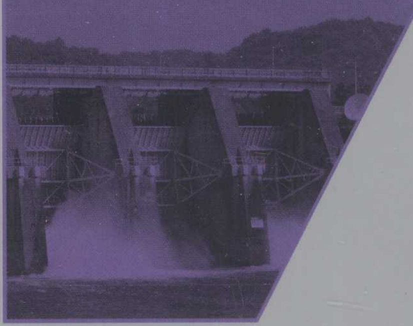
高等学校专门用途英语（ESP）系列教材

学术英语

ACADEMIC ENGLISH for SCIENCE AND ENGINEERING

主　编／蔡基刚

理工／



外语教学与研究出版社
FOREIGN LANGUAGE TEACHING AND RESEARCH PRESS

高等学校专门用途英语（ESP）系列教材

学术英语

ACADEMIC ENGLISH for SCIENCE AND ENGINEERING

主　编／蔡基刚

理工／

外语教学与研究出版社
FOREIGN LANGUAGE TEACHING AND RESEARCH PRESS
北京 BEIJING

ESP

图书在版编目(CIP)数据

学术英语：理工 = Academic English for Science and Engineering / 蔡基刚主编. — 北京：外语教学与研究出版社，2012.7
高等学校专门用途英语（ESP）系列教材
ISBN 978-7-5600-8527-2

Ⅰ. ①学… Ⅱ. ①蔡… Ⅲ. ①理科（教育）—英语—高等学校—教材 ②工科（教育）—英语—高等学校—教材 Ⅳ. ①H31

中国版本图书馆 CIP 数据核字（2012）第 148325 号

出 版 人：蔡剑峰
项目负责：姜琳琳
责任编辑：聂海鸿 姜琳琳
装帧设计：郭 子
出版发行：外语教学与研究出版社
社　　址：北京市西三环北路 19 号（100089）
网　　址：http://www.fltrp.com
印　　刷：北京京科印刷有限公司
开　　本：889×1194 1/16
印　　张：20
版　　次：2012 年 8 月第 1 版 2012 年 8 月第 1 次印刷
书　　号：ISBN 978-7-5600-8527-2
定　　价：42.90 元（含 DVD-ROM 光盘一张）

* * *

购书咨询：(010)88819929 电子邮箱：club@fltrp.com
如有印刷、装订质量问题，请与出版社联系
联系电话：(010)61207896 电子邮箱：zhijian@fltrp.com
制售盗版必究 举报查实奖励
版权保护办公室举报电话：(010)88817519
物料号：185270001

前言

高等学校专门用途英语（ESP）系列教材是针对新时期大学英语教学的发展方向和新形势下我国人才培养目标对高等教育的要求而开发，以教育部《普通高等学校本科专业目录》的学科设置为基础，结合专家、学者、教师对ESP教学的理论和实践研究成果，根据院校实际教学情况综合考虑而编写的一套教材。该系列教材旨在将大学英语教学与学生所学专业相结合，提高大学生的学术英语能力及专业英语水平，为学生毕业后直接使用英语从事本专业工作，或者继续深造学习、进行学术研究以及参加学术活动打下坚实基础。

本系列教材分为“学术提升”和“专业拓展”两大类，以专业学科为基础，以提高英语学术能力和专业英语应用能力为核心，为高等院校师生提供教学和学习资源，同时为教师课堂教学提供有力支持。

学术提升类

高等学校专门用途英语（ESP）系列学术提升类教材以“用中学（learning by doing）”的教育学理念为指导思想，以大学科概念为划分基础，如人文、社科、理工、管理、医学、农林等，旨在帮助学生夯实语言技能、提升学术能力（academic skills），包括学术阅读、学术听力、学术写作和学术口语的能力，以及批判性思维能力和创新思维能力等。

专业拓展类

高等学校专门用途英语（ESP）系列专业拓展类教材以“专业需要（discipline-specific）”的教育学理念为指导思想，在商务、医学、法律、理工等不同方向之下细分为不同专业，旨在帮助学生在具备基本的英语听、说、读、写技能的前提下，获取本专业相关的前沿信息，掌握专业词汇，熟练专业语言的运用，强调培养学生在英语环境下从事本专业工作的能力。

此外，高等学校专门用途英语（ESP）系列还将陆续推出根据实际教学需求而不断开发的新的分册，不断丰富该系列教材，全力支持大学英语课程体系建设。

编写说明

编写目的

《国家中长期教育改革和发展规划纲要（2010-2020）》提出高校要“培养大批具有国际视野、通晓国际规则、能够参与国际事务和国际竞争的国际化人才”，并提出“吸引更多世界一流的专家学者来华从事教学”、“有计划地引进海外高端人才和学术团队，引进境外优秀教材，提高高等学校聘任外籍教师的比例”，实施“卓越工程师”培养计划等措施。

在高等教育国际化背景下，我国大学生学习英语的目的发生了根本的变化。大学生越来越多地需要通过大学英语的学习来为他们的专业学习服务，如能参加以英语作为教学语言的专业课程和专业讲座，用英语查阅本专业的文献资料，撰写文献综述和小论文，并用英语在学术研讨会上进行宣读和讨论，这就是学术英语的内容。本教材正是为了适应这一新需求而编写的学术英语教材。

本教材适合完成大学基础英语课程，达到一般要求的学生，旨在培养学生在专业学习和研究上运用英语的能力，具体包括：

- 听专业课程和专业讲座的能力；
- 搜索、阅读和评价专业文献的能力；
- 撰写文献摘要、述评和专业小论文的能力；
- 口头陈述和演示科研成果的能力；
- 参加学术讨论的能力。

教材特色

1 采用国外学术英语教学中普遍运用的基于项目研究（research/project-based）的编写理念，即围绕学生在课程中选定的项目，开展学术英语综合能力训练和学术规范知识教学。

2 突出共性，淡化专业，重点培养学生跨学科的学术共核词汇能力和听说读写综合能力。阅读材料选自准学科类的真实语篇，主要为适合跨学科读者的科普刊物文章，主题涉及云计算、气候变化、转基因食品、核能辐射、纳米技术等。

3 培养学生的学术批判能力和解决实际问题的学术研究能力。教材中，同一单元通常选取几篇观点相异或相对立的阅读材料，同时还包括多个与主题相关的学术讲座视频。这些观点各异、来源不同的材料给学生提供了信息辨别和学术批评的机会。

使用建议

1 根据各学校的课程设置情况和教学需求，编者提供以下两种使用模式：1）供一个学期72课时的教学使用，即每周4课时。课堂上分析阅读材料、训练听讲座技能，同时安排两次全班性的口语陈述演示（一次基于文献综述，一次基于学期论文）。2）供一个学期36课时的教学使用，即每周2课时。使用这种模式的课堂教学，可多关注学生学术英语技能，尤其是学术论文写作技能。教材中的阅读材料、讲座听力和陈述演示练习等可供学生课后自主学习。

2 教学活动可按单元顺序开展，但第三单元的听讲座技巧和第六单元论文陈述演示可根据需要穿插在各个单元中进行。

3 作为以项目为依托的教材，建议教师从课程开始就让学生根据自己的专业兴趣，建立5-6人的小组，让学生通过团队合作方式，确定各自的研究课题和小论文题目。然后围绕这个项目进行资料搜索、听相关主题的学术讲座、开展文献综述、论文写作和成果演示汇报等学术技能的教学。

4 本教材通过学术技能的训练，提高学生的综合语言能力，因此教材中的课文既为各个单元学术英语技能主题服务，同时也为巩固语言基础服务。但为避免干扰主题，课文的语言练习集中放在每个单元最后的Enhancing your academic English部分。教师可根据实际情况，选择性使用语言练习，并让学生课后自主完成。

5 听力材料有两个目的：一是为当前单元的课文主题和学术技能服务；二是为提高学生学术讲座听力能力服务。前者的练习穿插在单元中，后者的练习集中放在每个单元后的Enhancing your academic English部分。本教材提供了20个讲座材料。72课时模式下，建议教师结合单元的课文主题，每周至少安排学生课堂听一个讲座。36课时模式下，也建议教师适当选取，并可充分利用课前、课间时间，大部分可放在课后作为练习。

6 为给学生创造真实的语境，本教材的课文和听力材料都选自真实的阅读资料和学术讲座。课文长度从1000词到1500词不等，听力材料5至20分钟不等。在实际使用中，教师也可以根据学生的水平提供适当的补充讲解。

7 为培养学生的学术口语陈述和演示能力，除第六单元有针对性的技巧讲解外，建议增加两次练习。第一次是基于学生的文献综述的陈述演示，第二次是基于最终写成的论文的陈述演示。72课时模式下，课堂时间可分别安排为：文献综述陈述每人2-3分钟，论文陈述每人7-8分钟（其中包括同学提问和回答）。36课时模式下，可由学生自己录像，将录像上交。

8 本教材内容丰富。练习设计按照国外大学授课和作业1:2的比例。教师可授课2课时布置4课时作业，让学生课后自主完成查阅文献和听讲座的任务。

参加本书部分单元编写的有廖雷昭、贺灿文、肖英、徐欣、程寅、王绍梅、李科、王登霞、蔡竹君等。

编者

2012年5月

CONTENTS

Unit 6 Making an Oral Presentation / P273

UNIT 1

Choosing a Topic

In this unit, you will learn how to:

- choose a particular topic for your research;
- formulate a research question;
- write a working title for your research essay;
- enhance your language skills related with reading and listening materials presented in this unit.

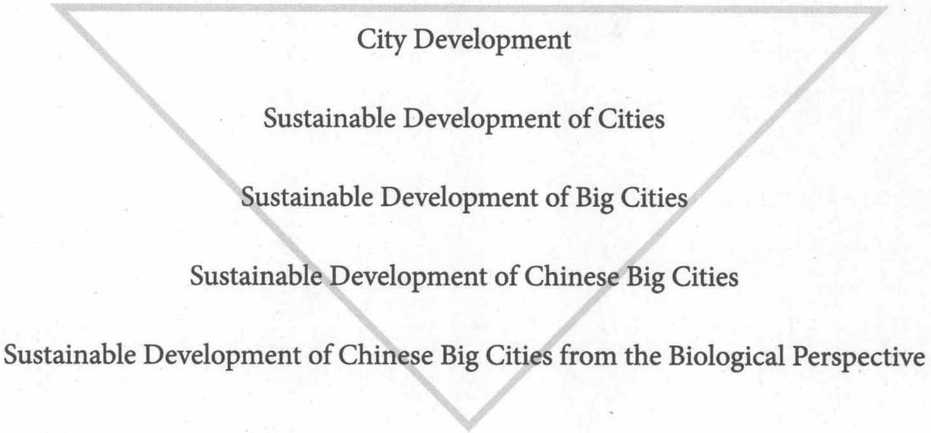
1 Deciding on a topic

As a college student of science and technology, you are often required to write a literature review about a certain topic, or a 1,500-word term paper. In either case, the writing is a complex process which involves choosing a topic, searching for relevant materials, and compiling a reference list. Hence the first thing you need to do is to choose a research topic.

A topic is what the essay or research paper is about. Choosing a topic for your literature review or research paper requires careful consideration. A topic that is too specialized or too general may bring many problems in terms of the time you can devote to the research or the sources of information available on the topic. How do you choose a topic which is possible to research? There are four principles:

1) **Interesting.** If a topic holds your interest, you will most likely enjoy working on it. However, you should also be aware of the interest of your readers. For example, if your readers are from different disciplines or academic backgrounds, your topic should not be too specific.
2) **Important.** You also have to consider the value of the topic you are likely to choose, both academic and social. An essay without practical or theoretical value will probably not attract readers.
3) **Manageable.** Narrow down your topic to make your paper manageable. For example, if you want to discuss the history of a disease, it may not be possible for you to cover all the important ideas in a 1,500-word essay.
4) **Adequate.** You have to ask the question: Can the topic I have chosen be researched? One criterion is that you must make sure that there are adequate source materials available on the topic. Avoid a topic that has very limited information about it, for it is difficult to carry out your research without previous studies.

TASK 1 **Analyze the steps as to how a topic is made more specific and manageable.**



City Development

Sustainable Development of Cities

Sustainable Development of Big Cities

Sustainable Development of Chinese Big Cities

Sustainable Development of Chinese Big Cities from the Biological Perspective

TASK 2 **Choose one of the following topics that you are familiar with or interested in. Then discuss with your partners about the following questions.**

1 Is the topic appropriate for a 1500-word essay? Why or why not?
2 If the topic is too general, how do you narrow it down to a more manageable topic?
3 Can you suggest some appropriate topics of each subject?

- **Global Warming**
  My narrower subtopics:
  1) ______________________________
  2) ______________________________
  3) ______________________________

- **Cancer**
  My narrower subtopics:
  1) ______________________________
  2) ______________________________
  3) ______________________________

- **Nanotechnology**
  My narrower subtopics:
  1) ______________________________
  2) ______________________________
  3) ______________________________

- **Internet**
  My narrower subtopics:
  1) ______________________________
  2) ______________________________
  3) ______________________________

- **Artificial Intelligence**
  My narrower subtopics:
  1) ______________________________
  2) ______________________________
  3) ______________________________

- **Energy**
  My narrower subtopics:
  1) ______________________________
  2) ______________________________
  3) ______________________________

- **Genetic Engineering**
  My narrower subtopics:
  1) ______________________________
  2) ______________________________
  3) ______________________________

- **Universe**
  My narrower subtopics:
  1) ______________________________
  2) ______________________________
  3) ______________________________

TASK 3 **Read the following two essays concerning computers and answer the following questions.**

1 What is the main idea that each essay tries to illustrate?
2 In which aspect do the two essays share the same idea?
3 In which aspect do the two essays differ?
4 What topic does each essay address? Do you think they are appropriate according to the four principles mentioned on Page 2?

Text 1

How Do Computer Hackers "Get Inside" a Computer?[1]

Julie J. C. H. Ryan

1 This seems like a straightforward question but it's actually quite complex in its implications, and the answer is anything but simple. The trivial response is that "hackers" get inside a target computer system by exploiting vulnerabilities, but in order to provide more detail, let's start from the beginning.

2 The term "hacker" is fairly controversial in its meaning and interpretation. Some people claim that hackers are good guys who simply push the boundaries of knowledge without doing any harm (at least not on purpose), whereas "crackers[2]" are the real bad guys. This debate is not productive; for the purposes of this discussion, the term "unauthorized user" (UU) will suffice. This term covers the entire range of folks, from those involved in organized criminal activities to insiders who are pushing the limits of what they are authorized to do on a system.

3 Next let's explore what it means to "get inside" a computer. This can refer to gaining access to the stored contents of a computer system, gaining access to the processing capabilities of a system, or capturing information being communicated between

systems. Each of these attacks requires a different set of skills and targets a different set of vulnerabilities.

4 So what do UUs take advantage of? Vulnerabilities exist in every system and there are two kinds: known and unknown. Known vulnerabilities often exist as the result of needed capabilities. For instance, if you require different people to use a system in order to accomplish some business process, you have a known vulnerability: users. Another example of a known vulnerability is the ability to communicate over the Internet; enabling this capability, you open an access path to unknown and untrusted entities. Unknown vulnerabilities, which the owner or operator of a system is not aware of, may be the result of poor engineering, or may arise from unintended consequences of some of the needed capabilities.

5 By definition, vulnerabilities may be exploited. These can range from poor password protection to leaving a computer turned on and physically accessible to visitors in the office. More than one technical exploit has been managed simply by sitting at the receptionist's desk and using his computer to access the desired information. Poor passwords (for example, a username of "Joe Smith" with an accompanying password of "joesmith") are also a rich source of access: password cracking programs can easily identify dictionary words, names, and even common phrases within a matter of minutes. Attempts to make those passwords more complex by replacing letters with numbers, such as replacing the letter O with the number zero, don't make the task much harder. And when a UU can utilize a valid username-password combination, getting access to a system is as easy as logging in.

6 If a target system is very strongly protected (by an architecture that includes both technical controls such as firewalls or security software, and managerial controls such as well-defined policies and procedures) and difficult to access remotely, a UU might employ low-technology attacks. These tactics may include bribing an authorized user, taking a temporary job with a cleaning company, or dumpster diving[3] (rifling through trash in search of information). If the target system is not so strongly protected, then a UU can use technical exploits to gain access.

7 To employ technical exploits a UU must first determine the specifications of the target system. It would do no good whatsoever for a UU to use a technical exploit against a Microsoft vulnerability if the target system is a Macintosh[4]. The UU must know what the target system is, how it is configured, and what kind of networking capabilities it has. Once these parameters (which can be determined remotely through a variety of methods) are known, then the UU can exploit the configuration's known vulnerabilities. The availability of preprogrammed attacks for common configurations can make this task quite simple; UUs that use these scripted capabilities are somewhat derisively known as "script kiddies[5]".

8 One way a technically proficient UU can remotely determine the configuration of a target system is through capabilities inherent in hypertext transfer protocol[6] (http).

Users who access certain websites actually send configuration information, such as the type of browser being used, to the requesting site. Once the system configuration is known, then exploits can be selected.

9 Another type of attack is one that is preprogrammed against specific vulnerabilities and is launched without any specific target—it is blasted out shotgun style with the goal of reaching as many potential targets as possible. This type of attack eliminates the need for the first step, but is less predictable in both outcome and effectiveness against any given target.

10 It's important to recognize that the end goal of unauthorized access varies depending on the UU's motivations. For example, if a UU is trying to gather a lot of zombie computers[7] for use in a distributed denial of service attack, then the goal is to sneak a client program onto as many computers as possible. One way to do this fairly effectively is through the use of a so-called Trojan horse program[8], which installs the malicious program without the knowledge or consent of the user. Some of more recent mass Internet attacks have had this profile as an element of the attack pattern.

11 Protecting yourself against attacks is a multi-step process, which aims to limit and manage the vulnerabilities of your system. (It's impossible to eliminate them all.) First, make sure you have all the latest patches for your operating system and applications—these patches generally fix exploitable vulnerabilities. Make sure your password is complex: It should include letters, numbers, and symbolic characters in a nonsensical manner. Also, consider getting a hardware firewall and limiting the flow of data to and from the Internet to only the few select ports you actually need, such as email and Web traffic. Make sure your anti-virus software is up-to-date and check frequently to see if there are new virus definitions available. (If you are using a Windows system, you should ideally update your virus definitions every day.) Finally, back up your data. That way if something bad does happen, you can at least recover the important stuff. (1,023 words)

Terms and notes

[1] This text is from *Scientific American*, August 16, 2004.

[2] cracker: someone who illegally breaks into a computer system in order to steal information or stop the system from working properly 黑客

[3] dumpster diving: the practice of sifting through commercial or residential trash to find items that have been discarded by their owners, but that may be useful to the dumpster diver 垃圾搜寻

[4] Macintosh: a series of personal computers designed, developed, and marketed by Apple Inc. 麦金塔电脑（苹果电脑其中一个系列的个人电脑）

[5] script kiddies: a derogative term used to describe those who use scripts or programs developed by others to attack computer systems and networks and deface websites. They are more immature, but unfortunately often just as dangerous exploiter of security lapses on the Internet. "脚本小子"

[6] hypertext transfer protocol: the set of rules for transferring files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web 超文本传输协议

[7] zombie computer: a computer that has been secretly compromised by hacking tools which allow a third party to control the computer and its resources remotely 僵尸电脑

[8] Trojan horse program: **a malicious computer program that poses as something desirable or is hidden within a different program to trick users into loading the malicious software onto their computers** 木马程序

Text
2

Electronic Threats of a Computer[1]

Will Knight

1 Any computer connected to the Internet faces a daunting range of electronic threats. Perhaps the biggest single threat to any computer is the humble software bug. Seemingly harmless programming errors can be exploited to force entry into a computer and also provide the weak spots that allow computer worms and viruses to multiply.

2 Many software bugs will simply cause a computer to crash. But an expert programmer can sometimes figure out how to make a computer malfunction in a creative way, so that it provides access to secure parts of a system, or shares protected data.

3 When a software vulnerability is revealed, it is often a race against the clock to apply the correct software patch before an attacker can convert the bug into an "exploit" that can be used to cause major damage.

Viruses and worms

4 A computer virus is a program that spreads between computers by hiding itself within a—seemingly innocent—document or application. A worm, on the other hand, is a program that replicates and travels without "infecting" anything else on a system.

5 Many modern specimens of malicious code, however, use a mixture of tricks to cheat their way onto computer systems, blurring the line between worms and viruses. The terms are now often used interchangeably.

6 The first worms appeared in the 1970s and spread slowly between computers connected to the same network. They simply displayed an annoying message on the screen of each infected machine. The first computer virus, called Elk Cloner[2], was written in 1982 and infected computers via floppy disks.

Trojans and zombies

7 But viruses and worms no longer just provide a way for hostile hackers to gain notoriety. Today's viral code can contaminate computers at lightning speed, spreading via email, peer-to-peer[3] file-sharing networks and even instant messaging programs. The most successful ones cause serious damage, forcing companies around the globe to close down while infected computers are cleaned up.

8 A string of recent specimens have been designed to snatch passwords or credit card information and install programs that can be used to remotely control infected machines. These programs are known as Trojan horses.

9 There is evidence that virus writers can earn large amounts of money by leasing access to networks of compromised computers[4]—often referred to as "botnets[5]". These groups of remote-controlled "zombies" have been used to squeeze out money from websites, by threatening to crash them with a denial-of-service (DoS) attack[6]. This involves overloading a server with fake page requests, so that real messages cannot get through.

Spam[7], Spam, Spam

10 Spammers have also begun using botnets to forward unwanted bulk email advertising, or spam, through scores of zombie PCs. This makes it far more difficult for spam hunters to block the messages at source and catch the offenders.

11 Once considered a fairly minor problem, spam is rapidly spiraling out of control, and much more than half of all email messages are now thought to consist of unwanted advertising messages.

12 To combat computer scientists' best efforts to stem the tide of junk email, the spammers have had to become more cunning and sophisticated. More recently, "spim" (spam by instant messenger) and "spit" (spam by Internet telephony) have joined the fight.

Phishing[8]

13 Spam's more sinister cousin is the phishing email. This is a con trick that arrives as an email and tries to trick a recipient into handing over money or sensitive personal information like their bank account details or a username and password.

14 The simplest phishing tricks try to deceive a target into sending money as part of a get-rich-quick scheme. But phishing tricksters are also getting more devious and recent scams pose as customer service emails and send users to fake banking or commercial websites where they are invited to "re-enter" their account information.

15 Some genuine sites have even proven vulnerable to software bugs that can be exploited to capture information from regular users. Phishing is especially threatening because it can be used to steal a person's digital identity.

Spyware

16 Along with spam and phishing, spyware represents the third of an unhappy trinity of Internet pests. These harmful and secret programs typically find their way onto a computer system alongside another, often free, software application, although some can also exploit software bugs to get onto a machine. The programs are used to serve up unwanted adverts, change system settings and gather information on a user's online behavior for marketing purposes.