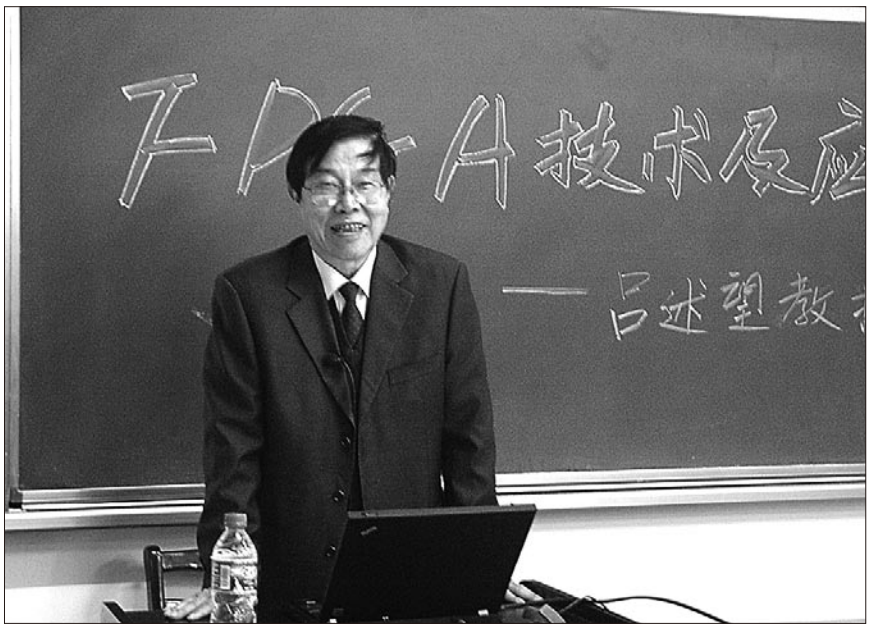

吕述望 密码一样的人生

□孙梦姝

吕述望，1965年毕业于中国科学技术大学无线电电子学系自动控制专业。

1995年4月受聘担任中国科技大学研究生院信息安全国家重点实验室研究员；1997年6月受聘担任中国科技大学研究生院博士生导师。曾获得1986年度和1988年度中国科学院科技进步一等奖、1988年度国家科技进步二等奖、1992年度国家科技进步一等奖、1995年度省部级科技进步一等奖、1996年度国家科技进步二等奖、1997年度省部级科技进步二等奖、2000年度国防科学技术三等奖、金融科技进步二等奖、2001年度国防科学技术三等奖，均为各奖项的主要完成人。1992年起享受国务院颁发的政府特殊津贴。

吕述望大学毕业后留校任教，曾任无线电基础教研室主任，从事电子学的基础课教学和科研工作；1978年调到中国科学技术大学研究生院（北京）任教，参与创建数据与通信保护研究教育中心，DCS中心担任实验室主任，1986年6月提升为副研究员；1980年以来主要从事密码学、信息安全方面研究。

当仅听到吕述望老师的声音时，就会让人产生一种错觉，觉得他是一位意气风发的年轻人；当我终于如愿访问到吕老师时，深深地感觉到他是一位智者，博览群书、博闻强识；你看到他和他的学生在一起讨论各种人生的话题时，就会觉得吕老师酷似老顽童一般，喜欢和学生们开玩笑，又像一位引领者指导着他的学生们，他教导学生要谦虚、谨慎地聆听他人的感想。通过访问吕老师，笔者了解到密码看似神秘，不过如果你掌握了钥匙key，密码就会变得有理可循、有据可依。学问如此，人生更是如此。

把中国的事情干好

刚见到吕述望老师的时候，他和他的学生们正在开会，雷厉风行、洪亮的嗓音让笔者觉得他更像一位将军，正在指挥他的将士制定战略部署。吕老师先给我看了一篇题为《母亲总是平凡而伟大的》的文章，其中讲述了吕老师的学生生涯和他母亲对他的深远影响。

幼年失去父亲的吕述望老师，在母亲的艰辛抚养下长大成人，而且学生时代读书成绩十分优异。他说：“我在北京读大学时，母亲就在北京干活挣钱。我不知道自己当时哪来的劲头，大学五年，晚上11点以前我根本没有睡过觉。在中国科技大学时，我是个遵守纪律的好学生。”吕老师回忆道，本来在年轻的时候是要被送到美国学习的，不过吕老师的母亲对他说了这样一段话：“中国有许多事情好干，有许多事情好学，跑到美国去干什么，中国人还是把中国的事情干好！”一席简短又质朴的话语，让吕老师突然间意识到自己今后所有的努力，必须根植中国这片黄土地上。吕老师说：“其实仔细想一想，一旦去了美国，是不是三五年就一定能回来，那就天晓得了，我是学过概率的，随机因素太多。虽然我提倡随机美，但还是让这种美在我们民族这块黄土地上展现吧！”正是有了这样的母亲，吕老师带着对祖国的热爱和对研究学问的热忱开始了密码学的研究。

望中国高校在国际上立足

母校对于任何一个人来说都是无法比拟的，中国科技大学是吕老师的母校，也是中国各大院校中出院士最多的学校之一，言谈中能感受到吕老师对母校的热爱之情。谈到母校时，他妙语连珠、神情激昂。“当时我那个年代，一个穷孩子能上大学已经很好了。那时中国科技大学是一所较好的学校，中国共产党说我们要办自己的学校，为两弹一星服务，所以学校里的专业基本上都是理工类学科，直到目前为止，许多人还将物理化学和化学物理混为一谈，可见现在教育普及的失败。当时的中国科技大学是一所新型的大学，我那一代人能到这所大学学习是得益于新中国的建设，科大最早由郭沫若来担任校长，后来又几经传承，他们能不能将这所大学办成一个一流的大学，我并不知道，这是中国教育人应该考虑的问题。以后在适当的时候我会带领我的团队回到中国科技大学看一看，是不是我们所希望的那样。”那么什么样的大学才是吕老师眼中的先进大学呢？他说：“我认为办先进的大学是很重要的。第一要有先进的团队，第二要有一流的目标，中国的大学毕业文凭在国外是不承认的，这就是我们的大学并没有在国外立足的最根本表现。当我们能和牛津、剑桥互换文凭的时候，这就叫在国际上立足了。”

当笔者问到我国高校如何才能做到屹立世界知名大学之林时，吕老师讲到：“怎么做，实际上这是人类的事情。说怎么去做是没有用的，实际上任何事物的生长，以我的观点看，这是一个多维空间，哪一个因素都会对这件事情有所影响。但是主要有四度：包括政治的、经济的、道德的、自然的等，这四者缺一不可，这就是我讲的人生本源的主要含义。例如，我国的封建社会，那时把道德空间拉得很高很高，把那个空间压扁了，限制了女性的自由，所以那时不是一个良性的发展空间，这个社会就是有问题的社会。解放战争时期，那时将政治这一维度拉得很高。所以任何事物的成长不是一个人可以左右的，都是大的环境所塑造的。至于我的母校中国科技大学会如何发展，如果问我，我会说很多意见，关键是谁来主持这个科技大学，大学当时所处的环境是什么样子的？”吕老师继续分析说，“外国人视他们大学发的这张文凭重于生命，如果什么时候我国也能如此，那么我们的大学就能在国际上立足了。”笔者深感，吕老师在教书育人、研究学问的同时，仍怀有忧国忧民的精神，时时不忘反思我国的教育现状。

精雕拙石用心良苦

何为知识？吕述望老师认为知识具备三个特性：被证实的、真的、被相信的。而在虚拟数字世界中，就出现了知识的表达难，安全传递不易；知识的保存难，安全传递不易；知识的认证难，安全审计不易；知识的挖掘难，产权保护不易。从而造成知识安全难，知识的泯灭容易。

眼前的这位长者，虽处花甲之年，但精神矍铄，除了额头上那些许的皱纹，甚至都捕捉不到一丝的白发。可正是这位前辈，在信息安全领域作出了卓越的贡献，他是中国第一个也是唯一一个公开商用算法SMS4的创始人。问到吕述望老师为何会将SMS4的密码算法公开，吕老师义正言辞地说：“这个算法是国家的算法，世界上都在做算法标准，我们国家也在做，我们也做了一系列的标准性的东西，并且获得了国家的认可，编好了序列号。在我编写的《完全映射及其密码学应用》这本书中就主要介绍了两类完全映射：正形置换和全向置换。我给出了主要面向密码算法设计的几种正形置换发生器的研究结果，为完全映射在密码学中的具体应用作好了准备。为阐述完全映射理论在密码算法设计中的应用，我还进一步给出了SP网络密码算法、Feistel网络密码算法的线性与差分安全性分析技术，并介绍了上述两种算法与正形置换之间的关系。在上述工作的基础上，又介绍了P逻辑密码算法，并给出了其线性与差分安全性分析技术，从而使正形置换理论得到了比较系统的应用。”

吕述望是数字物理噪音源芯片（WNG4）的发明者，他的名望遍及信息安全界，并且桃李满天下。吕老师的“安全信息系统概论”课程曾获得2004～2005年度中科院研究生院优秀课程。吕老师将密码学总结成“一二三四五六七”，这“一二三四五六七”即一种美，两类函数，三个假设，四项操作，五大属性，六难问题，七例应用。没有理论课的枯燥难懂，学生学习这门课，可以真正做到站在前辈的肩膀上看问题，汲取前辈的经验，消化前辈的思想精华。

吕老师感兴趣的事情很多，对各个学科都充满了无限的好奇心，正因为这样，他发现自然熵的有趣用途——用来分析性别。他曾用汉字的组合性来做成小诗，并编成密码，采访的时候，他的学生还在现场用《新华书目报》的文字编了一段密码。听说以前吕老师还用《三十六计》来编写密码。他希望学生博学强知，推荐学生看《时间简史》，看量子力学相关的书籍。吕老师语重心长地说：“我在乎我的学生们，希望在我这里学习真的能有所收获，对得起给他们的那张文凭。”

对学生付出如此之多的吕老师，自然也得到了学生的爱戴。虽然采访吕老师的那天是周末，但是他的学生们都聚集到吕老师的实验室，喜欢和老师天南海北地交谈，不仅仅只是谈论密码，更多的是一些人生中的思考。吕老师对笔者说：“我这个人不轻易说认识一个人，我们今天见面了，只能说我知道你，但不能说我认识你，要了解得更多就需要多多接触，只有这样才知道你是什么样的人。”也许正是吕老师有这样耿直、一丝不苟的态度，才使得他成为一位值得信赖的老师，一位值得尊敬的学者，一位值得钦佩的长者。

21264

吕述望的学术专著

《信息安全保密教程》（上下册）/信息安全系列丛书/赵战生、杜虹、吕述望主编/中国科学技术大学出版社/定价：136.00元

建设信息安全保障体系是信息安全保障工作的重要任务，信息安全保密是信息安全保障中的核心问题之一。为跟上信息化的飞速发展，使信息安全保密工作者更好地完成历史重任，本教程以20章的篇幅，对信息化与信息安全保密的形势、概念、技术、管理和人才的知识结构和技能等方面作了全面深入的介绍；本教程不但叙述了国际上信息安全保障的新情况、新技术、新法规、新标准，也系统全面地介绍了我国信息安全保密工作的政策、法规、标准和工作要求，从而为从事信息安全保密的领导、管理人员和技术人员提供了权威性教材。

吕述望印象

方晨（学生）

当初上吕述望老师的课，纯属偶然。还是课程试听期间，一次早起上课，听同路的同学百般推荐吕老师的课程，耐不住同学的热情，改变原计划，旁听吕老师的课。没想到这一听，居然下课就决定要修改已经和导师商量好的选课单，决定要上吕老师的课。

吕老师不仅亲自给我们授课，还经常请信息安全界的各领域专家来授课。吕老师说，他们都是各自领域的专家，他们的领域自己不是很熟悉，请他们讲自己的专业，比我讲得好，讲得透彻。从五笔字型发明人王永民开始，英特尔技术专家赵军、曲成义研究员、张明德工程师、美国的丁津泰教授、屈延文、南相浩、许榕生、卿斯汉等等，每一个名字都让人肃然起敬，每一个人现在或曾经都叱咤风云，每一次讲座都明知至理。我认为，也许在科学院，再也找不到一门正式课程能请这么多名人来作讲座，这都要归功于吕老师。许多来作讲座的老先生都说：“吕老师叫我来的，我不敢不来。”

陈新（记者）

中国科学院研究生院博士生导师、密码专家吕述望教授曾经应邀来到我的母校（北京物资学院）作了题为《信息安全前沿问题研究》的精彩讲座。吕述望教授用通俗的语言和生动活泼的实例讲述了信息安全现状、人们的安全意识和我国传统知识信息的传承问题，随后就密码学的相关理论和前沿问题进行了详细讲解。他将深奥的密码学知识生活化，教给广大师生如何应用密码学知识来增强自己的安全意识。吕老师富有理论深度，广征博引，实例生动，数据详实，语言通俗，与会师生均表示受益匪浅。

向永杨（记者）

正值立秋之后，我在北京林业大学的研究室里如约见到了仰慕已久的吕述望老师。当时窗外跳跃着细细碎碎的阳光，空气清爽。吕老师坐在对面，谦和的微笑，厚重而具亲和力的表情，让我感觉就像面对朋友般轻松自然。这位老前辈，在信息安全领域作出了卓越的贡献。他的名望遍及信息安全圈内，桃李满天下。通过采访，我认为吕老师教授的“安全信息系统概论”课，是真正意义上的概论课。他用“一二三四五六七”全面介绍了信息安全的问题(需求)、理论、实现(技术)、应用、发展。