，大多与计算机学科相关，如离散数学。从数学的分类包括：数论、近世代数、矩阵论、域论，以及其它结合较为紧密地理论：信息论、编码论、量子学、混沌论。

密码学还有许许多多这样的问题。当前,密码学发展面临着挑战和机遇。计算机网络通信技术的发展和信息时代的到来，给密码学提供了前所未有的发展机遇。在密码理论、密码技术、密码保障、密码管理等方面进行创造性思维，去开辟密码学发展的新纪元才是我们的追求。

北京科技大学

班级: 计1102

姓名:杨勇

学号: 41155047