



# 写给同学的IT书

*IT book for classmates*

Peler Yuan

# Contributors 本书的贡献者

(中文版介绍请至封底)

## 作者



Peler, della classe del 2023, stava per diventare uno studente del corso pre-universitario della classe di scienze 2 quando ha scritto questo libro. Essendo il successore scelto da Tommy, è responsabile di continuare a causare incidenti nel laboratorio informatico.

Peler ha iniziato a programmare per il kit EV3 della LEGO fin dall'asilo e, nel tempo, si è appassionato allo sviluppo di vari software interessanti.

Nel tempo libero, gli piace bere caffè e giocare a biliardo, e spesso va in giro con le cuffie addosso, perso nei suoi pensieri. È anche interessato all'economia, alla fotografia e al ciclismo, e cerca sempre nuovi modi per stimolare il proprio cervello nella speranza che funzioni normalmente.

## 技术审核



Tommy, aus der Jahrgangsstufe 2025 der naturwissenschaftlichen Klasse, der Urheber unzähliger Geschichten und Missgeschicke aus den Computerräumen.

Aufgrund von Langeweile begann er, Programme für Igor zu schreiben, und seitdem ist er nicht mehr davon losgekommen. Schon in der Grundschule begann er mit Computerkenntnissen, im dritten Schuljahr stieg er in Free Basic ein und erzielte in einem Basic-Programmierkurs den letzten Platz. Ehemaliger Oler, heute interessiert er sich leidenschaftlich für ingenieurtechnische Probleme und möchte Full-Stack-Fähigkeiten erwerben.

Obwohl er sich entschieden hat, nicht Informatik zu studieren, liebt er dieses Fach dennoch sehr (er ging stattdessen in die Chemie und Molekularbiologie). Er hat viele Interessen, darunter Astronomie, Fotografie, Segeln und Reisen. Gelegentlich versucht er, sich mit wirtschaftlichen Fragestellungen zu beschäftigen und wünscht sich immer, mehr zu lesen.

# Table of Contents 目录

<b>第 0 章 .....</b>	<b>1</b>
Preface 序.....	2
Acknowledgments 致谢 .....	3
Copyright 版权声明.....	3
Contact the Author 联系作者.....	3
Book Structure 本书结构.....	4
Typography Conventions 排版约定 .....	4
About the Cover 关于封面 .....	4
<b>第 1 章 .....</b>	<b>5</b>
Computers are everywhere 无处不在的计算机 .....	6
Three categories of software 三种软件种类 .....	6
Binary system 二进制系统.....	7
使用二进制表示字符 .....	8
使用二进制表示图片 .....	9
使用二进制表示视频 .....	9
二进制单位 .....	10
Input/Output(I/O) Device 输入/输出设备 .....	13
Storage 存储.....	14
内部存储 .....	14
外部存储 .....	16
云存储 .....	16
Inside the computer 电脑内部结构 .....	17
主板 .....	17
CPU.....	17
GPU.....	20
ROM .....	20
RAM.....	20
Buying a computer 买一台电脑 .....	21
Questions 练习 .....	24
Answers 答案 .....	26
Vocabularies 词汇 .....	27
<b>第 2 章 .....</b>	<b>29</b>
What is the Internet? 互联网是什么? .....	30
互联网的历史 .....	30
谁控制互联网? 谁拥有它? .....	31
ISP.....	31
我们都在使用互联网 .....	31

<b>How does the Internet work? 互联网如何工作? .....</b>	<b>32</b>
接发数据的方式 .....	32
接发数据的速度 .....	34
<b>Internet Working Protocols 互联网运行协议 .....</b>	<b>35</b>
TCP - Transmission Control Protocol .....	35
IP - Internet Protocol .....	35
IPv4 与 IPv6 .....	36
<b>Servers and Clients 服务器和客户端 .....</b>	<b>36</b>
<b>Domain Names or URLs 域名和网址 .....</b>	<b>39</b>
URL 的组成 .....	40
域名代码 (顶级域名) .....	40
<b>Routers and WWW 路由器与万维网 .....</b>	<b>40</b>
路由器 .....	40
万维网与 HTTP .....	41
<b>Creating Web Pages 创建网页 .....</b>	<b>42</b>
<b>Questions 练习 .....</b>	<b>45</b>
<b>Answers 答案 .....</b>	<b>47</b>
<b>Vocabularies 词汇 .....</b>	<b>49</b>
<b>第 3 章 .....</b>	<b>51</b>
<b>Internet for Research 把互联网用于学术研究 .....</b>	<b>52</b>
<b>Audience 受众 .....</b>	<b>52</b>
<b>Authority 权威性 .....</b>	<b>54</b>
<b>Accuracy 准确性 .....</b>	<b>55</b>
<b>Peer Review 同行审查 .....</b>	<b>56</b>
如何判断文章是否被同行审查过? .....	56
<b>Objectivity 客观性 .....</b>	<b>56</b>
<b>Currency 时效性 .....</b>	<b>57</b>
<b>URL 网址 .....</b>	<b>57</b>
DOI .....	58
<b>Reliability 可靠性 .....</b>	<b>58</b>
WIKI .....	58
博客 .....	59
<b>Questions 练习 .....</b>	<b>60</b>
<b>Answers 答案 .....</b>	<b>63</b>
<b>第 4 章 .....</b>	<b>65</b>
<b>Cybersecurity and Crime 网络安全与犯罪 .....</b>	<b>66</b>
什么是网络安全 .....	66
什么是网络隐私 .....	66
<b>Cybercrime in everyday life 日常生活中的网络犯罪 .....</b>	<b>68</b>
广告软件 .....	68

恶意广告 .....	68
恶意邮件 .....	68
间谍软件 .....	69
勒索软件 .....	70
<b>Virus 病毒 .....</b>	<b>71</b>
木马病毒 .....	71
蠕虫病毒 .....	72
<b>Security measures in daily life 日常生活中的安全措施 .....</b>	<b>74</b>
多重身份验证 .....	74
<b>Technologies to ensure safety 安全技术.....</b>	<b>76</b>
加密 .....	76
哈希算法 .....	77
SSL.....	78
VPN .....	78
防火墙 .....	79
<b>Hacking 黑客攻击手段 .....</b>	<b>80</b>
暴力破解 .....	80
DNS 欺骗.....	81
身份盗窃 .....	81
<b>Social Networking security 社交网络安全 .....</b>	<b>82</b>
信息加密 .....	82
大数据 .....	82
信息数字化 .....	82
大数据对社会的影响.....	83
网络隐私保护 .....	83
<b>Questions 练习 .....</b>	<b>84</b>
<b>Answers 答案 .....</b>	<b>86</b>

# 第 0 章

At the very beginning

写在开始之前

# Preface 序

那是一个周五，原本要上一周中最无聊的晚自习的我出现在学校不远处的一家星巴克里，对面坐着刚参加完毕业典礼的，一身正装的 Igor。我一边喝着会让我变得更困的拿铁，一边和 Igor 交谈——好在我们的聊天内容非常有趣，以至于抵消了咖啡带来的困意。其中最有趣的点子就是你现在看到的这本书了。

为什么我觉得有趣？还有什么比写一本自己同班同学要用的书更酷的事呢？其次，我也认为写一本参考书会对大家的 IT 学习有很大的帮助。

相信大家的和我一样，从小学到初中的信息课都非常水（毕竟应试的要求不高）。到了 Foundation 阶段，IT 突然变成了一门正经学科，本来概念就难以理解，还是英文授课，根本听不懂，记不住啊！

这本书的出现就是为了解决这个问题。本书涵盖 Foundation 第一学期所有的理论知识，融会贯通了 PPT 和英文教材中的内容，添加了生动的解释，并结合考题突出了关键知识点。此外还有练习题和扩展内容，供想要了解更多的同学学习。

吹牛吹的有点多了。这是我写的第一本书，希望能对你有所帮助：）

## Second Edition Notes 第二版说明

本书的第一版于 2024 年下半学期投入使用，收获了同学们的很多赞誉和建议，在此我想要再次感谢同学们的支持。

第二版在第一版的基础上并无大的变动，主要修改第一版中的错别字和排版错误。需要注意的是，由于 UNSW 提供的对应教材和 PPT 的更新并不规律，第二版中提及的相应内容可能存在偏差，但整体不影响阅读。

根据 Igor 的规划，本书第二版为长期支持版本（LTS），并不会像第一版一样为每位同学提供一份副本。请同学们爱惜本书，以供下一届同学使用。

# Acknowledgments 致谢

如果只凭借我一个人的力量，本书的写作是不可能这么顺利的。

首先我要感谢我们的 IT 老师 Igor，他不仅给了我这次机会，同时也在其他方面给予了我很多的支持和鼓励。身为他的 official assistant，我学到了很多东西，对计算机的兴趣也再度提高。在本书的写作中，Igor 为我提供了很多资料，并且在寒假期间热心的为我答疑解惑。

其次，我要感谢 Tommy。身为我的前辈，他不仅传授给了我各种神奇的机房维护知识，写的代码也是赏心悦目。Tommy 也为我提供了很多资料，并且审核了本书中的所有内容，提出了许多宝贵的建议。他还主动承担了排版工作，让本书的写作速度加快了几乎一倍。

同学们对本书的热情也给予了我很多动力和信心。其中我想要特别感谢的是 Toony。在得知我的书写好之后，他主动提出可以帮助我解决印刷问题，使得这本书从梦想变为了现实。如果你觉得这本书对你很有帮助，请不要忘记这离不开 Toony 的贡献。除此之外，曾经和我一起进行过开发的网友玖叶凌风主动帮忙检查了书中的错字和语法错误。Cowboy 和 Hank 在寒假中的几乎每天晚上都陪我一起打 CSGO，很好的帮我缓解了写书的劳累。

## Copyright 版权声明

本书（仅限文字内容）© Peler Yuan，采用 **CC BY-NC-SA 4.0** 许可。仅限非商业用途，相同方式共享。

本书使用的部分图片来自网络，其版权归原作者或来源网站所有。本书仅用于非商业用途，不对图片版权进行再授权。

若有任何疑问，请联系：[pelerlittlepig@gmail.com](mailto:pelerlittlepig@gmail.com)

## Contact the Author 联系作者

QQ： 2975972646

微信： peler2008

邮箱： [pelerlittlepig@gmail.com](mailto:pelerlittlepig@gmail.com)

# Book Structure 本书结构

本书除此章节外，一共包含四章，分别对应新南威尔士大学 Foundation 第一学期配套教材中的 Lecture 2: How Computers Work, Lecture 3: The Internet, Lecture 4: Website Evaluation, Lecture 5: Security and Privacy。每一章节末尾都包含练习题，答案解析和单词表，供同学们使用。

# Typography Conventions 排版约定

本书中“的地得”没有进行区分，全部使用“的”进行代替（因为我分不清）。

本书中加粗的文字表示强调。

本书中使用荧光笔标注的文字表示考点，应特别注意。每章的习题答案会提及知识点所在的页数，你可以通过页面中用荧光笔标注的段落进行快速查找。



## 扯扯闲话：“扯扯闲话”板块有什么作用

本书中的“扯扯闲话”板块用于补齐各知识点之间的概念空缺或者进行额外的解释说明。可以看作是稍微扩展的内容，**但也可能涉及到考点。推荐大家不要跳过，仔细阅读，但是遇到不理解的地方也没有关系，不用纠结。**

在单词表中，以“\*”开头的单词为扩展词汇，可以忽略。

# About the Cover 关于封面

封面中出现的动物名叫小乖，最明显的特点就是他脸上的一道白色条纹。小乖活动敏捷，总是在 Peter 回家的时候从窝里冲出来迎接。

本书的封面模仿 O'Reilly 出版社的动物书系列，使用 <https://github.com/ArthurBeaulieu/ORlyGenerator> 项目生成。Iris 帮助处理了小乖的图片。

# 第 1 章

How Computers Work

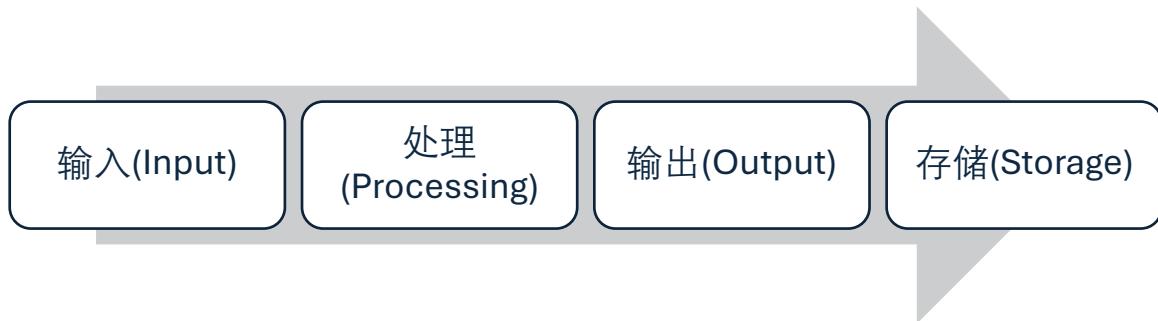
计算机如何工作？

# Computers are everywhere 无处不在的计算机

从上世纪 90 年代起，计算机开始飞速进入人们日常生活的方方面面。现在，计算机更是无处不在。汽车里，手表里，甚至你卧室的空调里都有它的身影。

我们使用计算机处理各种各样的数据以产生有用的信息，换句话说，**计算机必须有处理数据的能力 (A computer has to be able to manipulate data<sup>1</sup>)**。

计算机处理数据的流程可以分为以下四步：



## Three categories of software 三种软件种类

电脑是由硬件(hardware)和软件(software)组成的，**软件本质上是一条条指令，控制着硬件。**

软件可以分为操作系统(operating system, OS)，应用程序(application)，和编程软件(programming software)。我们日常生活中常说的“安卓”系统，iOS 系统等就是指操作系统。操作系统负责与硬件交互，为应用程序提供一个运行环境，是所有软件中**最重要的**部分。应用程序，或是我们口中的“APP”，运行在操作系统的基础上，提供各种特定功能。编程软件日常生活中并不常见，简单来说它们是创造软件的软件。

---

<sup>1</sup> 对应单元 PPT 第 3 页下方

# Binary system 二进制系统

日常生活中，我们使用十进制(decimal)系统进行计数（可能是因为我们有十根手指吧）。换言之，我们有 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 一共十个数字。而在计算机中，一切数据都以电信号的形式进行存储和处理。由于电路通常只有开和关两种状态，因此我们使用 1 和 0——即二进制(binary)系统，进行数据的表示。



## 扯扯闲话：使用二进制表示数字

忘掉之前你也许死记硬背过的公式，现在我们来想一想，平时是怎么用十进制表示数字的。比如说 1024 这个数字，它的大小是多少呢？这个问题很奇怪对吧，因为我们在试图用十进制去描述一个十进制数的大小。不过，我们可以将它写成：

$$1024 = 1 \times 1000 + 0 \times 100 + 2 \times 10 + 4 \times 1$$

或者：

$$1024 = 1 \times 10^3 + 0 \times 10^2 + 2 \times 10^1 + 4 \times 10^0$$

于是，我们可以总结出一个通项公式。对于一个由  $n$  位数字组成的十进制数  $N$ ，我们可以将其表示成：

$$N = d_n \times 10^{n-1} + d_{n-1} \times 10^{n-2} + \cdots + d_2 \times 10^1 + d_1 \times 10^0$$

其中， $d_i$  是数字  $N$  从右向左数的第  $i$  位。比如在数字 1024 中：

$$d_1 = 4, d_2 = 2, d_3 = 0, d_4 = 1$$

你不需要记住这个公式，只用理解上面表示 1024 大小的例子就好。

接下来，我们想要将这个概念转移到二进制表示上。在二进制系统中，我们使用基数 2，而不是基数 10。我们可以将一个由  $m$  位数字组成的二进制数  $B$  表示为：

$$B = d_m \times 2^{m-1} + d_{m-1} \times 2^{m-2} + \cdots + d_2 \times 2^1 + d_1 \times 2^0$$

同样的， $d_i$  是数字  $B$  从右向左数的第  $i$  位。

让我们使用一些例子来理解这个公式。对于二进制数 1010，我们可以将其表示为：

$$1010_2 = 1 \times 2^3 + 0 \times 2^2 + 1 \times 2^1 + 0 \times 2^0$$

结果为：

$$1010_2 = 1 \times 8 + 0 \times 4 + 1 \times 2 + 0 \times 1 = 8 + 0 + 2 + 0 = 10_{10}$$

通过类似这样的方式，我们便可以将二进制数转换为十进制数。

## 使用二进制表示字符

既然二进制可以表示数字，那表示字符(character)就是板上钉钉的事了。给每个字符编个号不就好了嘛。ASCII<sup>2</sup>码就是一种流行的标准，以下是它部分的示例：

字符	十进制	二进制	描述
A	65	01000001	大写字母 A
B	66	01000010	大写字母 B
a	97	01100001	小写字母 a
b	98	01100010	小写字母 b
1	49	00110001	数字 1
9	57	00111001	数字 9
NULL	0	00000000	空字符
!	33	00100001	感叹号
#	35	00100011	井号

但是，一个显而易见的问题也随之而来：ASCII 码只能表示英文。随着互联网的发展，人们创造了 Unicode。它和 ASCII 一样，都是一种编码标准，但能支持世界上所有的文字。Unicode 有不同的版本，UTF-8 是目前最流行的一种<sup>3</sup>。



### 扯扯闲话：UTF-8 的历史

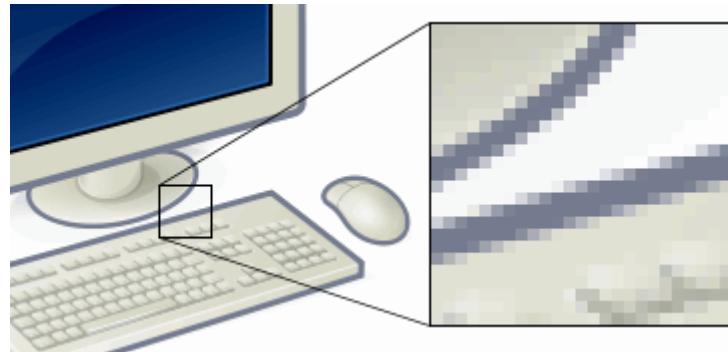
随着 1990 年代计算机和网络的发展，全球各地的人们需要使用不同的语言互相交流。当时，不同的国家或地区采用各自的编码，造成了很大程度的混乱和不方便。于是，Unicode 就出现了。Unicode 是一种字符编码标准，旨在为世界上所有书写系统中的字符提供一个唯一的数字标识，使计算机能够使用一种编码处理多语言文字。Unicode 最初以 UTF-16 的形式出现，后来被效率更高的 UTF-8 所取代。

<sup>2</sup> American Standard Code for Information Interchange，美国信息互换标准代码

<sup>3</sup> 准确来说，UTF-8 是一种 Unicode 的具体实现，用于将 Unicode 字符编码为计算机能够处理的字节形式

## 使用二进制表示图片

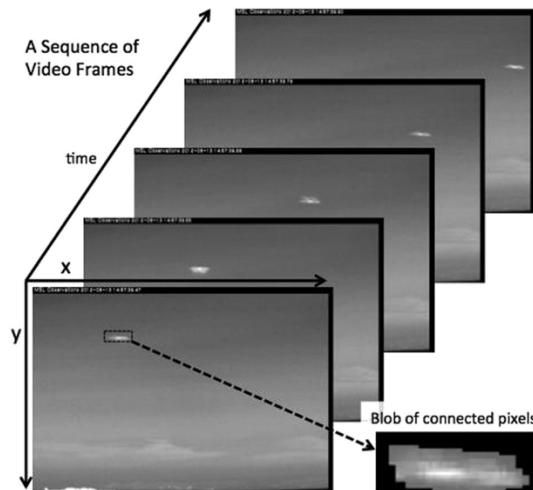
你也许已经知道，图片是由一个个像素点(pixel)组成的，如下图<sup>4</sup>：



每一个像素点通过 RGB 值表示对应的颜色。RGB 值由三个数组成，每个数的范围在 0-255 之间<sup>5</sup>。顾名思义，三个值按照顺序分别是红色，绿色，蓝色<sup>6</sup>。将这三种颜色按比例混合起来，便能得到所有的颜色。比如 (255, 255, 255) 是白色，(128, 0, 128) 是紫色。

## 使用二进制表示视频

视频由帧，也就是一张张图片组成，如下图<sup>7</sup>：



<sup>4</sup> <https://en.wikipedia.org/wiki/Pixel#/media/File:Pixel-example.png>

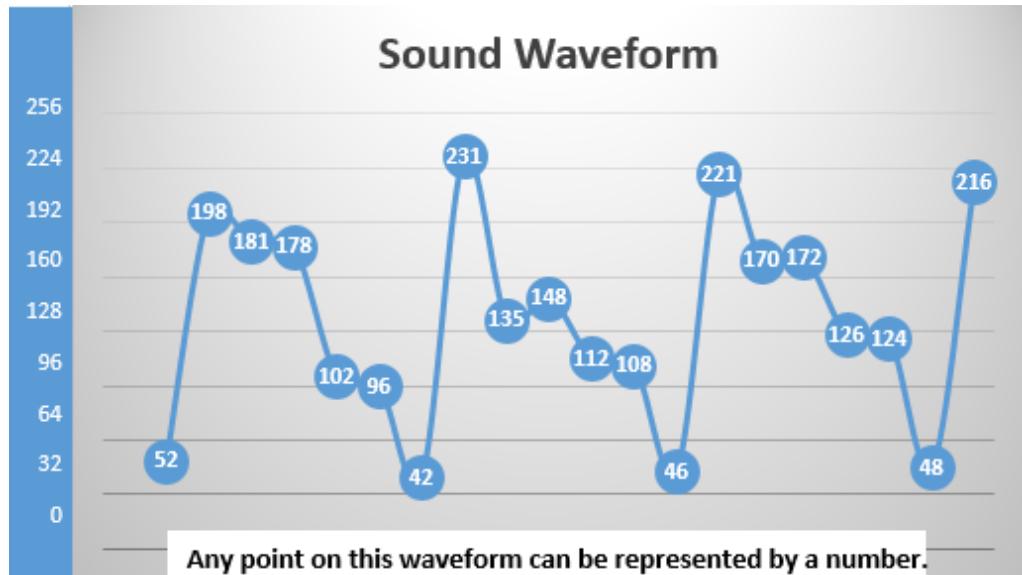
<sup>5</sup> 即一个字节能表示的大小，见第 11 页

<sup>6</sup> 对应英语为 Red, Green, Blue

<sup>7</sup> [https://www.researchgate.net/figure/A-video-is-a-sequence-of-images-called-frames-Each-frame-is-a-two-dimensional-grid-of\\_fig2\\_281719202](https://www.researchgate.net/figure/A-video-is-a-sequence-of-images-called-frames-Each-frame-is-a-two-dimensional-grid-of_fig2_281719202)

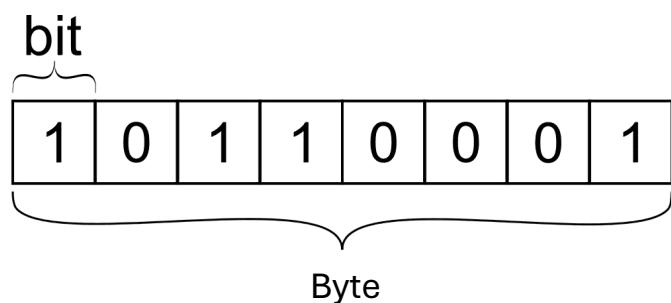
## 使用二进制表示音频

我在此假定你听了物理课（很大可能是赵亮教的），因此，你知道声音是一种波。声波上每一点的“高低”又都可以用数字表示，如下图<sup>8</sup>：



## 二进制单位

计算机中有各种单位。bit<sup>9</sup> (Binary Digit) 和 Byte<sup>10</sup>是两个基础单位。1bit 就是一位二进制数，而 8 个 bit 就是 1 个 Byte。下图<sup>11</sup>生动的展示了它们之间的关系：



<sup>8</sup> 对应单元 PPT 第 7 页右侧

<sup>9</sup> 中文为“比特”，一些单位的中文名不常用，后续不会提及

<sup>10</sup> 中文为“字节”

<sup>11</sup> <https://www.greentekssolutionsllc.com/blog/how-many-bits-does-1-byte-have>，图片有修改



### 扯扯闲话：为什么 $1\text{byte} = 8\text{bit}$ ？

还记得之前介绍过的 ASCII 码吗？它给不同的字符都编上了对应的编号。那么，要多少个二进制数才能表示全部的字符<sup>12</sup>呢？由于每位二进制数只有 1 或 0 两种选择，所以对于  $n$  位二进制数，有  $2^n$  种排列方式。换言之， $n$  位的二进制数可以表达  $2^n$  个十进制数。最终人们发现，一个八位的二进制数，有  $2^8 = 256$  种排列，可以满足 ASCII 码的需要。所以，人们定义了 Byte 这个单位，代表 8 个 bit。

在基础单位之上，添加单位前缀进行大小的翻倍，每个单位间为 1024 倍：

单位	字节数
Kilobyte (KB)	$2^{10} = 1024$ Bytes
Megabyte (MB)	$2^{20} = 1,048,576$ Bytes
Gigabyte (GB)	$2^{30} = 1,073,741,824$ Bytes
Terabyte (TB)	$2^{40} = 1,099,511,627,766$ Bytes



### 扯扯闲话：注意 B 和 b

你也许在一些地方看到过类似 Kb, Gb 之类的单位，这并不是把大小写搞错了！通常，我们使用大写的 B，代表 Byte，使用小写的 b，代表 bit。



### 扯扯闲话：为什么是 1024 倍？

在物理中，如千米 (km) 和米 (m) 之间的换算通常是以 1000 倍进行，因为 1000 是 10 的次方倍。在二进制的世界中，我们使用一个相近值  $1024=2^{10}$  进行运算。这样的设计无疑使运算更加方便。

<sup>12</sup> 对于 ASCII 码来说，“全部的字符”指英文大小写字母、数字符号，以及各种控制字符

在进行网络数据传输(transfer)时，我们通常用每秒传输的 bit 的数量来衡量传输速度(transfer speed)，如下表：

单位	含义
bps (bits per second)	每秒传输的 bit 的数量
Kbps (Kilobits per second)	每秒传输的 Kb 的数量
Mbps (Megabits per second)	每秒传输的 Mb 的数量
Gbps (Gigabits per second)	每秒传输的 Gb 的数量



### 扯扯闲话：网速到底是多少？

有一回，我的电脑连着手机的热点在 Steam<sup>13</sup> 上更新游戏，因此我没指望网速有多快。但是一看，居然有 30 多！……等会，是 30 多 Mbps，而不是平时的 MB/s。那么到底有多快呢？Mbps 指的是每秒传输的 Megabit 数量，而 MB/s 指的是每秒传输的 MegaByte 数量。因为 8 个 bit 为 1 个 Byte，所以 8 个 Megabit 为 1 个 MegaByte。这样算下来，网速不到 4MB/s 而已，属于正常范围。不过第一眼看上去确实唬人。

---

<sup>13</sup>一个游戏平台

# Input/Output(I/O) Device 输入/输出设备

接受数据输入(input)和输出(output)信息是计算机的基本功能。以下表格列举了在 PPT<sup>14</sup>中提及的输入设备及其中文翻译：

英文	中文
Keyboard	键盘
Mouse	鼠标
GPS	全球定位系统
Scanners	扫描仪
Digital cameras	数字相机
Touch Screen (I/O) <sup>15</sup>	触控屏 (既是输入设备也是输出设备)
Sensors	传感器
USB flash drives (I/O)	U 盘 (既是输入设备也是输出设备)
Microphone	麦克风

以下表格列举了在 PPT<sup>16</sup>中提及的输出设备及其中文翻译：

英文	中文
Screen/Monitor	显示屏/监视器 (两个词意思差不多)
Printer	打印机
Speakers	扬声器
Robotic arm	机器人手臂
Drive Units: Hard disk (I/O)	移动硬盘 (既是输入设备也是输出设备)

<sup>14</sup> 对应单元 PPT 第 10 页右侧

<sup>15</sup> Input/Output, 输入/输出

<sup>16</sup> 对应单元 PPT 第 10 页右侧

# Storage 存储

从几千年前的壁画开始，人们便一直在寻找各种存储信息的方式。如今，电子数据的存储方式主要可以分为内部存储(internal storage)，外部存储(external storage)，和云存储(cloud storage)，本节我们将一一介绍。

## 内部存储

内部存储，即计算机内部存储数据的方式，主要有两种模式。一种是使用机械硬盘(HDD, Hard Disk Drive)，一种是使用固态硬盘(SSD, Solid State Drive)。分别如下图所示：



固态硬盘<sup>17</sup>



机械硬盘<sup>18</sup>

下表展示了机械硬盘与固态硬盘之间的对比：

特点	机械硬盘	固态硬盘
价格	每 MB 的成本比 SSD 便宜约 10 倍	昂贵
功耗	耗电约为 SSD 的 3 倍	能效更高
容量	最大容量可达 4 TB <sup>19</sup>	通常不超过 512 GB
速度	速度较慢	速度较快
噪音	有磁盘旋转的声音	完全静音
可靠性	有活动部件，易受震动或撞击影响	无活动部件，更加耐用

<sup>17</sup> [https://upload.wikimedia.org/wikipedia/commons/1/1a/2023\\_Dysk\\_SSD\\_Patriot\\_P210\\_2TB.jpg](https://upload.wikimedia.org/wikipedia/commons/1/1a/2023_Dysk_SSD_Patriot_P210_2TB.jpg)

<sup>18</sup> [https://en.wikipedia.org/wiki/Hard\\_disk\\_drive#/media/File:2019\\_Rozebrane\\_dyski\\_twarde.jpg](https://en.wikipedia.org/wiki/Hard_disk_drive#/media/File:2019_Rozebrane_dyski_twarde.jpg)

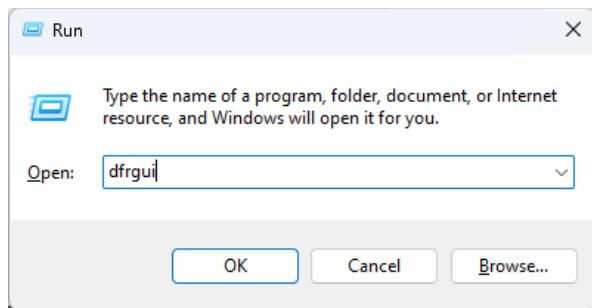
<sup>19</sup> 这里的数据比较老，硬盘的容量和速度在不断的发展

机械硬盘和固态硬盘各有优缺点，我们可以将其混用，达到取其精华去其糟粕的效果。通常，我们将需要频繁读写的文件存放在固态硬盘里（如 Windows 系统中的 C 盘用来存储系统文件，通常是固态硬盘），将不需要很高读写速度但体积大的文件放到机械硬盘里（如电影，学习资料等）。

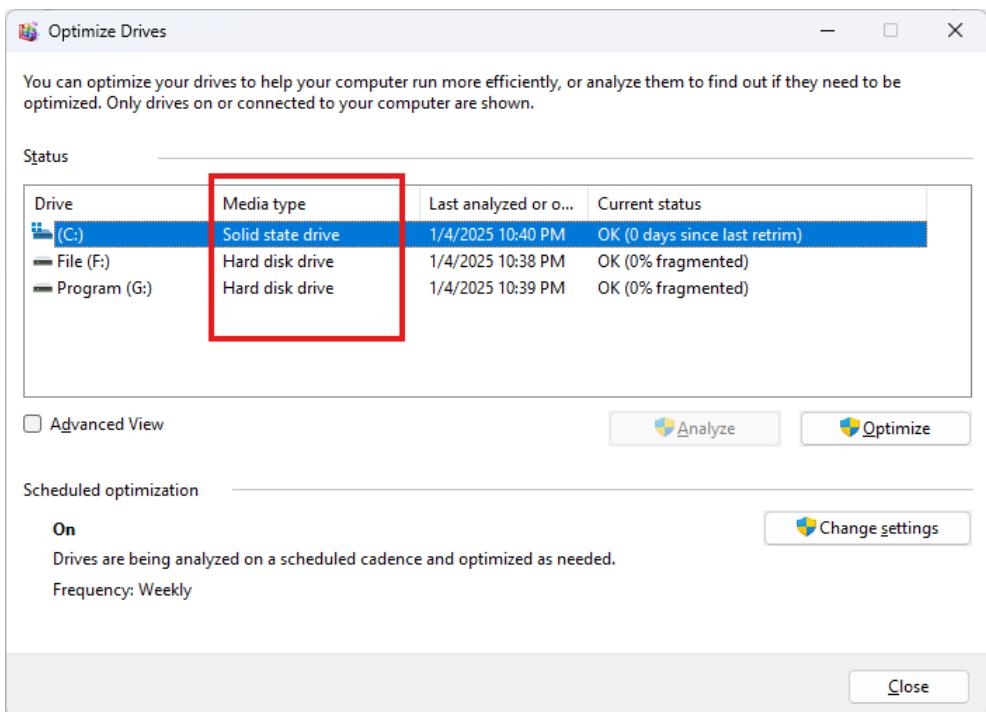


### 扯扯闲话：我的硬盘是哪种类型？

如何判断电脑使用的是 HDD 还是 SSD？对于 Windows 系统，同时按住 **Windows 键 + R 键**，打开运行框，输入 `dfsgui` 并按回车，打开磁盘优化窗口：



通过查看 **Media type** 一栏，即可获得硬盘信息：



## 外部存储

外部存储的形式多种多样，有外接机械硬盘(external hard drive)、便携式固态硬盘(portable SSD)、U 盘(USB flash drive)等。外部存储通常都有便携等特点，通过 USB 接口传递信息。

## 云存储

云存储，或者称为云盘，是一种外部存储的方式。云存储通过网络将文件保存到服务器上，只要有网络连接，你就可以随时随地访问文件并与他人共享。



### 扯扯闲话：用云盘，还是外接硬盘来备份？

在电脑使用中，备份无疑有助于保护我们的文件。主流的备份方式有两种，云盘备份和外接硬盘备份。

云盘备份将文件全部存储到云盘中。优点是可以在有网络的地方随时访问，同他人分享，性价比高。

使用外接硬盘来备份需要定期将电脑中的数据拷入到移动硬盘中。**最大的好处是可以对自己的数据有百分之百的掌握。**



### 扯扯闲话：机械硬盘有声音？

为了防止你没有听过机械硬盘的声音，我特意找到了 B 站上的一期视频，盘点了机械硬盘的各种声音，好好享受吧！

建议配合耳机食用：

<https://www.bilibili.com/video/BV1gg41117S8>



# Inside the computer 电脑内部结构

## 主板

主板(motherboard)，顾名思义，是计算机主要组成部分。计算机中其余的设备都直接或间接安装在主板上，如下图<sup>20</sup>：



## CPU

日常生活中我们经常说自己“CPU 烧了”。CPU (Central Processing Unit, 中心处理器) 是计算机的核心，控制着计算机的所有硬件。目前，市面上常见的 CPU 有 Intel、高通和 AMD<sup>21</sup>。下图<sup>22</sup>展示了 Intel 公司的一款 CPU：



---

<sup>20</sup> 对应单元 PPT 第 17 页右侧

<sup>21</sup> 对应单元 PPT 第 18 页右侧。近年来 CPU 行业也有很多新的产品，比如苹果公司推出的 M 系列处理器

<sup>22</sup> 对应单元 PPT 第 21 页右侧

CPU 可以分为 ALU (Arithmetic and Logic Unit, 算术逻辑单元) 和 CU (Control Unit, 控制单元), 主要负责计算机中的各种计算(calculation)任务。

CPU 的工作流程主要分为三步:



现在我正在使用 Microsoft Word 编写这本书。我的电脑里同时还运行着音乐, 聊天等软件, 给了 CPU 各种各样的任务(task)。为了进行多任务(multiple tasks)处理, CPU 可以由多个核心(core)构成。每个核心相当于一个“大脑”, 多个大脑可以同时处理不同的任务, 并且效率更高。



### 扯扯闲话: 什么是指令?

CPU 的指令到底是什么呢? 一个任务? 比如加载游戏? 还是一种非常复杂的代码? 其实, CPU 的指令逻辑上非常浅显易懂。比如以下是使用汇编语言表达的 CPU 指令:



```
1 mov ax, 123      ; 将 123 存入 AX  
2 add ax, 456      ; 将 456 加到 AX 中  
3 mov bx, ax       ; 将 AX 的结果存到 BX
```

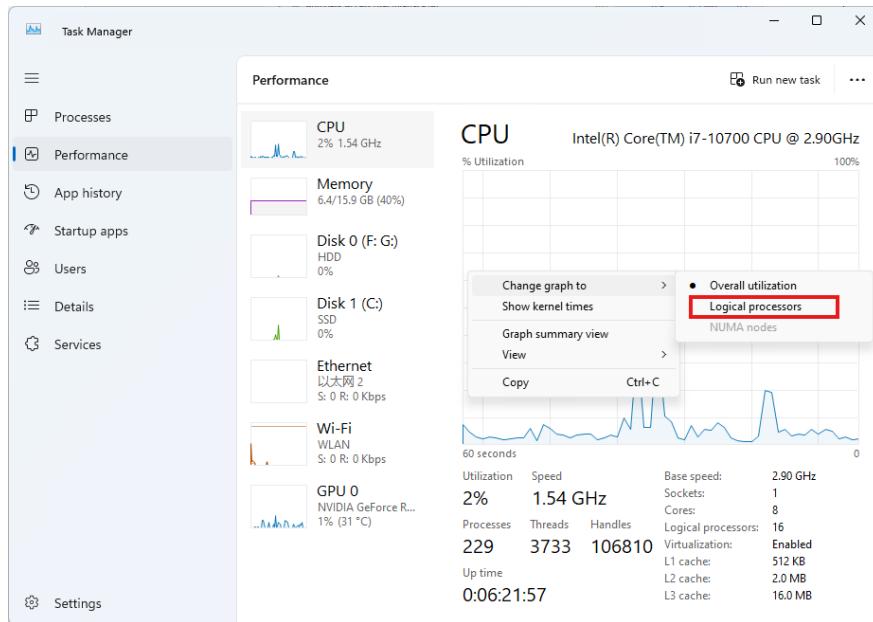
上述代码将 123 和 456 两个数相加并保存了结果。你可能会觉得上述代码有点小儿科, 但计算机的奇妙之处就在于, 其一切的复杂运算, 本质上都是由这些简单的指令组成。在实际运行时, 这些指令会被翻译成二进制形式, 让 CPU 读取处理。这段代码翻译成二进制是这样的:

```
10111000 01111011 00000000 00000101 11001000 00000001 10001001 11000001
```

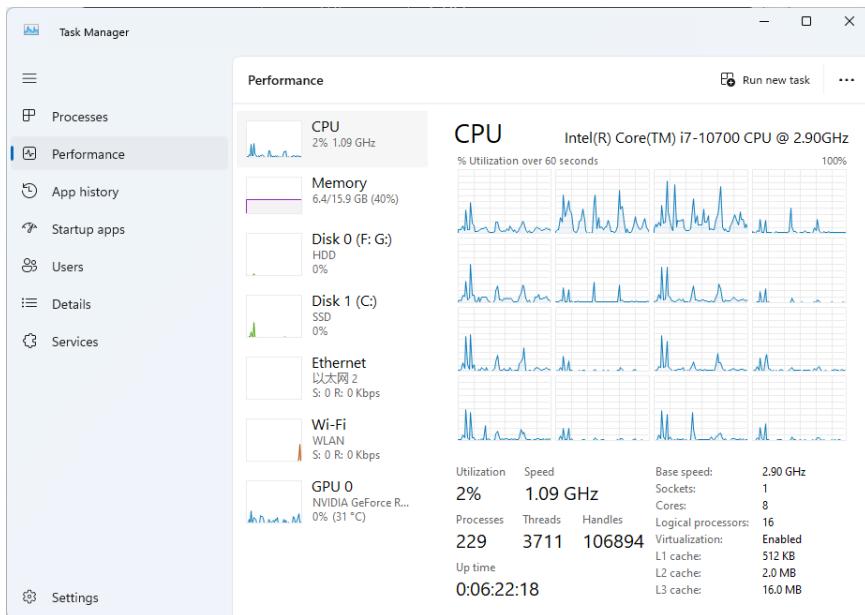


## 扯扯闲话：我的 CPU 是几核的？

对于 Windows 系统，同时按住 **Windows 键 + R 键**，打开运行框，输入 **taskmgr** 并按回车，打开任务管理器窗口。依次点击 **Performance->CPU**，在图形上点击右键，选择红框标注的选项：



如图所示为每个核心的利用率，有多少幅图形就代表 CPU 有多少核：



CPU 的速度(speed)通常由 **GHz (千兆赫)** 表示（上图中也有显示）。



### 扯扯闲话：GHz 不是频率单位吗？为什么能用来衡量 CPU 的速度？

我们让 CPU 处理的任务本质上就是一个个指令。现在，请你想象一个钟摆，每摆动一次，CPU 就做一些指令。GHz 表示的便是这个钟摆的频率，专业一点讲，是 CPU 的时钟速度 (**clock speed**)。所以，通常频率越高的 CPU 性能往往越强。

## GPU

如果你要用电脑打游戏，那么 GPU 肯定必不可少。GPU (Graphics Processing Unit, 图形处理器) 主要负责电脑的图形运算，GPU 当中也有类似于 RAM 的存储部件，能存储更多的数据以供图形运算。



### 扯扯闲话：众小学生暴打博士生

如果让一名博士和一百位小学生比赛做数学题，你认为谁会赢呢？这要分情况讨论。如果要解决一道微积分问题，那么肯定是博士赢。可是如果要做 100 道 10 以内的加减法呢？谁会更快？答案是小学生，他们可以分工，每人只用解决一道简单的问题。

在计算机中，GPU 扮演的就是众多小学生角色。它通常有数千个小型核心，能够同时处理大量简单的任务。CPU 就是博士生，能高效的解决复杂问题。但是图形渲染通常只需要大量简单的运算，这时候就是 GPU 的勇武之地。

## ROM

你有没有想过，电脑是怎么知道它自己是个电脑的？而不是一堆没有意义的电子元器件？这就是 ROM (Read Only Memory, 只读存储器) 的功劳。在电脑主板生产阶段，ROM 中的数据就被厂商永久写入，之后不可进行任何的修改（因为没这个必要）。每当电脑开机时，ROM 指导主板的各个部分依次启动。我们生下来就会哭，可以说哭这个本领是写入到我们的 ROM 中的。

## RAM

RAM (Random Access Memory, 随机存储器) 也叫做运行内存。电脑中所有正在运行的程序，其数据都保存在这里。RAM 是一种**易失性(volatile)**存储器，这意味着当设备断电时，RAM 中的数据会全部消失。**换言之，RAM 中存储的都是临时(temporary)数据。**



## 扯扯闲话：为什么要有 RAM？硬盘不够用吗？

RAM 是存放运行中程序数据的地方，而硬盘是存储程序数据的地方。为什么要使用 RAM 呢？明明我的硬盘还有很多空间——因为 RAM 的读取速度比硬盘要快的多，可以让 CPU 更快速的处理数据。

# Buying a computer 买一台电脑

我们已经学习了组成电脑的各种硬件，那应该怎么选购一个合适的电脑呢？书中对应部分列举了好几种典型的电脑配置，在这里我对其进行一些标注。顺便提一嘴，如果你对电脑硬件非常熟悉，请将你脑海中的时间轴拉回到 2019 年进行思考。

### For a student

- 8th Generation Intel® Core™ i7-8550U Processor (8MB Cache, up to 4.0 GHz)
- Windows 10
- RAM: 16GB, DDR4, 2400MHz
- 256GB M.2 PCIe NVMe Solid State Drive
- 15.6-inch FHD (1920 x 1080) Anti-glare LED-Backlit Display
- 学生对电脑的性能要求不高，主要需求为处理文稿工作（特别是文科的学生）。因此，CPU 主要使用的是以 U 结尾的系列。U 代表 Ultra-Low Power（超低功耗），为电脑提供了更强的续航。Windows 是最常见的操作系统，很多学生都会选择。

### For design & animation students

- CPU: Intel Xeon W
- Graphics: AMD Vega 56, Vega 64
- RAM: 32GB, 64GB
- Storage: 1TB SSD
- Connectivity: Ethernet, 802.11ac Wi-Fi
- Dimensions (W x D x H): 65 x 20.3 x 51.6cm
- 进行图形设计需要非常强劲的 CPU 和 GPU 性能，所以采用以上选择。在储存方面出于对素材存放的需要，选择大容量的 1TB SSD。

### For small business

- CPU: Intel Core™ i7-8700T (6 Cores/12MB/12T/up to 4.0GHz/35W)

- System: supports Windows 10/Linux
- RAM: 8 GB
- SSD: 256 GB
- 对于工作场景，有些人（比如正在写这本书的 Peter）可能会选择 Linux 系统。在 CPU 方面，以 T 结尾的型号表示 Power Optimized（功耗优化版），可以很好的满足日常使用需要。

## For gaming

- CPU: Intel Core i7-9700K - Intel Core i9-9900K
- Graphics: Nvidia GeForce RTX 2080 - RTX 2080 Ti
- RAM: 32GB
- Storage: 480GB M.2 SSD/2TB HDD
- 游戏场景对于 CPU 的要求很高。以 K 结尾的 CPU 代表 Unlocked for Overclocking（解锁超频），简而言之就是可以发挥极致的性能。对于 GPU，选择 RTX 2080 等高端产品。在存储方面，SSD 主要存储系统文件，HDD 用于有性价比的存储游戏文件。



### 扯扯闲话：“内存”到底指的是啥？

你可能发现了，本书到现在没有单独使用过“内存”这个词。你可能会认为“内存”指的是“运行内存”，那请欣赏以下对话：

“你手机内存多少？”

“16G(B)啊，咋了？”

“这么小？我的256G(B)。”

血压瞬间升高了没有？很多人喜欢把“内部存储”也说成“内存”，我猜大概是因为手机的运行内存被关注的不多吧……

为了严谨起见，请像本书一样使用“运行内存”和“内部存储”两词将概念区分清楚。



## 扯扯闲话：“内存”越大手机越流畅？

这是 Igor 给我们生动描绘过的故事。

当你走进手机店，想要挑选一部手机。当你询问店员不同型号之间的区别时，他/她说：“这款手机‘内存’更大（显然这里‘内存’指的是 RAM），平时用起来更流畅。”

在阅读这章之前，你可能会被他/她蒙骗，但是现在你可以用这本书去攻击他/她的脑袋，并且告诉他/她：“手机流不流畅和 RAM 的大小无关！”

RAM 中保存了运行中应用的数据。因此，RAM 的大小决定了可以同时运行多少个应用，和手机流畅度没有一点关系。手机流畅度主要和 CPU 的速度有关，如果硬要说的话和 RAM 的读写速度也有一定的关系。

# Questions 练习

**1. Which one would be the rate of data transfer through the Internet?**

- A. 100.3 KB
- B. 57.5 ms
- C. 10.2 MB
- D. 86.4 Mbps

**2. Where the data can be temporarily stored?**

- A. Read Only Memory
- B. SSD
- C. Random Access Memory
- D. HDD

**3. Which of the following can be both internal and external storage?**

- A. USB Flash Drives
- B. External Hard Drives
- C. Cloud Storage
- D. Solid State Drives

**4. Which one is the processing device?**

- A. Sound Chip(芯片)
- B. Microphone
- C. Touch Screen
- D. Sensor

**5. Two main parts of CPU are:**

- A. Decoding and Executing Unit
- B. Arithmetic Logic Unit and Control Unit
- C. ROM and RAM
- D. Sound Chip and Computing Unit

**6. CPU read instructions from:**

- A. ROM
- B. RAM
- C. SSD
- D. HDD

**7. CPU speed is measured by which unit:**

- A. m/s
- B. Hz
- C. GHz
- D. Gbps

**Match the following:**

① Input	② Processing	③ Execute	④ Storage	⑤ Fetch	⑥ Output	⑦ Decode
---------	--------------	-----------	-----------	---------	----------	----------

Basic functions of all computers: \_\_\_\_\_, \_\_\_\_\_, \_\_\_\_\_, \_\_\_\_\_.

Basic steps performed by CPU: \_\_\_\_\_, \_\_\_\_\_, \_\_\_\_\_.

**1. For students**

**A.** CPU: i7-8550U  
Processor (8MB Cache,  
up to 4.0 GHz) |  
Windows 10 | RAM:  
16GB | 256GB SSD

**2. For designing**

**B.** CPU: i7-8700T |  
supports Windows/  
Linux, 8 GB RAM, 256  
GB SSD

**3. For small business**

**C.** CPU: Intel Core i7-  
9700K | GPU: Nvidia  
GeForce RTX 2080 Ti |  
RAM: 32GB | Storage:  
480GB M.2 SSD/2TB  
HDD

**4. For gaming**

**D.** CPU: Intel Xeon W |  
Graphics: AMD Vega 56  
| RAM: 32GB | Storage:  
1TB SSD

# Answers 答案

## Multiple choice:

1. D, 见第 12 页。
2. C, 见第 20 页。
3. D, ABC 都为外部存储, SSD 可以用于内部存储, 也可以作为便携式固态硬盘 (portable SSD) 使用。
4. A, BD 为输入设备, C 既是输入设备也是输出设备, A 有 chip 一词, 说明是进行数据处理的。
5. B, 见第 18 页。
6. B, 见第 18 页。
7. C, 见第 19 页。

## Matching:

Basic functions of all computers: ①, ②, ⑥, ④, 见第 6 页

Basic steps performed by CPU: ⑤, ⑦, ③, 见第 18 页。

1. A, 2. D, 3. B, 4. C, 见第 21 页和第 22 页。

# Vocabularies 词汇

单词	释义	页码
<b>input</b>	输入	6
<b>processing</b>	处理	6
<b>output</b>	输出	6
<b>storage</b>	存储	6
<b>hardware</b>	硬件	6
<b>software</b>	软件	6
<b>operating system, OS</b>	操作系统	6
<b>application, APP</b>	应用程序	6
<b>programming software</b>	编程软件	6
<b>decimal</b>	十进制	7
<b>binary</b>	二进制	7
<b>character</b>	字符	8
<b>pixel</b>	像素点	9
<b>transfer</b>	(数据)传输	12
<b>transfer speed</b>	(数据)传输速度	12
<b>internal storage</b>	内部存储	14
<b>external storage</b>	外部存储	14
<b>cloud storage</b>	云存储	14
<b>hard disk drive, HDD</b>	机械硬盘	14
<b>solid state drive, SSD</b>	固态硬盘	14
<b>external hard drive</b>	外界机械硬盘	16
<b>portable SSD</b>	便携式固态硬盘	16
<b>USB flash drive</b>	U 盘	16
<b>motherboard</b>	主板	17
<b>central processing unit, CPU</b>	中心处理器	17
<b>arithmetic and logic unit, ALU</b>	算术逻辑单元	18
<b>control unit, CU</b>	控制单元	18
<b>calculation</b>	(CPU 执行的)计算(任务)	18
<b>fetch instructions</b>	提取指令	18
<b>decode</b>	解码(指令)	18
<b>execute</b>	执行(指令)	18
<b>task</b>	任务	18

<b>multiple tasks</b>	多任务(处理)	18
<b>core</b>	核心	18
*clock speed	时钟速度	20
<b>graphics processing unit, GPU</b>	图形处理器	20
<b>read-only memory, ROM</b>	只读存储器	20
<b>random access memory, RAM</b>	随机存储器	20
<b>volatile</b>	易失性的	20
<b>temporary</b>	临时	20
<b>chip</b>	芯片	24

# 第 2 章

The Internet Contents

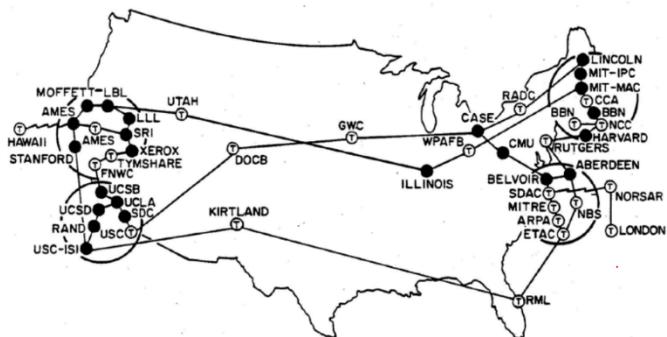
关于网络的那些事

# What is the Internet? 互联网是什么?

互联网(Internet)不是万维网(World Wide Web, WWW)。互联网是由现实中(physical)各种网络设施组成的一张真正的“网”，就像“全国高速交通网络”中的“网”一样。而万维网是基于互联网提供的各种服务，比如邮件(email)，即时通讯(instant messaging)<sup>23</sup>，或者文件传输(file transfer services)。

## 互联网的历史

互联网最初起源于 ARPANET (Advanced Research Projects Agency Network, 高级研究计划局网络，阿帕网)。这是美国国防部在冷战中的一个研究项目，旨在构建一个可以在核打击之后依然工作的通讯网络——这就要求分布式而非集中式的结构。这样，即使网络中的一片区域被彻底摧毁，网络通信还是不会中断。换句话说，鸡蛋别都放到一个框里，分开来放，就算一个框摔了其他的鸡蛋也碎不了。以下是 1970 年代 ARPANET 在美国的分布图<sup>24</sup>：



### 扯扯闲话：互联网本来应该是伏特加味的？

冷战是个神奇的时代，人类的科技在这 40 年中飞速进步。

在苏联，也有类似阿帕网的“红书计划”。B 站上的这个视频介绍并讲述了“红书计划”及其历史发展。你可以通过以下链接或者扫描二维码观看<sup>25</sup>：

<https://www.bilibili.com/video/BV1Yf4y1B7tg>



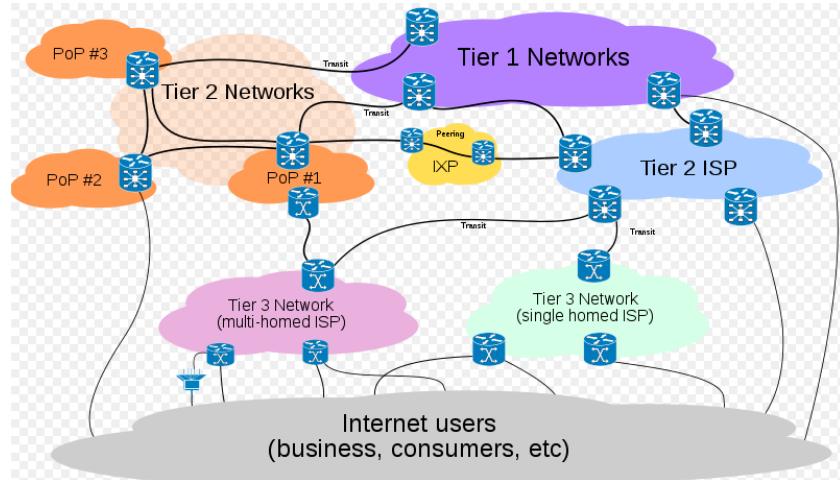
<sup>23</sup> 例如微信等软件，在发出信息的几乎瞬间对方就可以收到

<sup>24</sup> [https://en.wikipedia.org/wiki/ARPANET#/media/File:Arpanet\\_in\\_the\\_1970s.png](https://en.wikipedia.org/wiki/ARPANET#/media/File:Arpanet_in_the_1970s.png)

<sup>25</sup> 视频中提到的阿帕网的起源不同，以书为准

谁控制互联网？谁拥有它？

互联网由无数个独立的网络组成，包含各个网络中数十亿台计算机。因此，**没有任何人、机构、国家可以控制互联网，互联网属于所有人！**但是，一些政府，企业或学术机构拥有一级网络(Tier1 Network)，绝大多数的网络交通都要经过这些一级网络。如下图<sup>26</sup>，一级网络之下又可以细分为二级、三级网络，最终连接到互联网用户，也就是我们的电脑上：



## ISP

图中的 ISP 是什么意思？**ISP 是 Internet Service Provider (互联网服务供应商) 的缩写。** ISP 机构拥有，控制，并维持各种网络设施（例如海底连接两大洲之间的光缆），使互联网的连接成为可能。

## 我们都在使用互联网

日常生活中，我们通过互联网使用社交媒体(social media)，打电子游戏(play games)，观看新闻(news)，购物(shopping)，进行研究(research)等。我们还可以使用互联网进行语音通话(Voice Over IP, VOIP)<sup>27</sup>。

<sup>26</sup> 对应单元 PPT 第 4 页右侧

<sup>27</sup> 国外常用软件为 Skype，类似于国内的微信通话

# How does the Internet work? 互联网如何工作?

希望你不要忘记上一章的内容。在计算机中，一切数据以二进制的形式进行存储和处理。**互联网也是这样，所有数据都以二进制的形式进行发送和接收。**发送数据的方式有很多，有线(wired)渠道使用光纤和电缆，无线(wireless)渠道有射频(radio wave)、微波(microwave)、红外线(line-of-sight infrared)和卫星通讯(satellite communication)等……好在我们只用了解一些常见的。



## 扯扯闲话：红外线还能收发数据？

首先说明这是一项古老的技术，在现在的家用电脑上已经看不到了。我一开始得知这项技术的时候也很吃惊（更吃惊的是 Tommy 居然有两台支持这个功能的老 IBM 笔记本），但想想也合理，毕竟空调遥控器就是用红外线通信的，说明红外线可以用来传递信息。B 站上的一个视频使用夜视仪精彩的展示了这一过程，你可以扫描二维码或者输入以下链接观看：

<https://www.bilibili.com/video/BV1GG4y1M7ud>



如果你观看了视频，你会发现红外线光一闪一闪的。这就是光脉冲。你可以简单的理解为灯亮为 1，灭为 0。光传输通过这种方式以二进制的形式运输数据。

## 接发数据的方式

电力(electricity)传输：使用同轴电缆(coaxial cable)，适用于较短的距离，例如在建筑物内连接计算机实验室或办公室，适用范围非常有限。

**光(light)传输：光纤(fibre optic cable)通信。**还记得物理课上讲过的全反射吗（仅限理科班同学），其应用场景之一就是进行光纤通信。**光脉冲(light pulse)**的信号会在光纤内不断反射，传输很长的距离。光缆由多根光纤组成，能够同时传输大量数据，连接全球各大洲（它们铺设在海底），且速度达到光速<sup>28</sup>。

<sup>28</sup> 其实达不到光速，抛开光纤介质内光速降低不谈，光线在光纤中不断反射，大大增加了路程，因此整体达不到光速。但是袋鼠的书中是这样写的，以书为准

光纤传输的速度<sup>29</sup>最快，但成本较高，并且容易受到干扰或破坏。为了便于理解，你可以想象一条条飞快闪动的光线在光纤中穿梭。

无线传输：使用频率(frequency)不同的射频波代表二进制中的 0 和 1，用以接收和发送数据，适用于较小的范围（比如我们日常生活中使用的 WIFI）。



同轴电缆<sup>30</sup>



光纤<sup>31</sup>



### 扯扯闲话：宽带是什么？

宽带(broadband)（注意与下文带宽区分）指一切长期稳定的(permanent)、高速的网络连接，不管使用的是光纤，网线，还是 WIFI，甚至是卫星。日常生活中，我们能接触到的唯一不是宽带的网络连接可能就是手机热点了，因为它并不能长期稳定的存在。



### 扯扯闲话：卫星通讯

在传统的印象中，卫星通讯的速度要比其它宽带形式慢，并且还要配备用来接收和调解卫星信号的设备。但是近年来，SpaceX 旗下的 StarLink 项目逐渐引人注目。其通过部署在近地轨道的大量卫星为地面提供无死角的高速网络服务，旨在为世界上每个人提供高速的互联网服务。在写作本书时，StarLink 在轨卫星的数量约为 6000 颗，在全球超 120 个国家开通了服务（不包括中国），在南极洲实测的速度可以用于观看 8K 直播<sup>32</sup>。

<sup>29</sup> 应该为带宽最大，但是袋鼠的书上是这么写的，以书为准

<sup>30</sup> <https://www.gettyimages.com/detail/photo/connectors-royalty-free-image/147706848>

<sup>31</sup> <https://loebtxey.blob.core.windows.net/vkd1finfwb/different-types-fiber-optic-cables.html>

<sup>32</sup> <https://x.com/elonmusk/status/1874997897571561472>

## 接发数据的速度

如果你在和我打游戏，那我说网卡了有两种意思：一，我的操作太下饭了给我自己找个台阶下；二，我的网真卡了。那么为什么会网卡呢？网络传输的速度通常由以下两种因素决定：

1. 带宽(bandwidth): 理论上一定时间内可以传输的数据量。因此，一条给定路径的带宽越宽，传输速度就越大。可以将带宽想象为高速公路的宽度，规定了理论上同时可以通过的车辆数量。传输速率(data transfer rate)指的是一段时间内实际传输的数据量，也就是高速公路实际通行的车辆数量。带宽和传输速率都使用比特率 (bps)，以及其扩展单位衡量<sup>33</sup>。
2. 延迟(latency): 数据包从源设备(source device)<sup>34</sup>到请求设备(requesting device)<sup>35</sup>所需要的时间，通常用毫秒 (ms) 为单位来衡量。延迟越低，网速越快。



扯扯闲话：互联网中的信号全是以电脉冲的形式发送的？？？蛤？

在对应单元 PPT 第 14 页，袋鼠说：

Everything on the internet whether words, images, videos, emails all use ones and zeroes, being delivered by electrical pulses.

**Electrical pulses? 电脉冲? Everything? 不! BU EN<sup>36</sup>!**

光纤使用光脉冲来传递信号，是互联网的重要组成部分，负责连接各个大洲。

我以为这里袋鼠大抵想说的是互联网中的数据都是使用脉冲，也就是以二进制的形式传输罢。

<sup>33</sup> 参考第 1 章有关部分

<sup>34</sup> 发送数据的设备

<sup>35</sup> 接收数据的设备

<sup>36</sup> 化学老师 Jason 的常用词，用以表示对某个观点的强烈反对。反义词有 EN 和 BU BU EN。

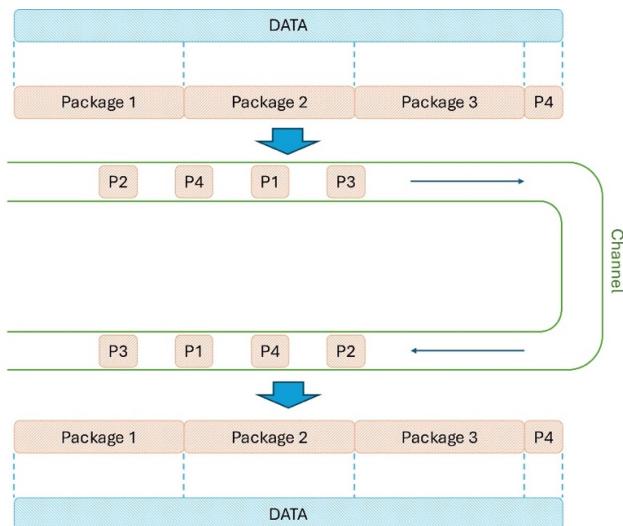
(理论上基于“双重否定表示肯定”的原理，当词语组成为  $2k \times "BU" + "EN"$ ,  $k \in \mathbb{N}$  时，表示肯定，等价为 EN；当词语组成为  $(2k + 1) \times "BU" + "EN"$ ,  $k \in \mathbb{N}$  时，表示否定，等价为 BU EN)

# Internet Working Protocols 互联网运行协议

互联网在全球范围内涉及到数十亿个设备，如果没有一个统一的运行**协议** (**protocol**)，告诉不同的计算机我们要用哪种语言交流，用什么样的格式写信，鬼知道会乱成什么样子！

## TCP - Transmission Control Protocol

TCP 的中文为传输控制协议，当然我们一般都叫它的英文名。它规定了一个信息(message)如何被拆分成多个的数据包(packet)发送出去，被接收后再重新组装起来。换句话说，通过互联网发送的信息都是按照 TCP 的标准拆分成不同数据包运输的。Tommy 为此使用 PowerPoint 制作了一张精美的示意图：



## IP - Internet Protocol

TCP 定义了怎么运输数据，那么起始点和目的地是什么？这就需要 IP 系统了。互联网上每个连接到网络的设备都有一个唯一标识符<sup>37</sup>，以便于数据的传输。这就是 IP 地址 (IP address)。IP 地址是一串由点 (.) 分隔的数字。

例如 220.181.112.244<sup>38</sup>。这是百度官网的 IP 地址之一。将它输入到浏览器中，知道了目的地，你就能访问它，显示结果如下图所示：



<sup>37</sup> 实际上，IP 地址会在不同的网络中进行动态分配，但内容较为复杂，以书为准

<sup>38</sup> 此 IP 可能由于时间问题或网络环境无法访问，仅用作演示用途

每一个按照 TCP 协议拆分成的数据包中都包含起始点和目的地的 IP 地址。如果某个数据包在传输过程中丢失，**源设备(originator)**<sup>39</sup>可以重新发送该数据包。

## IPv4 与 IPv6

220.181.112.244 就是一个 IPv4 地址。IPv4 地址由 32 位二进制数组成（此 IP 地址转换之后为 11011100.10110101.01110000.11110100，你可以数一数是不是 32 位）。IPv4 系统可以提供大约 40 亿个 IP 地址，但是这个数字在现在已经不够用了！于是人们发明了 IPv6 系统，由 128 位二进制数组成。这提供了 340 万亿亿亿（340 undecillion，即 340 后面跟着 66 个零）个地址……应该够用了吧……谁知道呢。



## Servers and Clients 服务器和客户端

日常生活中，我们经常听到“服务器”这个词，比如游戏服务器。那么什么是服务器呢？**服务器，说白了就是一台计算机，为其他互联网上的计算机提供服务。在我们打游戏的时候，我们的手机或电脑与游戏服务器进行通讯。**

**访问网站时，本质上是我们的浏览器(web browser)获取了存放在网站服务器特定文件夹中的资源文件(resource file)，并据此将页面显示出来<sup>41</sup>。**

<sup>39</sup> originator 和 source device 为同义替换

<sup>40</sup> [https://www.reddit.com/r/MrRobot/comments/78oxer/when\\_someone.asking\\_you\\_your\\_address/](https://www.reddit.com/r/MrRobot/comments/78oxer/when_someone.asking_you_your_address/)，此为图中的一部分

<sup>41</sup> 指静态网站，动态网站与此有些许不同，以书为准

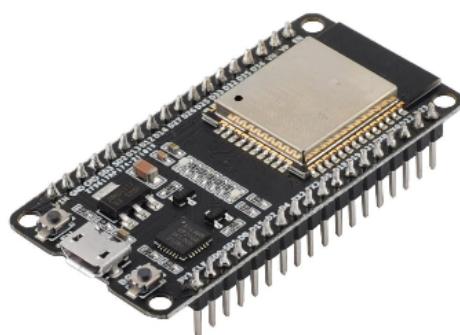


## 扯扯闲话：服务器长啥样？

小时候的我想起服务器，脑海里浮现出的是一台占据一整座房子的电脑。其实，服务器可以特别小，也可以很平常。你也许不知道，在我们机房的这个柜子里，就放着一台服务器（放在机架上面的那一个，平时应该放在机架中最底下的位置）：



以及一个没有手掌大，不到一杯奶茶价格的 esp32 开发板就可以作为一个简单的网页服务器<sup>42</sup>：



<sup>42</sup> [https://www.amazon.com/-/zh\\_TW/DIYmall-DEVKIT-ESP32-WROOM-32-ESP-32S-Arduino/dp/B084KWNMM4](https://www.amazon.com/-/zh_TW/DIYmall-DEVKIT-ESP32-WROOM-32-ESP-32S-Arduino/dp/B084KWNMM4)

客户端(client)指那些连接到服务器，以获取相应网络服务的计算机，以及运行在其中的软件，比如浏览器。



## 扯扯闲话：你使用的是什么网络浏览器？

你知道哪些网络浏览器？360？谷歌？火狐？Edge？IE？Safari？Opera？实际上这一堆名字里只有四个浏览器：Chrome（谷歌浏览器），Firefox（火狐），Safari 和 IE<sup>43</sup>。为什么这么说？因为诸如 360 浏览器等国内软件厂商“自主研发”的浏览器其实都是基于 Chrome 的<sup>44</sup>，你可以想象谷歌公开了一个蛋糕胚子的做法，360 等厂商往蛋糕胚子上抹了些奶油就做成了自己的蛋糕。

微软的 Edge 浏览器为了替代逐渐老旧的 IE 浏览器而诞生，一开始使用微软自研的 EdgeHTML5 引擎，但是非常不稳定且性能不佳。你甚至能在 B 站上看到微软员工现场演示时 Edge 浏览器崩溃，不得不下载 Chrome 的视频。随后，Edge 浏览器干脆直接投向了 Chrome 的怀抱，也开始使用 Chrome 作为其内核。

B 站的一名 UP 盘点了浏览器大战的大事年表，记录了 IE 浏览器崛起的历史，还有一期视频讲述了 IE 的没落和 Chrome 的崛起。计算机技术的发展是迅猛的，随之而来的是残酷的竞争。YouTube 上有博主甚至把浏览器娘化制作成番剧，讲述了这段历史（也算是神人了）：



IE 的起起落落



微软发布会下载 Chrome



IE 番剧



浏览器大战

链接从左到右依次为：

<https://www.bilibili.com/video/BV1D5411M7zs>

<https://www.bilibili.com/video/BV1vx411E7Mb>

<https://www.youtube.com/playlist?list=PL-RpAexxhr74x5r9wuU-aWyhIZlRLBwXt>

<https://www.bilibili.com/video/BV1u3wNeZEUM>

<sup>43</sup> 这是个墓碑，预知情节请见推荐视频

<sup>44</sup> 准确的说是基于谷歌开源的 Chromium 内核，下同

# Domain Names or URLs 域名和网址

身为一名 UNSW 预科的学生，我想要访问它的官网。于是，我搬来一本比牛津字典厚两三倍的《澳洲网站服务器 IP 地址大全》，经过查询，我知道它的网站服务器的地址是 18.154.132.52，并将其输入到了浏览器中。下回我要访问的时候，估计还要再查阅一次——这简直太蠢了。计算机擅长使用数字，而我们人类擅长使用名称。于是人们建立了域名系统(Domain Name System, DNS)，支持你使用各种各样的域名 (domain name)。

当你在浏览器中输入域名 `www.unsw.edu.au` 时，浏览器找到 DNS 服务器。

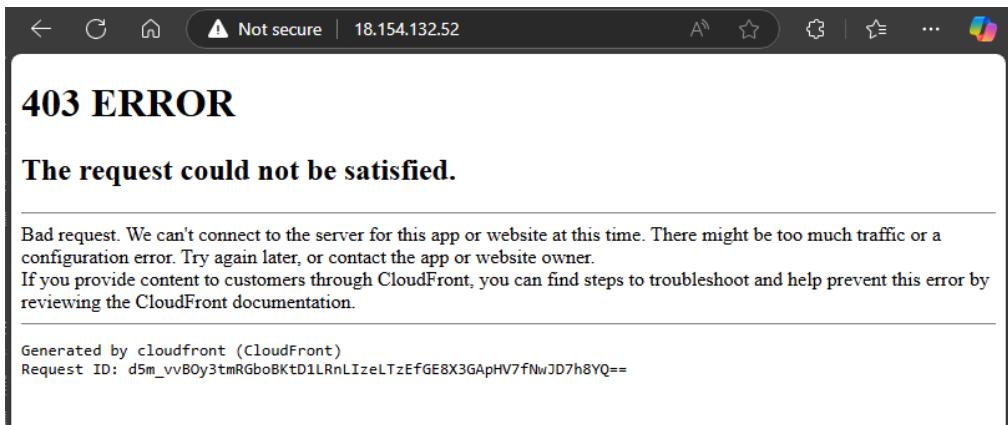
DNS 服务器查询过数据库之后告诉浏览器这个域名对应的 IP 地址是

18.154.132.52，于是浏览器去访问这个地址，最终将网页呈现出来。



## 扯扯闲话：为什么我输入 IP 地址打不开网站？

在前文中我提到了 UNSW 网站的 IP 地址，然而当你在浏览器地址栏输入时，你会发现这个界面好像出了点问题：



这并不代表这个网站服务器使用 IP 地址访问不了（怎么可能呢）。事实上，浏览器成功通过 IP 地址访问到了网站的服务器，但是出于安全等因素考虑，网站服务器决定拦截直接通过 IP 地址访问的请求。

## URL 的组成

网址, 学术点说就是 URL (Universal Resource Locator, 统一资源定位符), 是我们访问网站的常用方式, 通常由以下这几个部分组成<sup>45</sup>:



### 域名代码 (顶级域名)

域名末尾的代码称为域名代码(domain code), 常见的包括:

.com	用于商业目的
.gov	用于政府机构
.org	用于非营利组织
.edu	用于教育机构
.net	用于网络提供商

不过现在都没多少人遵守这个规则了。唯独 **.edu** 和 **.gov** 依然只能用于教育和政府目的。

除此之外每个国家还有自己的域名代码, 如:

.cn	China, 中国域名代码
.au	Australia, 澳大利亚域名代码
.br	Brazil, 巴西
.it	Italy, 意大利

## Routers and WWW 路由器与万维网

### 路由器

互联网由众多较小的网络组成, 路由器(router)在其中充当了交通枢纽的作用。路由器可以将数据包通过不同的网络进行传输, 从而起到连接不同网络的作用 (如果我坐车从家出发去学校的话, 那就是一个叫 Peter 的数据包在高速公路

<sup>45</sup> 图片截取于新南威尔士大学 Foundation 阶段配套教材对应单元第 6 页, 进行了翻译处理。

上运输，从 G25 高速转入 G42 高速，中间经过的枢纽就是路由器）。它还可以在其中负责翻译不同的网络协议，并确保网络之间的安全。

家用路由器的作用就是将家中的局域网(LAN)（连接了你的手机，电脑等设备）接入互联网。

## 万维网与 HTTP

万维网是指你能通过网络浏览器访问到的世界，即各种网页和相关服务。

当网络浏览器与服务器进行通信，获取网页时，它们遵循的通讯规则是 HTTP (Hyper Text Transfer Protocol，超文本传输协议)。客户端向服务器发送“GET (获取) ”请求获取页面，服务器返回该页面的代码。

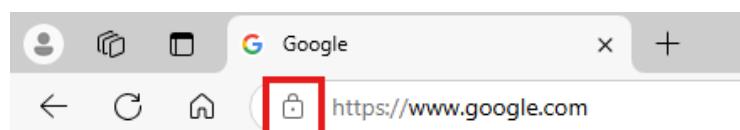


### 扯扯闲话：HTTP 状态码

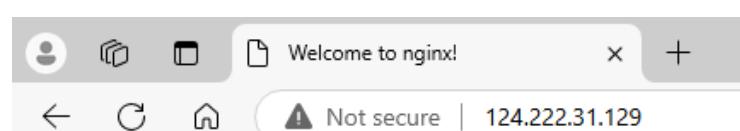
上一个扯扯闲话中我们直接使用 IP 地址访问了 UNSW 网站的服务器，得到的错误页面上写着一个大大的 403。这是什么意思呢？403 是 HTTP 状态码，表示客户端发来的 HTTP 请求被拒绝。HTTP 状态码用来表示 HTTP 请求的状态。我们日常经常听说的 404 也是一个非常经典的 HTTP 状态码，表示服务器没有找到客户端请求的资源。如果 HTTP 请求成功进行，那么 HTTP 状态码就是 200。

不知道你有没有观察过浏览器的地址栏。很多情况下，域名前面的并不是 http，而是 https。这又是怎么回事呢？https 可以理解为 http secure，安全的 http。网络浏览器通过 TLS (Transport Layer Security，传输层安全协议) 与服务器进行安全连接时会率先检查服务器的数字证书 (digital certificate)，用来验证(verify)服务器的身份，让整个过程更加安全。这就是 https。

如果一个网站使用的是 https，那么你通常可以看到一个锁的标志出现在网址的左侧，代表这个网站是安全的，如下图：



我的服务器由于没有拿到安全认证（这需要一点经费），所以就没有……





### 扯扯闲话：TCP 不是通用的协议吗？HTTP 和 TLS 是啥？

HTTP 建立在 TCP 之上。TCP 是底层协议，确保数据包都能被顺利送达。HTTP 是应用层协议，利用 TCP 来完成对网页内容的请求和传输。而 TLS 是传输层协议，规定如何传输信息。这就好比 TCP 规定了寄一封信要装在信封里，写上邮编（IP 地址）。而 HTTP 规定了信的格式，比如使用 GET 请求作为信的开头<sup>46</sup>。最终你使用一本叫 TLS 的密码本，将信的内容进行加密，并放到信封中。

## Creating Web Pages 创建网页

网页由 HTML（Hyper Text Markup Language，超文本标记语言）和 CSS（Cascading Style Sheets）层叠样式表构成。

HTML 就像房屋的设计图一样，规定了建筑的基本结构和框架。有几个门？有几个窗户？天花板有多高？而 CSS 在 HTML 所构建的毛坯房的基础上进行装饰。墙壁是什么颜色的？家具放在哪里？下图<sup>47</sup>生动展示了 HTML 和 CSS 的区别：



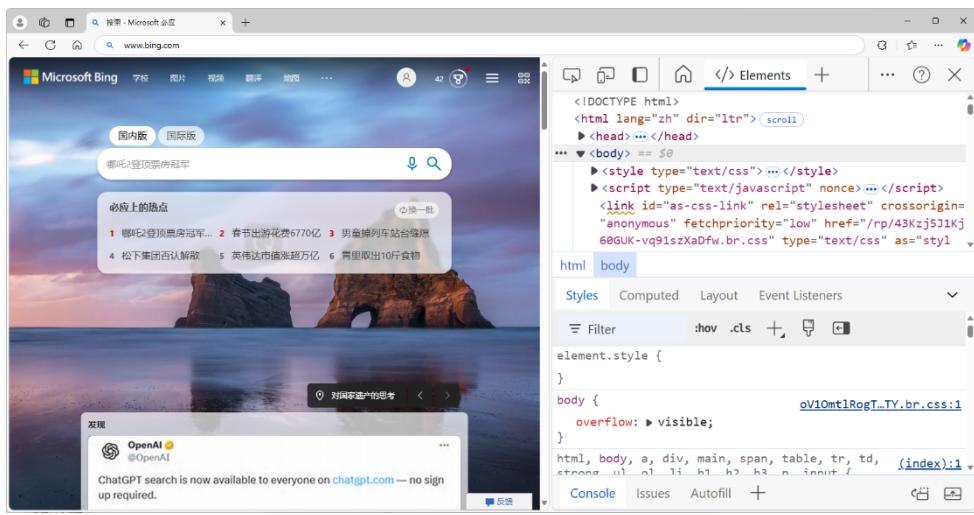
<sup>46</sup> 专业术语为 HTTP 请求头

<sup>47</sup> <https://www.pinterest.com/pin/789326272178096075>

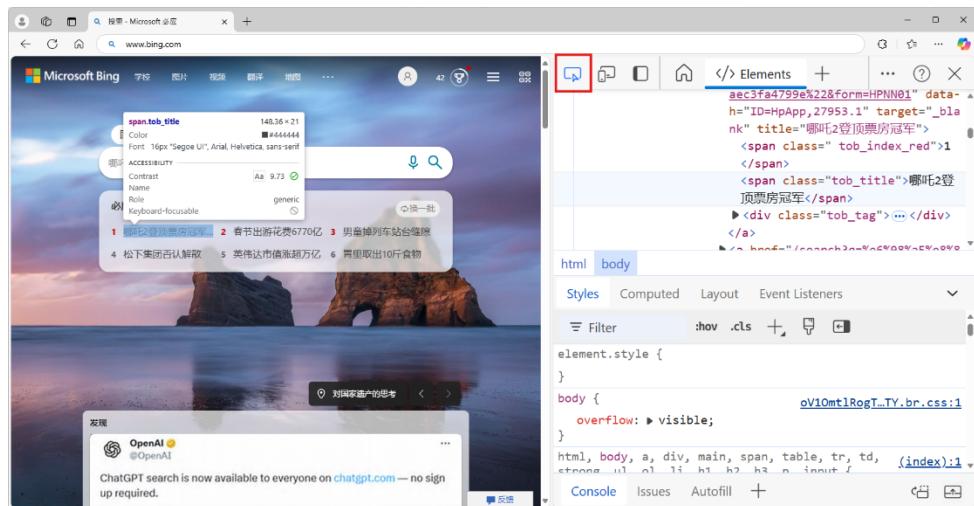


## 扯扯闲话：看看网页的真面目

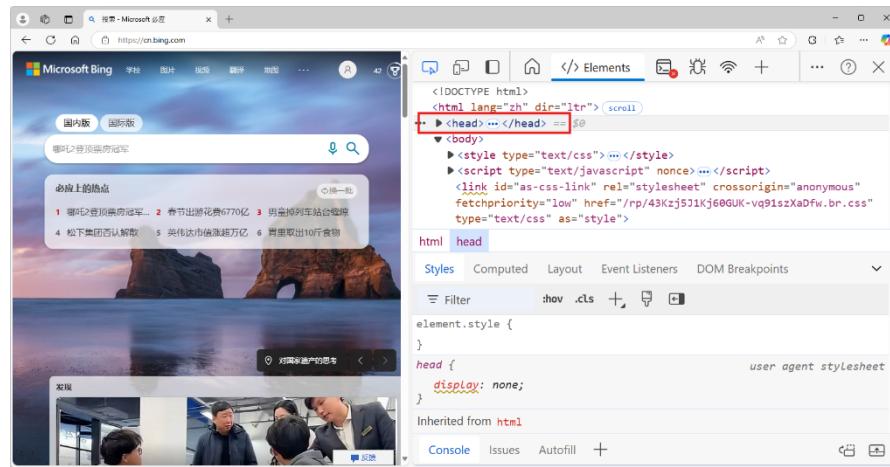
当你在目前主流的浏览器中打开一个网页时，点击 F12 键（笔记本电脑可能要同时按下 FN 键和 F12 键），便可以打开开发者窗口。在此窗口中，你可以查看关于网页的全部信息。在浏览器的地址栏中输入 [www.bing.com](http://www.bing.com)，我们可以使用必应官网做尝试。开发者窗口中的一切修改只局限在客户端中，对网站服务器中的文件不会有影响。以下我将以此进行演示：



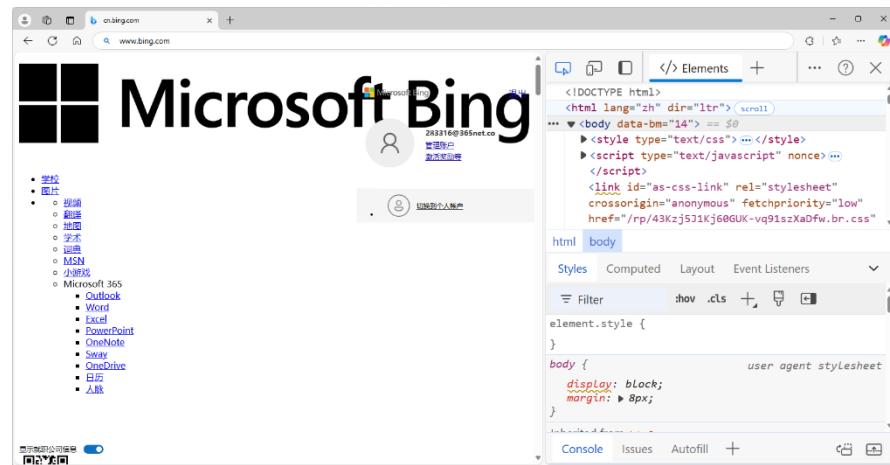
如图，打开开发者窗口，选择 Elements 选项，便可以查看网页的 HTML 代码



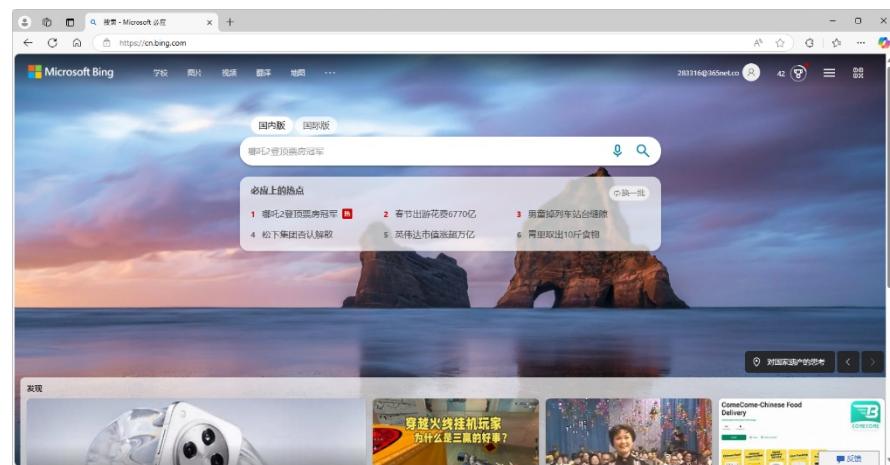
点击红框使用工具。在页面上移动鼠标，便可以看到网页各种元素对应的代码



找到红框标注的<head>一栏（这里放着 CSS 代码），选中，点击 DEL 键删除



如图所示便是网页失去 CSS 之后的样子，可见 CSS 真的必不可少啊！



点击刷新按钮，网页恢复了原状，因为浏览器又一次从服务器获取了 HTML 代码，我们刚才做的更改就没有了。

# Questions 练习

**1. When you send data through fibre optic cables, data is sent as:**

- A. Radio signal
- B. Microwave
- C. Light pulses
- D. Electrical signals

**2. What does latency mean in the prospect of the Internet?**

- A. the amount of data that transferred through the Internet
- B. the time taken for data from source to requesting device
- C. the amount of data that can be simultaneously transferred
- D. an Internet user's delay in replying to a message

**3. What is the Internet?**

- A. Physical connection between networks and computers
- B. The WWW, World Wide Web
- C. All wireless networks
- D. Wireless networks and wired networks

**4. Which two domain code are still being used properly?**

- A. .com and .org
- B. .edu and .gov
- C. .org and .net
- D. .info and .top

**5. A web browser is also called:**

- A. a server
- B. a router
- C. a channel
- D. a client

**6. TCP is a standard controlling how:**

- A. messages are broken into pieces, sent and received.
- B. data transferred in binary form.
- C. web browser communicate with servers.
- D. messages are sent by electric pulses.

**7. Which device below acts like a traffic manager on the Internet, connect each network and ensure the data goes the right way?**

- A. Router
- B. Server
- C. Fibre Optic Cable
- D. TCP/IP

**Match the following:**

① HTTP	② CSS	③ TCP/IP	④ TLS	⑤ HTML	⑥ DNS	⑦ URL
--------	-------	----------	-------	--------	-------	-------

Two main technologies to create a website: \_\_\_\_\_, \_\_\_\_\_.

\_\_\_\_\_ system search IP addresses of servers by domain names, which enables us to use \_\_\_\_\_.

\_\_\_\_\_ controlled how data being transferred through the Internet, \_\_\_\_\_ enhance its safety, while \_\_\_\_\_ is the standard that being used when web browsers communicate with servers.

**Judge each statement:**

1. Everything on the internet, whether words, images, videos, emails all use ones and zeroes, being delivered by electrical pulses. ( )
2. The Internet is controlled by no one. ( )
3. Http is safer than https. ( )
4. When you type an URL in a web browser, the browser translates it into IP address and then visits the server. ( )
5. Using fibre optic cables is the fastest way of transferring data. ( )

# Answers 答案

## **Multiple choice:**

1. C, 见第 32 页。
2. B, 见第 34 页。
3. A, 见第 30 页。
4. B, 见第 40 页。
5. D, 见第 38 页。
6. A, 见第 35 页。
7. A, 见第 40 页。

## **Matching:**

Two main technologies to create a website: ⑤, ② OR ②, ⑤, 见第 42 页。

⑥ system search IP addresses of servers by domain names, which enables us to use ⑦, 见第 39 页。

③ controlled how data being transferred through the Internet, ④ enhance its safety, while ① is the standard that being used when web browsers communicate with servers, 见第 35 页和第 41 页。

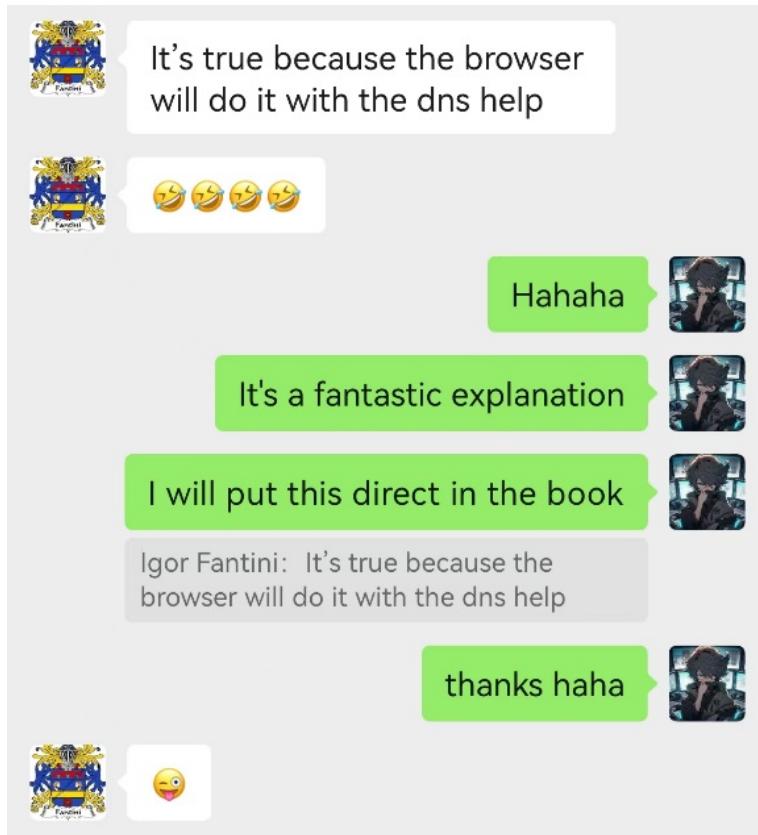
## **Judging:**

1. ×, 见第 34 页。
2. √, 见第 31 页。
3. ×, 见第 41 页。
4. √, 见第 39 页, 以及下面的扯扯闲话。
5. √, 见第 33 页。



## 扯扯闲话：不是 DNS 服务器将域名转换为 IP 地址吗？

题目说浏览器将域名转换为 IP 地址，居然是对的？为此，Igor 亲自给出了一个极好的解释（请忽略我的语法错误，这就是雅思首考 7.5 的实力）：



# Vocabularies 词汇

单词	释义	页码
<b>Internet</b>	互联网	30
<b>world wide web, WWW</b>	万维网	30
<b>physical</b>	现实中的	30
<b>email</b>	(电子)邮件	30
<b>instant messaging</b>	即时通讯	30
<b>file transfer service</b>	文件传输	30
<b>tier1 network</b>	一级网络	31
<b>Internet service provider, ISP</b>	互联网服务提供商	31
<b>social media</b>	社交媒体	31
<b>voice over IP, VOIP</b>	语音通话	31
<b>wired</b>	有线	32
<b>wireless</b>	无线	32
<b>radio wave</b>	射频	32
<b>microwave</b>	微波	32
<b>line-of-sight infrared</b>	红外线	32
<b>satellite communication</b>	卫星通讯	32
<b>electricity</b>	电力	32
<b>coaxial cable</b>	同轴电缆	32
<b>light</b>	光	32
<b>fibre optic cable</b>	光纤	32
<b>light pulse</b>	光脉冲	32
<b>frequency</b>	频率	33
<b>broadband</b>	宽带	33
<b>permanent</b>	长期稳定的	33
<b>bandwidth</b>	带宽	33
<b>data transfer rate</b>	(数据)传输速率	34
<b>latency</b>	延迟	34
<b>source device</b>	源设备	34
<b>requesting device</b>	请求设备	34
<b>protocol</b>	协议	35
<b>message</b>	信息	35
<b>packet</b>	数据包	35

<b>Internet protocol, IP</b>	IP (系统)	35
<b>IP address</b>	IP 地址	35
<b>originator</b>	源设备	36
<b>server</b>	服务器	36
<b>web browser</b>	网络浏览器	36
<b>resource file</b>	资源文件	36
<b>client</b>	客户端	38
<b>domain name system, DNS</b>	域名系统	39
<b>domain name</b>	域名	39
<b>universal resource locator, URL</b>	网址	40
<b>domain code</b>	域名代码	40
<b>router</b>	路由器	40
* <b>LAN</b>	局域网	41
<b>hyper text transfer protocol, HTTP</b>	超文本传输协议	41
* <b>GET</b>	HTTP 获取请求	41
<b>transport layer security, TLS</b>	传输层安全协议	41
<b>digital certificate</b>	数字证书	41
<b>verify</b>	验证	41
<b>hyper text markup language, HTML</b>	超文本标记语言	42
<b>cascading style sheets, CSS</b>	层叠样式表	42

# 第 3 章

## Website Evaluation

网页评估

# Internet for Research 把互联网用于学术研究

互联网上有大量的信息可供我们进行学术研究，但是：

- 我们怎么知道这个信息是准确，可信，权威的呢？
- 我们怎么确认这个信息是最新的呢？
- 我们怎么判断这种类型的信息是否可以用于学术研究？

这就是我们要在这章探讨的内容。谢天谢地，这章的内容在理解难度上较低，这对你我来说都是个好消息。

## Audience 受众

观察一个内容的受众群体是一个非常有用的评估方法，因为内容总是为受众服务的。换句话说，什么样的话说给什么样的人听嘛。《三体》中有一段精彩的描写<sup>48</sup>：

有一次，她放下书，看到大风把纳着的鞋底放到膝上，呆呆地看着灯花。发现叶文洁在看自己，大风突然问：

“姐，你说天上的星星咋的就不会掉下来呢？”

“你害怕星星掉下来吗？”叶文洁轻轻地问。

大风笑着摇摇头：“怕啥呢？它们那么小。”

叶文洁终于还是没有做出一个天体物理学家的回答，她只是说：“它们都很远很远，掉不下来的。”

大风对这回答已经很满意，又埋头做起针线活儿来。

在这段文字中，大风只是一位农家妇女，并没有受过什么教育，而叶文洁是一名天体物理学家。由于受众的原因，她的回答并不是专业的物理知识，而是一个看似错误的解释。当我们抱着学术研究的目的去网络上检索信息时，也需要注意类似的情况，确保内容的受众是为学术目的服务的。

下图<sup>49</sup>标注了一些常见的内容类型及其对应受众，学术性从左向右递减：

---

<sup>48</sup> 《三体》第一部中的内容，有删改

<sup>49</sup> 对应单元 PPT 第 5 页

Article Type	Academic Journals	Substantial News/General Interest	Popular Magazines	Newspapers
Intended audience	Researchers, students, specialists who are peers of the contributors	A general but educated and well-read audience	A general readership of non-specialists	A general audience with an interest in the news



### 扯扯闲话：Substantial News 是什么？

Substantial News（重要新闻或实质性新闻）是指具有重要性和影响力的新闻内容，通常涉及对公众、行业或特定领域产生重大影响的事件、政策变化、重大发现或进展。这类新闻的特点是信息量大、内容意义深远，且对受众具有较高的关注价值。<sup>50</sup>



### 扯扯闲话：General interest 是什么？

General interest（广泛兴趣）指的是大众感兴趣的主題或內容。这类內容通常涉及日常生活中普遍关注的话题，包括文化、娱乐、健康、科学、旅行、美食、历史等。与专业或特定领域的兴趣相比，广泛兴趣的内容更加普及，满足人们对知识、娱乐和信息的需求。

此外，观察一个网站的设计也可以鉴别一个网站是否专业。比如，对比一个充满着广告，杂乱不堪的网站，我更倾向于相信一个排版工整，页面整洁的网站。此外，我们还可以通过网站的字体和颜色设计判断其是否为学术网站。

<sup>50</sup> 本段由 Tommy 提供

# Authority 权威性

为什么身边有些人的发言总是让我们听着觉得非常扯，而有些人能让我们信服。请你对比一下以下三个发言：

“根据德国著名心理学家赫尔曼·艾宾浩斯在 1885 年提出的“记忆遗忘曲线”理论，学习是一个持续的过程，我们要在不断地积累新知识的同时注重复习。”

“书山有路勤为径，学海无涯苦作舟。我们要不断努力学习，积累知识。”

“来，你吃一个馒头吃不饱，两个馒头吃不饱，吃了三个馒头饱了。是第三个馒头让你饱的吗？所以说学习就要持续努力。”

第一个发言引用了一个具体的研究结果，并且说明了对应的研究者，让听众有迹可循，是一个接受过正经文化教育并且脑子正常的人在正式场合发言的基本要求。第二个发言借用了古诗，虽说不那么严谨，但是毕竟是古人的智慧，也能凑合。第三种发言虚构了一个场景，用了一个不符合实际的类比，强行说明了一个道理，所以让人难以信服和接受。如果一个老师能大言不惭的说出这种话，那我不得不怀疑他大学甚至高中学历的真实性，以及他的脑子是否还能够正常运转。对于这种人，我不认为他是我的老师。并且我也建议在日常生活中少跟这种人接触，更是不要和他争论他的观点。因为他缺乏基础的逻辑训练，连出发点都是错误的，讨论的整个场景都是他虚构出来的，你不仅无法在他构建的不切实际的世界中与这个蠢笨的上帝争论，还会浪费自己的时间。

在学术研究中的要求比以上发言的场景更加苛刻。你引用的文章必须包含以下内容：

1. 作者(author)，应是相关领域公认(recognized)的专家
2. 作者所属的机构(affiliation)，应是相关领域认可(recognized)的专业协会或研究机构
3. 通讯作者(correspondence)，对这篇文章的研究结果负责

下图<sup>51</sup>提供了一个很好的例子：

---

<sup>51</sup> 对应单元 PPT 第 6 页



The screenshot shows the homepage of the IOS Press Content Library. The top navigation bar includes the IOS Press logo and links for 'Home' and 'Journals'. Below the navigation is a search bar with a magnifying glass icon and the word 'Search'. Underneath the search bar is a date range selector labeled 'Published between:' with input fields for 'YYYY' and 'and' followed by another 'YYYY' field. The main content area features a research article summary. The article title is 'A group decision making framework based on neutrosophic VIKOR approach for e-government website evaluation'. The 'Article type' is listed as 'Research Article'. The 'Authors' are 'Abdel-Basset, Mohamed<sup>a,\*</sup> | Zhou, Yongquan<sup>b</sup> | Mohamed, Mai<sup>a</sup> | Chang, Victor<sup>c</sup>'. The 'Affiliations' are 'a] Department of Operations Research, Faculty of Computers and Informatics, Zagazig University, Zagazig, Sharqiyah, Egypt | b] College of Information Science and Engineering, Guangxi University for Nationalities, Nanning, China | c] International Business School Suzhou, Xi'an Jiaotong-Liverpool University, China'. The 'Correspondence' information includes the address 'Mohamed Abdel-Basset, Department of Operations Research, Faculty of Computers and Informatics, Zagazig University, Zagazig, Sharqiyah, Egypt', telephone number '+20 11 2228 8843', and email 'analyst\_mohamed@yahoo.com'. The 'Abstract' is: 'Since the emergence of digital revolution, many governments have sought to use the internet for the benefits of communication and information easiness to present public services. Due to citizen's consciousness of internet, the online public services have increased rapidly. Allowing citizens'.



### 扯扯闲话：什么是通讯作者？

通讯作者是在学术论文中负责与编辑部、审稿人以及读者进行联系的人。其主要职责包括提交论文、回答审稿意见、协调修订，以及负责后续的学术交流。通讯作者通常是项目的负责人或导师，但也可以是主要参与研究的其他成员。<sup>52</sup>

## Accuracy 准确性

学术文章应当没有语法和拼写错误(free of grammatical and spelling errors)，并且应按专业学术文章的结构进行组织。例如，大多数研究文献包含摘要(abstract)、文献综述(literature review)、方法论(methodology)、结果(results of findings)、结论(conclusion)和参考文献(references)。此外，还可以通过检查一个文章中是否包含专业术语(terminology)来判断一个文章的学术性。

<sup>52</sup> 本段由 Tommy 提供

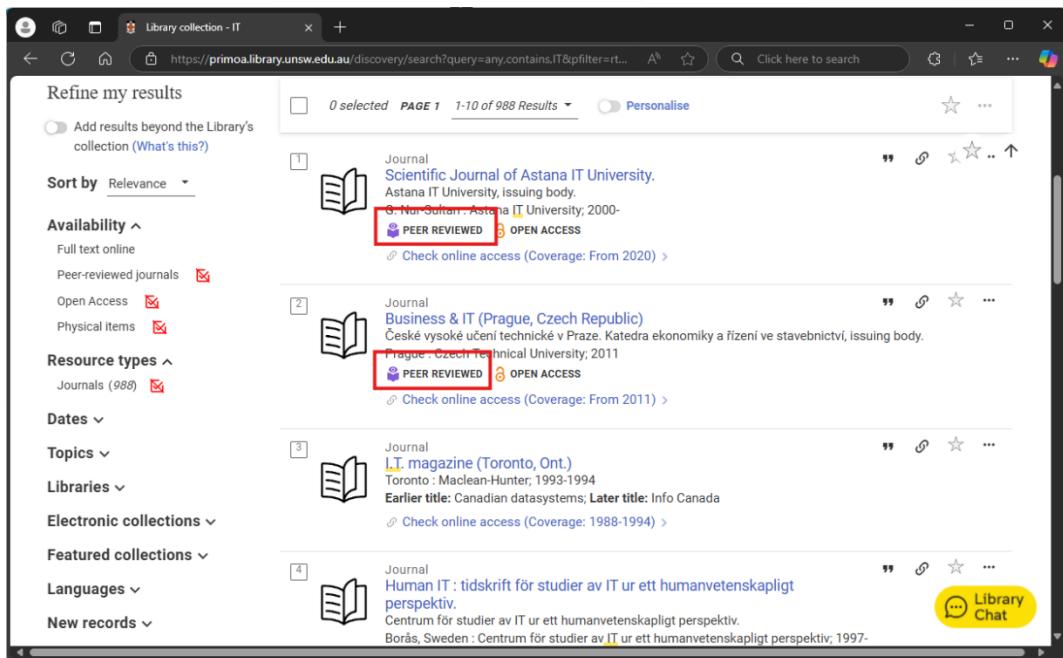
# Peer Review 同行审查

同行评审是一个将作者的学术工作提交给同领域其他专家审查的过程，目的是确保文章的质量。大多数情况下，审稿人并不知道文章的作者是谁，这很好的防止了作者声誉对审查结果产生的影响。因此，经过同行审查的文章最适合用于学术研究。

如何判断文章是否被同行审查过？

在 **Ulrichsweb.com** 网站上查找文章时，如果文章经过同行审查，那么他的旁边应该带有  <sup>53</sup> 标志。除此之外，**Google Scholar**（谷歌学术）等网站也提供了搜索同行审查文章的功能。

当你在 UNSW 的图书馆中搜索时，网站也会给同行审查的文章添加标识：



The screenshot shows a library search interface for 'library collection - IT'. The results page displays 1-10 of 988 results. Three journal entries are listed:

- Scientific Journal of Astana IT University.** Issuing body: Astana IT University, 2000. **PEER REVIEWED** **OPEN ACCESS**
- Business & IT (Prague, Czech Republic)** Issuing body: České vysoké učení technické v Praze. Katedra ekonomiky a řízení ve stavebnictví, issuing body. Prague, Czech Technical University, 2011. **PEER REVIEWED** **OPEN ACCESS**
- I.T. magazine (Toronto, Ont.)** Issuing body: Maclean-Hunter, 1993-1994. Earlier title: Canadian datateams; Later title: Info Canada. **PEER REVIEWED** **OPEN ACCESS**

Each journal entry includes a 'Check online access (Coverage: From 2020)' or 'Check online access (Coverage: From 2011)' link. A 'Library Chat' button is visible in the bottom right corner of the interface.

# Objectivity 客观性

内容的客观性取决于作者无偏见议论(unbiased argument)的能力。无偏见的呈现一个问题要求作者能够从问题的不同方面进行讨论，而不会受到个人因素影响。如果作者在文章中表达了自己的个人意见，需要将其明确标识出来。

<sup>53</sup> Igor 说这是一个 T-shirt

评估一个网站的重要部分是确定这个网站的动机(motive)——尤其是对于商业网站。它们可能会列举一些看似科学的结论，但实际上是为了商业宣传。

政府网站通常应被视为可信，因为它们发布的信息来自特定领域的专家。然而，要注意的是，政府可能有特定的议程，试图通过呈现某一特定观点来影响公众舆论。尽管这些信息可能是学术的和准确的，但他们可能会隐瞒其他信息或观点，这对于公众做出准确和明智的决策至关重要。(我直接机翻的和我没关系哈)

## Currency 时效性

对于某些内容来说，时效性非常重要。比如有关科技(technology)内容的网站，如果网站上的内容来自于 5 年前，那它们可能已经完全过时<sup>54</sup>了。



### 扯扯闲话：IT 的发展有多快？

我在小学五年级时接触过 Android 应用开发（就是写 Android 系统上用的软件）。当时用的技术主要还是 Java<sup>55</sup>，甚至还有 C++。上初中时再去看，Kotlin 已经逐渐替代 Java 成为主流。到了初三毕业，Kotlin 又有非常多的变化，我按照初一的写法写出的代码很多都过时了。

对于某些领域（如地质或历史），5 年前的内容大概率不会过时。前提是网站一直要有人维护（保证其正常运行），网站内容中包含的链接所对应的网站也仍然可以访问，且该主题没有更新的研究成果。

## URL 网址

我们可以通过网址判断一个网站的内容是否能用于学术场景。例如，通常带有 .gov 或 .edu 后缀<sup>56</sup>的网站包含有效的信息。

<sup>54</sup> 原文为 *inaccurate and irrelevant*，此处简化翻译

<sup>55</sup> 编程语言的名称，下同，不必在意

<sup>56</sup> 学名为域名代码，参考第 2 章有关部分

然而，仍然需要谨慎，因为政府在制定特定议程时，可能只会呈现问题的单一  
方面，而选择不揭示所有方面，以免影响公众舆论，尤其是在政府认为会对其  
计划产生负面影响的情况下。因此，虽然这些网站通常可靠，但在使用其信息  
时，仍需保持批判性思维，尽量寻找其他来源以获得更全面的视角。（这还是机  
翻的和我没关系哈）

## DOI

数字对象标识符（Digital Object Identifier System, DOI）是一种在“数字网络上  
识别知识产权的方法”<sup>57</sup>。与传统的 URL 不同，当相关内容存放位置移动时，  
URL 就必须更改，否则就会失效。而 DOI 则是针对对象(object)本身的标识，不  
会随对象位置的变动而改变，因此始终保持有效（即使资源文件的 URL 变动，  
DOI 也不会变动，并且仍然能正确指向新的 URL）。

要为一个网站获取 DOI，需要向 DOI 注册机构(DOI Registration Agency)申请，  
并支付一次性费用(one-off cost)。目前有多个注册机构，例如 Airiti、Crossref  
和中国知网（CNKI）等。

使用 DOI 可以方便地引用和查找学术资源，确保研究人员能够始终访问所需  
的信息，因此其在学术领域被广泛采用。

## Reliability 可靠性

要将一个网站作为学术资源使用，那么这个网站的内容必须有可靠的来源。

## WIKI

WIKI 是由互联网上任何愿意做贡献的人撰写的百科知识，国内常见的百度百科  
就是 WIKI 的一种。由于可能存在的假信息(misinformation)，WIKI 上的内容不  
能被用于学术目的。正如维基百科自己所说，“我们不指望你的信任”<sup>58</sup>：



<sup>57</sup> 翻译自：[http://www.doi.org/10DEC99\\_presentation/faq.html#1.1](http://www.doi.org/10DEC99_presentation/faq.html#1.1)

<sup>58</sup> [https://en.wikipedia.org/wiki/Wikipedia:Ten\\_things\\_you\\_may\\_not\\_know\\_about\\_Wikipedia](https://en.wikipedia.org/wiki/Wikipedia:Ten_things_you_may_not_know_about_Wikipedia)



## 扯扯闲话：这真的很重要！

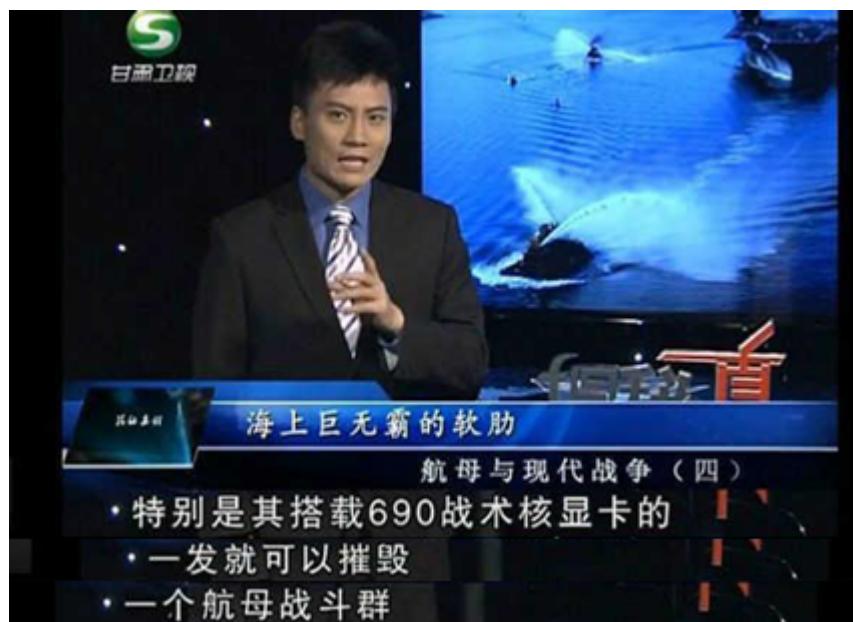
早先的 GTX690 显卡出现过电容爆炸的现象，因此被发烧友们戏称为战术核显卡。有网友去恶搞了百度百科（远古时期的事了，图不可避免的包浆）：

排行榜

### 火箭推进榴弹

许多第三世界国家甚至西方国家的军队或者反政府武装都广泛使用。反坦克有一定的实力，甚至被用于攻击低空目标。因此用其攻击航母亦是可行方案。由十万发火箭推进榴弹对航母进行的饱和攻击即可击沉任何艘航母，且对其无有效拦截手段。特别是其搭载690战术核显卡的改进型号，一发即可摧毁一个航母战斗群。

显而易见的是，甘肃卫视的编辑缺乏这方面的学术知识，不知道不能使用 WIKI 中的内容作为资料参考，于是发生了令人哭笑不得的名场面：



(这主持人是被纯恶搞了)

但是，WIKI 并不是没有任何学术价值。许多 WIKI 的参考资料中都标明了相关的学术资料，以及同行审查的论文，可以作为一个很好的起点。

在各类 WIKI 网站中最著名的当属 Wikipedia，其余的有 Investopedia, Astro-Databank，以及中国的百度百科。

## 博客

博客(Blog)可以由任何人创建（我从小学到现在自己搭建了三个博客网站，但毫无意外的都没有坚持写下去），包含个人的观点，新闻，视频，和图片资料。博客中的内容通常只针对于特定的群体和个人兴趣。博客不能作为学术资料使用。

# Questions 练习

**1. Which of the following is the academic structure of an article:**

- A. Introduction, Body paragraph, Conclusion
- B. Title, Heading, Text
- C. Cover page, Table of Contents, Contents
- D. Abstract, Literature review, Methodology, Results of findings, Conclusion, Reference

**2. Which of the following tells you that the article has been peer reviewed?**

- A. The website contains little advertisement
- B. The website is well-designed
- C. It has a peer-reviewed symbol next to the title of the article
- D. The URL of the website ends with .edu

**3. Evaluate an article by verifying its author(s). What is it called?**

- A. Accuracy
- B. Authority
- C. Currency
- D. Objectivity

**4. Peer reviewed article is:**

- A. an article that undergoes a formal review by several experts
- B. an article that edited by government departments
- C. an article that written and reviewed by a famous expert
- D. an article that has been discussed with author's friends

**5. Which article is the best to be used in academic research?**

- A. An article written by famous experts from recognized institutions
- B. An article written by professional students
- C. An article that is peer-reviewed
- D. An article that is written by your teacher

**6. Which of the following is the biggest problem for WIKIs?**

- A. Grammatical error
- B. Misinformation
- C. Illegal information
- D. Sensitive topic

**7. Who would be the most suitable audience for a scholarly journal article?**

- A. The author
- B. A General, well-educated readership
- C. A specialist in the field who want to acquire more knowledge
- D. A General readership that is interested in news and hot topics

**8. When doing academic writing, can WIKIs be considered as a helpful resource?**

- A. Yes, but only used as a starting point for further research and reference.
- B. No, because there is plenty of misinformation on WIKIs.
- C. Yes, WIKIs are written by famous scholars from recognized institutions.
- D. No, because the information on WIKIs may out-of-date.

**9. Which of the following will most inform you of the website's accuracy?**

- A. The author is recognized and from a famous university.
- B. The content is free of spelling errors, and is well-written in academic structure.
- C. The website is well-designed for academic purpose.
- D. The author is a successful businessman that own his own company.

**10. Which URL is recommended to be used in academic research?**

- A. <https://www.environment.nsw.gov.au/beachmapp/Beaches/SydneyOceanBeaches>
- B. <https://www.smh.com.au/environment/state-of-the-beaches-20162017-report.html>
- C. <https://www.ellaslist.com.au/articles/is-this-the-most-polluted-beach-in-sydney>
- D. [https://en.wikipedis.org/wiki/Bondi\\_Beach](https://en.wikipedis.org/wiki/Bondi_Beach)

**Extra:**

Engineering students are writing a research paper on applications of the latest technologies in engineering. They have found the following article in Google Scholar.

**Title:** Compression Testing of Concrete: Latest Technology

**Author(s):** R. G. Burg; M. A. Calderone; G. Detwiler, D. C. Jansen; and T. J. Willem

**Publication:** Concrete International

**Volume:** 21 **Issue:** 8 **Date:** 8/1/1999

**Abstract:** Concrete is now available commercially having a compressive strength approaching 20,000 psi (138 MPa). Researchers predict that even higher strengths can eventually be achieved without the use of exotic materials, special processing under high temperatures, or special atmospheres and high casting pressures.

Would you recommend they use this article in this research paper? Why?

---

# Answers 答案

## Multiple choice:

1. D, 见第 55 页。

2. C, 见第 56 页, peer-reviewed symbol 指 。

3. B, 见第 54 页。

4. A, 见第 56 页。

5. C, 见第 56 页。

6. B, 见第 58 页。

7. C, 见第 53 页。

8. A, 见第 59 页。

9. B, 见第 55 页。

10. A, 见第 57 页, 基本上只要域名末尾含有 gov 就可以视为政府网站。

## Extra:

One possible version: No, because the article is out-of-date.

见第 57 页, 学生们要研究最新的科技, 但是这篇论文是 1999 年写的。

# Vocabularies 词汇

单词	释义	页码
<b>audience</b>	受众	52
<b>authority</b>	权威性	54
<b>author</b>	作者	54
<b>recognized</b>	公认的, 认可的	54
<b>affiliation</b>	所属机构	54
<b>correspondence</b>	通讯作者	54
<b>accuracy</b>	准确性	55
<b>peer review</b>	同行审查	56
<b>objectivity</b>	客观性	56
<b>unbiased argument</b>	无偏见议论	56
<b>motive</b>	动机	57
<b>currency</b>	时效性	57
<b>technology</b>	科技	57
<b>digital object identifier system, DOI</b>	数字对象标识符	58
<b>object</b>	对象	58
<b>DOI registration agency</b>	DOI 注册机构	58
<b>one-off cost</b>	一次性费用	58
<b>reliability</b>	可靠性	58
<b>misinformation</b>	假信息	58
<b>blog</b>	博客	59

# 第 4 章

## Security and Privacy

安全和隐私

# Cybersecurity and Crime 网络安全与犯罪

随着互联网的发展，网络犯罪(cyber crime)对社会的影响越来越大。根据《福布斯》杂志的数据，在 2019 年，有 25% 的恶意软件(malware)针对金融行业，信用卡诈骗的数量上升了 200%。<sup>59</sup>



## 扯扯闲话：Kangaroo did a really bad job!

袋鼠在书中写：

according to Forbes magazine, Apr 29, 2019, '2.5% of all malware targets financial services, and credit card fraud is up 200%'

看到这段的时候我就在想，2.5%也不是一个很惊人的数字啊，比我想的少多了。于是一搜原文……袋鼠果然错了。原文的链接在脚注，标题是：

### **Cybercrime: 25% Of All Malware Targets Financial Services, Credit Card Fraud Up 200%**

简直天差地别……我们还是要辩证性的看待袋鼠的这本书。

在袋鼠国，针对个人的身份盗窃犯罪使每年有一百万人受害<sup>60</sup>。在国家层面，如果一个国家的网络基础设施遭到破坏（如卫星信号被劫持(hijack)），那么这个国家的安全就毫无疑问的会受到威胁。

## 什么是网络安全

黑客等不法分子的最终目标是非法从计算机系统中获得可读的(readable)明文（即没有加密过的文字）信息(plaintext)，并以此牟利。网络安全(cyber security)旨在对抗这一行为，保护计算机系统及其中的数据不会被未经授权的访问(unauthorised access)。

## 什么是网络隐私

网络隐私(cyber privacy)管理是网络安全的重要部分，并与我们每个人的日常生活息息相关。使用手机上的应用程序时，它需要我们的哪些数据？这些数据会被如何使用？是否会共享给相应的科技公司？如何确保它们不会在没有我授权

<sup>59</sup> <https://www.forbes.com/sites/zakdoffman/2019/04/29/new-cyber-report-25-of-all-malware-hits-financial-services-card-fraud-up-200/>

<sup>60</sup> 数据来源于新南威尔士大学 Foundation 阶段配套教材，未验证

的情况下滥用(abuse)数据？甚至是共享给其它组织？这些都是网络隐私需要研究和考虑的内容。



### 0day 漏洞

0day 漏洞(zero-day vulnerability)指非常严重的计算机系统漏洞——以至于厂商有 0 天时间来修复它们。在一个 0day 漏洞被曝光之后，攻击者会立刻利用这个 0day 漏洞攻击计算机系统，而厂商也会立刻开始制作安全补丁进行防御。这也导致一个 0day 漏洞的讯息非常值钱，如果有能力的话你可以去试试。

B 站上的一个视频从技术层面介绍了苹果芯片存在的 0day 漏洞：

<https://www.bilibili.com/video/BV1ua4y1z7MH>



# Cybercrime in everyday life 日常生活中的网络犯罪

在各种影视剧中，网络犯罪通常是一伙超高智商的黑客对一个大型企业甚至是国家发起有预谋的攻击。可实际上，网络犯罪的定义非常广泛。在阅读了下文之后，你会发现我们几乎每天都在经历网络犯罪。

## 广告软件

广告软件(adware)恐怕是日常生活中最常见的一种。电脑中的有些软件会附带弹窗，通常十分烦人。

## 恶意广告

如果光是弹出一个广告弹窗，那顶多是烦人。恶意广告(maladvertising)就要严重的多。恶意广告指通过不正确或者有误导性的广告内容诱导用户安装其他恶意软件的行为。比如，你的电脑上安装了某“安全卫士”软件。它不断提示你的电脑有重大安全隐患，需要立刻修复。对计算机了解不多的你很快被蒙骗，选择了修复，随即获得了包括某安全浏览器和某壁纸软件在内的流氓软件大礼包。



### 扯扯闲话：360 是病毒还是防病毒软件？

看了上文的描述，我的第一反应是：这不就是360吗。杀毒软件固然重要，但是我不建议你主动往自己的电脑里安装360病毒。

B 站上的一个视频很好的介绍了国内杀毒软件的发展历史：

<https://www.bilibili.com/video/BV1iQ4y1e7rm>



## 恶意邮件

恶意邮件(malspam)指网络犯罪人员通过邮件发送各种信息，以诱导用户达到其非法目的的过程。这个过程也被称作网络钓鱼(phishing)。这些信息的编写会用到社会工程学(social engineering)知识，通常的目的是套取你的信息或引诱你下载恶意软件。

我曾经就收到过一个恶意邮件，请求我为一个游戏竞赛中的一支中国队伍投票，并承诺在投票后会赠送一些便宜的游戏物品。在我打开邮件中的链接之后，投票网站要求必须先登录 Steam<sup>61</sup>账号才能进行投票。这看似正常，但其实那个登录界面并不来自 Steam 官方，是伪造的。如果将账号密码输入进去，我的账号就会被盗取，后果不堪设想。



### 扯扯闲话：什么是社会工程学？

社会工程学是指在信息安全方面操纵人的心理，使其采取行动或泄露机密信息。<sup>62</sup>

广义来说，所有与人打交道获取对方信息的方式都可以叫做社会工程学。所以如果你很擅长套出别人的八卦，请叫自己社会工程学家。有一个段子是公司每天 17 点准时断网，技术人员怎么也查不清楚，最后发现是有人收买了保洁，每天准时拔网线。这就是使用社会工程学的手段进行物理上的黑客攻击。

如果用社会工程学的角度对我遇到的案例进行分析，整个邮件充满诱导性和欺骗性。在邮件中提及的“游戏赛事”激起了身为玩家的好奇心，且“为中国队伍投票”也能一定程度上的激发所谓的爱国情怀，“附赠一些便宜的游戏物品”利用了人的贪婪心理，也让请求变得合情合理。学术一点讲，这属于社会工程学中的奖励诱骗(baiting) 策略。同时，邮件的欺骗性在于其设计很像一个正式的官方邮件，并且其中的网站也看上去非常正规。强制登录再投票等环节也与正常投票流程相同，可以很好的降低玩家的怀疑。这属于社会工程学中的伪造(pretexting) 手段，即通过构造一个可信场景让受害者落入陷阱。最后，你问我为啥没被骗？很简单，我太懒了，加上我根本记不住我的 Steam 账号，于是就没有登录。这就是傻人有傻福吧……

## 间谍软件

这个名字听上去好像都和国家安全相关了。但其实间谍软件(spyware)也可以在我们的日常生活之中。比如一些企业和组织可能会在其员工的电脑中安装相应软件，用以监视员工对电脑的使用。因此，间谍软件有时不被认为是恶意软件。<sup>63</sup>

<sup>61</sup> 一个游戏平台

<sup>62</sup><https://zh.wikipedia.org/wiki/%E7%A4%BE%E4%BC%9A%E5%B7%A5%E7%A8%8B%E5%AD%A6>

<sup>63</sup> 新南威尔士大学 Foundation 阶段配套教材中观点

## 勒索软件

勒索软件(ransomware)会阻止用户访问电脑中的数据，直到用户向犯罪分子支付赎金。勒索软件离我们的日常生活较远，通常只针对于企业或组织。近期较为有名的勒索病毒是爆发在 2017 年 WannaCry，几乎对全球都产生了影响<sup>64</sup>：



### 扯扯闲话：用词根词缀记住这些单词

我承认这单元确实有很多单词，但是它们都是随着网络的发展逐渐被人们造出来的。因此，从词根词缀的角度来说，简直太公整了。

首先是前缀 **mal-**。它源自拉丁语，如意大利语中<sup>65</sup>的 *male* 一词，意指坏的，恶意的。高一上学期王华老师让我们背的写作词汇中有一词叫 *maltreatment*，用的也是这个词根，意为体罚——不好的对待。本章中出现过的词有 *malware* (恶意软件)，*malicious* (恶意的)，*malspam* (恶意邮件)，*maladvertising* (恶意广告)。

之后是后缀 **-ware**，这个出现过很多次。有 *hardware* (硬件)，*software* (软件)，*malware* (恶意软件)，*adware* (广告软件，这里的 *ad* 是 *advertising* 的缩写) 等。你可以简单的将它理解成“件”。准确来说，**-ware** 来自日耳曼语系，在德语中指商品，在英语中保留有器具的意思。

其次还有一个很有意思的词：*phishing*。源于 *fishing*，钓鱼。由于各种奇妙的历史因素，现代英语中的 *ph* 也发 /f/ 的音。网络钓鱼一般发生在哪呢？手机上。于是造词的人直接把 *phone* 中的 *ph* 拆下来组合了一下。

<sup>64</sup> [https://en.wikipedia.org/wiki/WannaCry\\_ransomware\\_attack](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack)

<sup>65</sup> 由于鄙人不会拉丁语，网上查到的各种结果也因为变位问题各不相同，因此此处使用意大利语代替

# Virus 病毒

病毒(virus)是一种恶意软件, 由一些恶意的(malicious)程序(program)或代码(code)组成, 通常被用户在不经意间安装, 并自主在不同的计算机之间传播, 以达到损害用户利益和入侵计算机系统的目的 (这就是它名字的来源)。身在一个互联的世界中, 我们的计算机很容易感染(contract)病毒。邮件附件(attachment), 网络上下载的文件, 社交媒体中的诈骗链接(scam link), 以及手机中下载的可疑的(shady)小软件 (原文就是这么写的, 不是我想加点啥) 都有可能成为病毒的来源。除了之前介绍的恶意软件之外, 病毒还有以下两种经典种类。

## 木马病毒

木马病毒(trojans)是十分常见和有名的一种病毒种类。它的名字来源于希腊军队攻打特洛伊人的那场著名战役: <sup>66</sup>



《行进中的木马》, Domenico Tiepolo (1773)

就像希腊神话中描写的那样, 木马病毒会伪装成合法的(legitimate)程序, 让用户毫无防备的运行。很多人喜欢将“木马”一词与“病毒”一词混用, 但实际上它们并不相同。很简单的一点, 病毒可以自行传播, 但是木马不行, 需要特洛伊人(用户)将它们当作战利品(正常软件)拖到城中(运行), 其中的希腊军队才能攻击城池(电脑)。如果你的电脑在很长的一段时间内突然变的比以前卡了, 特别是网速慢了很多, 那你的电脑可能是中了DDoS木马。简单来说, 你的电脑被人变成水军上战场去了。

<sup>66</sup><https://zh.wikipedia.org/wiki/%E7%89%B9%E6%B4%9B%E4%BC%8A%E6%9C%A8%E9%A6%AC>



## 扯扯闲话：什么是 DDoS 攻击

拒绝服务攻击(DoS, Denial-of-Service attack)是一种常见的网络攻击方式。通常，对于非法的访问，网站的服务器会予以拦截。但是当非法访问过多时，网站服务器就会应付不过来，网站便会崩溃。我们从小就知道不要给陌生人开门，但是如果陌生人连续敲了数千亿次门，那房子早就被敲塌了。

DDoS(Distributed Denial-of-Service attack)在单词前面加了一个 Distributed，代表分布式拒绝服务攻击。黑客可能会通过木马病毒控制很多电脑，让他们同时对某服务器发动 DoS 攻击，从而利用数量优势将服务器快速击垮。

## 蠕虫病毒

木马病毒虽然是恶意软件，但是至少听上去能让人想起发生在特洛伊的伟大战役了。而蠕虫病毒(worms)则不同，听上去就很恶心，实际也确实如此。蠕虫病毒会不断的复制它本身，直到将电脑中的运行内存和磁盘空间全部沾满为止。它们还会在网络中传播，顺路搞垮各个计算机系统<sup>67</sup>：



<sup>67</sup> <https://baike.baidu.com/item/%E8%A0%95%E8%99%AB%E7%97%85%E6%AF%92/4094075>



### 扯扯闲话：拼多多拼齐了系统中的漏洞，多多窃取用户信息

不知道你在使用拼多多的时候有没有注意到什么诡异的事情。我在很早之前就逐渐察觉到不对劲。直到有一天，我在客厅提及了一本叫《编码》的书，然后打开了拼多多，一看主页，不是根据我之前的购买记录给我推荐各种国内便宜实惠的开发板，而是满屏的——《编码》。

过了几周，国内的独立网络安全机构深蓝洞察公布了拼多多如何利用手机系统中的 0day 漏洞编写恶意代码，从而实现防止自己被用户卸载（假卸载，你以为卸载了实际没有），和各种提权操作（如未经允许使用摄像头或麦克风）的具体技术细节。[https://github.com/davinci1010/pinduoduo\\_backdoor](https://github.com/davinci1010/pinduoduo_backdoor) 中包含了对本次事件的基础报道，<https://github.com/davinci01010> 指向的用户主页发布了相关的代码以及各种证据。（网站在国内可能访问不上）

事件发生之后，Google 立刻在其应用商店对拼多多进行了下架，是一副吃了败仗落荒而逃的狼狈景象。而我们辩证性的看待了这个问题，基于我们已经有著名的反诈 APP 和诸如鸿蒙之类优秀自研国产操作系统，配合上我们全球唯二能享受到全国网络防火墙的幸福待遇，我们对网络隐私问题的担忧可以通过弘扬特色传统文化，增强文化自信的方式来解决。于是，“恐慌误导信息”得到了良好的处理，“境外势力”再次挫败，我们又一次毫无疑问的赢了，赢麻了。

# Security measures in daily life 日常生活中的安全措施

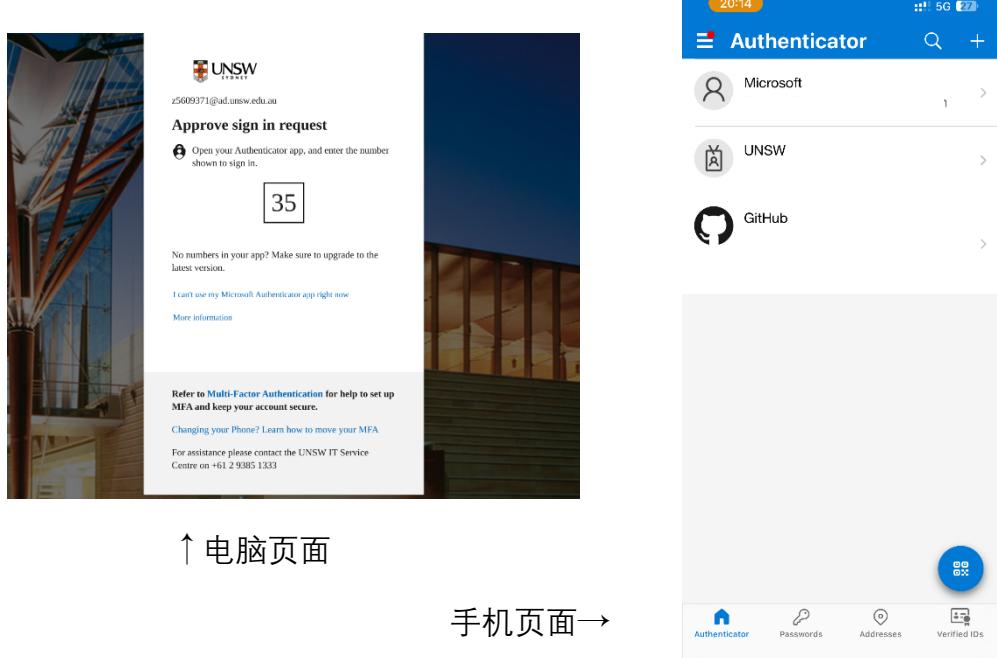
日常生活中我们可以通过以下措施来减少自己被网络攻击的概率：

1. 使用强密码 (包含大小写字母, 数字, 特殊字符及符号等)
2. 不点击可疑链接
3. 安装防病毒软件
4. 规律的更新系统的安全补丁(security update)
5. 不安装盗版软件(pirated software)
6. 不随意连接公众场所的开放 WIFI
7. 使用电脑中的防火墙功能 (下文会详细介绍)

## 多重身份验证

除了以上这些老生常谈的内容, 多重身份认证(multi-factor authentication)在我们生活中的应用也越来越多, 形式也更多种多样。比如, 很多登录系统会要求你在输入正确密码之后使用手机或者邮箱接收验证码, 用来二次验证你的身份。

普通输入密码的验证方式被称作知识验证(knowledge authentication), 因为其基于你所知道的密码。除此之外还有所有权验证(possession authentication)。例如, 当我们登录 UNSW 的相关网站时, 它会要求我使用手机上相应的软件进行验证<sup>68</sup>:



<sup>68</sup> 照片由 Tommy 提供

与普通手机验证码不同的是，用户的账号只能通过指定的手机软件绑定到唯一一部手机上，以此通过验证用户对手机的所有权来验证身份。

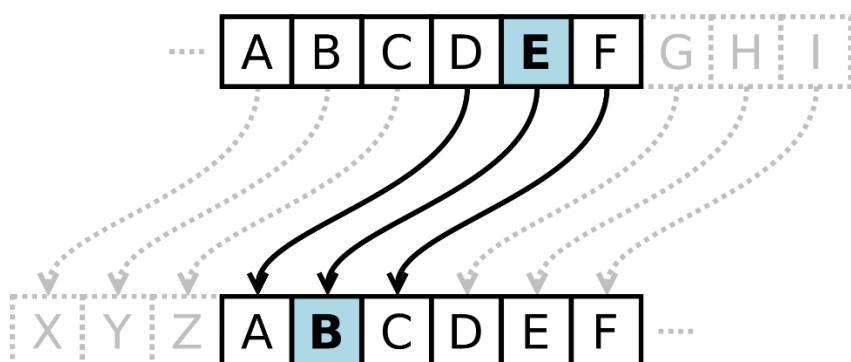
生物验证(biometric authentication)也逐渐成为手机和电脑的标配。通过指纹识别(fingerprint recognition)，视网膜扫描(retina scan)等方式，生物识别可以进一步确保我们的信息安全。

# Technologies to ensure safety 安全技术

## 加密

加密( encryption)是人们一直以来在研究的领域。最早的加密信息可能是公元前 1900 古埃及的抄写员使用非标准的象形文字进行抄写。在罗马共和国时期，将军们使用凯撒密码(Caesar cipher)进行军事机密的传递。

加密的过程通常要使用一个密钥(key)。密钥规定了信息将被如何加密，加密过的信息也只有用密钥才能解开。比如凯撒密码，它的工作原理是将 26 个字母按照顺序移位，如下图<sup>69</sup>：



图中字母向前移动了 3“格”。也就是说，原文中的 D 变成了 A，而 A 变成了 X，如下表<sup>70</sup>：

原 文	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
加 密	X Y Z A B C D E F G H I J K L M N O P Q R S T U V W

单词 Hello 加密过后变为了 Ebii!。我们只有知道单词的加密方式是向前移动 3 “格”才可以还原出原文。3“格”在这里就是加密算法的密钥。



### 扯扯闲话：密码学初探

B 站上的一个科普视频进一步介绍了以上内容：

<https://www.bilibili.com/video/BV1Wv411y7UA>



<sup>69</sup> [https://en.wikipedia.org/wiki/Caesar\\_cipher](https://en.wikipedia.org/wiki/Caesar_cipher)

<sup>70</sup> [https://en.wikipedia.org/wiki/Caesar\\_cipher](https://en.wikipedia.org/wiki/Caesar_cipher)

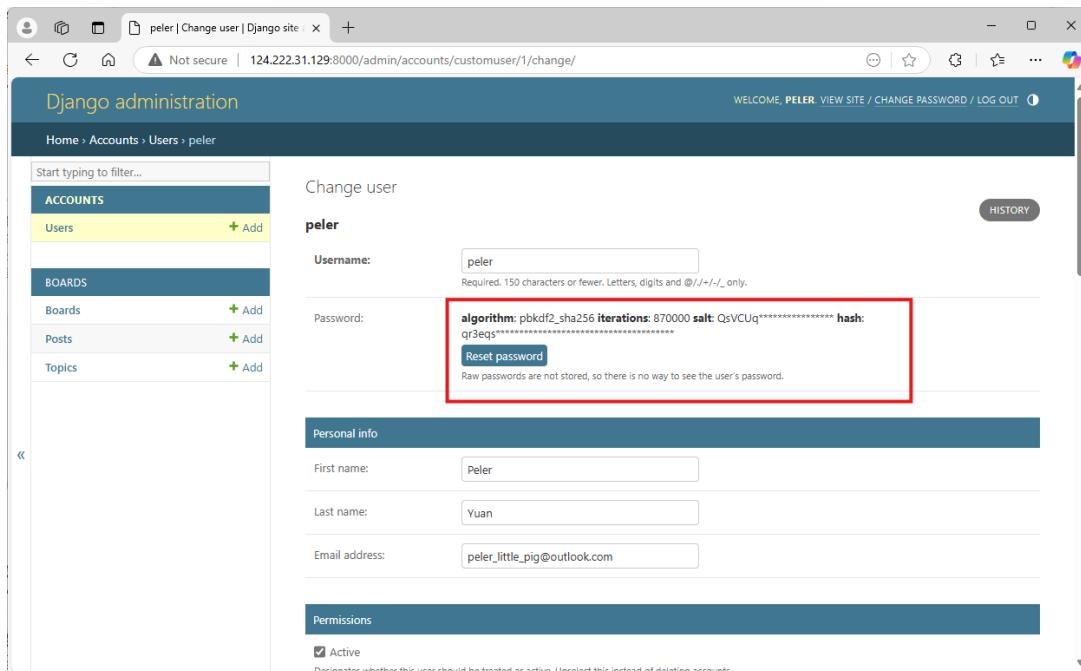
## 哈希算法

哈希算法(hash algorithm)是一种单向函数(one-way function)，它会将任意长度的明文内容转换为固定长度的哈希值。为什么是单向函数？“单向”体现在你很难（或者不可能）通过哈希值反推出原文的内容，这被称为不可逆性(irreversibility)。“函数”体现在一段明文只会对应唯一一种哈希值，且一般情况下不同明文的哈希值也并不会相等。哈希函数还有高敏感性(avalanche effect)，明文内容的微小改变就会让哈希值看起来完全不同<sup>71</sup>：

hello → 2cf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c1fa7425e7 ...

Hello → 185f8db32271fe25f561a6fc938b2e264306ec304eda51800 ...

哈希算法通常被公司们用来加密密码等信息，以防止黑客攻击。比如我搭建的文件管理网站。在其后台管理界面，身为管理员的我也不可能看到网站上用户的密码，只能看到一串哈希值，这很好的阻止了信息的内部泄露：



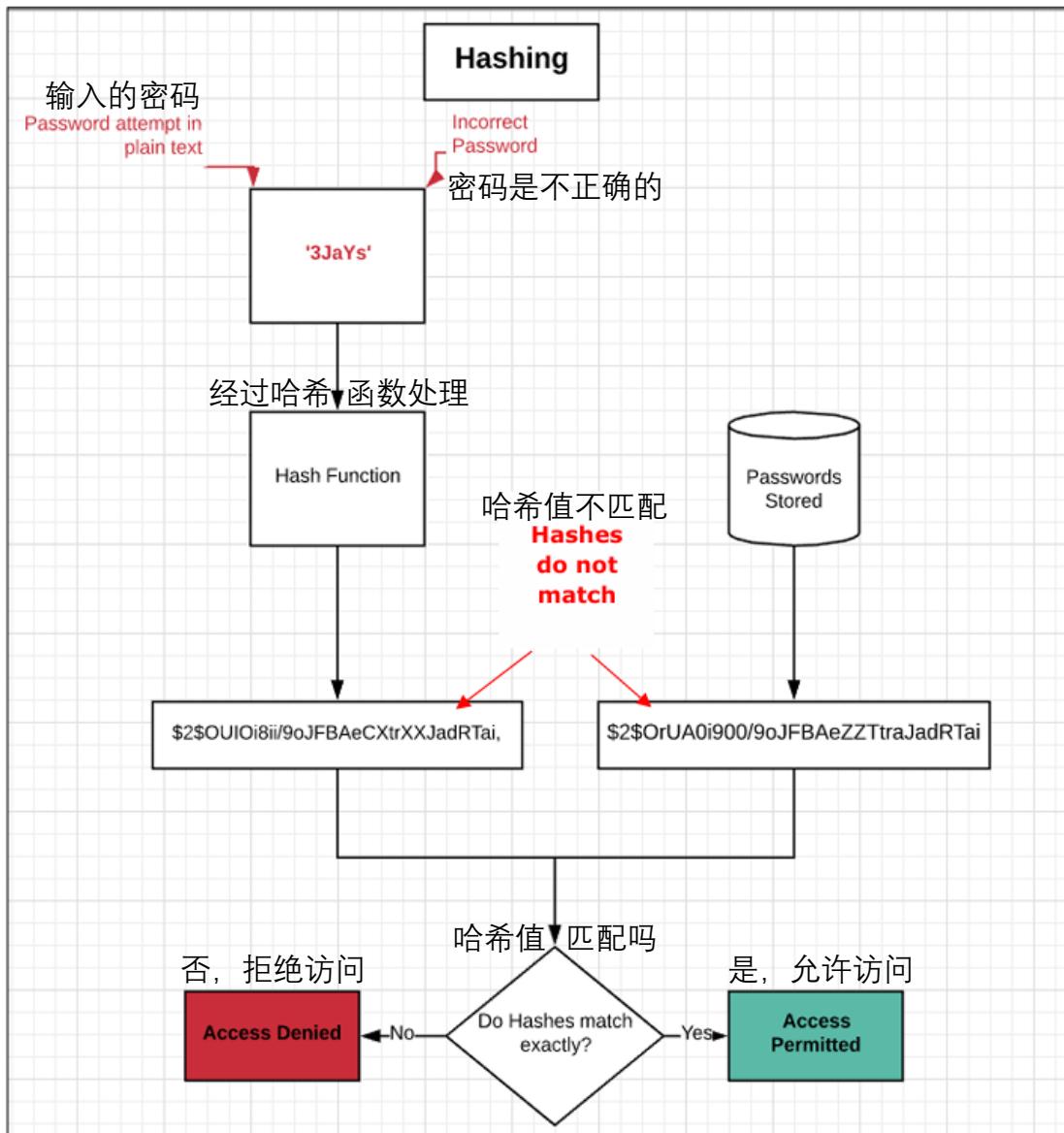
The screenshot shows the Django administration 'Change user' page for a user named 'peler'. The 'Password' field is displayed as a redacted string: 'algorithm: pbkdf2\_sha256 iterations: 870000 salt: QsVCUq\*\*\*\*\* hash: qr3eqs\*\*\*\*\*'. This string is highlighted with a red box. Below the password field, a note says 'Raw passwords are not stored, so there is no way to see the user's password.'

当用户在登录页面输入密码时，系统会将他/她输入的密码转换为哈希值，再与服务器中的哈希值进行比对。此过程防止了密码在传输以及储存过程中的泄露（即使哈希值被窃取，由于其不可逆性，犯罪分子也难以复原出明文信息）。书中<sup>72</sup>提供了一副很好的示意图<sup>73</sup>：

<sup>71</sup> 以下示例使用 SHA-256 算法

<sup>72</sup> 新南威尔士大学 Foundation 阶段配套教材

<sup>73</sup> 引用原图进行翻译处理



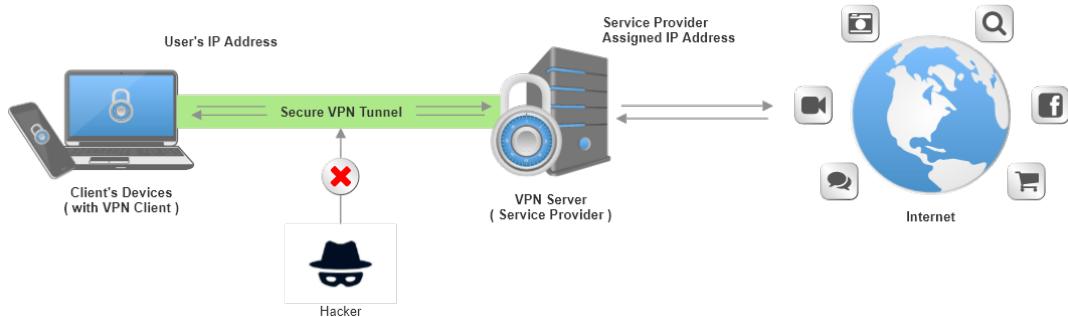
## SSL

在第 2 章中，我们已经了解了 HTTPs 和 TLS。SSL 是 TLS 的前身，现在已经被 TLS 取代。SSL 通过验证服务器的公钥（公共的密钥(public key)，由证书颁发机构(Certificate Authority, CA)提供）来验证服务器的身份，以确保网络连接的安全。

## VPN

VPN(Virtual Private Network)又称虚拟私人网络。使用 VPN 时，你的电脑会先通过隧道协议(tunnelling protocol)连接到 VPN 服务器。VPN 服务器通常会将你真实的 IP 地址掩盖(mask)，并用一个境外的 IP 地址访问相应的网站服务器，从而达到欺骗网站服务器的目的。如下图<sup>74</sup>：

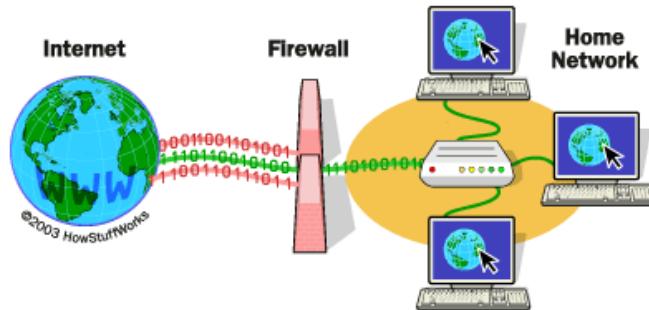
<sup>74</sup> <https://www.hkcert.org/security-guideline/personal-vpn-security-guideline>



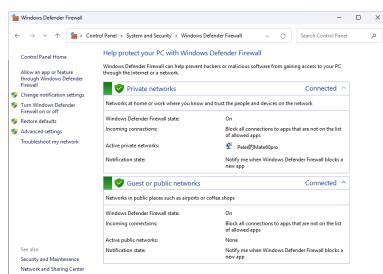
当黑客试图侵入你的电脑和 VPN 服务器之间的通讯时，负责通讯的私有管道(private tunnel)将立刻断裂(drop out)，同时一个新的管道将会形成，用以继续通讯。

## 防火墙

防火墙(firewall)可以防止外部流量的侵入(penetrate)以及内部网络(internal network/intranet)信息的泄露。它就像是一座城门一样，对出入的数据进行审查，并阻止可疑的连接。如下图<sup>75</sup>：



防火墙既有硬件形式也有软件形式。通常，我们的家用路由器中就包含着防火墙，保护着整个家庭网络。MacOS 和 Windows 系统的电脑上也都装有防火墙软件，可以进一步保护我们的电脑，非常重要。



Windows 系统中的软件防火墙控制中心

硬件防火墙<sup>76</sup>

<sup>75</sup> <https://www.comodo.com/resources/home/how-firewalls-work.php>

<sup>76</sup> <https://www.amazon.com/Firewall-Hardware-OPNsense-Security-Appliance/dp/B09H6YJ9G2>

# Hacking 黑客攻击手段

黑客(hacker)通常指编写恶意软件攻击计算机系统的人。为了便于区分，这些人也被叫做黑帽(black hat)黑客。除此之外还有白帽(white hat<sup>77</sup>)黑客，或称为道德黑客(ethical hacker)。他们查找计算机的漏洞用以更好的保护计算机。接下来，我们将了解常见的黑客攻击手段。

## 暴力破解

暴力破解(brute force attack)大概是最简单粗暴的一种方式——编写一个计算机程序不断尝试密码，直到将密码试出来。

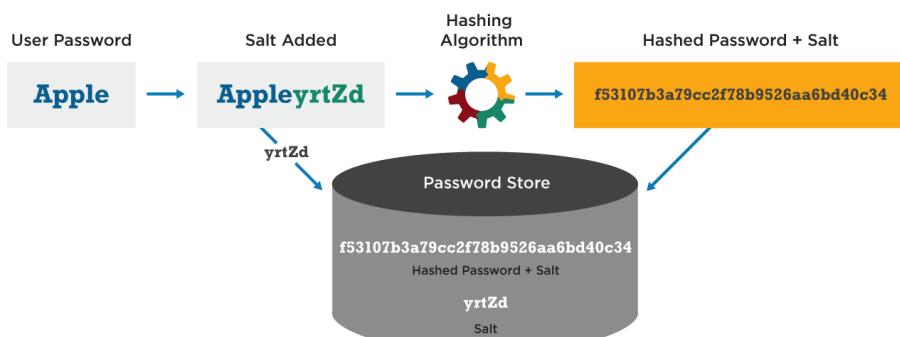
还记得我们之前讲过的哈希加密吧。一种对其暴力破解的方法是使用彩虹表(rainbow table)。彩虹表中包含大量预先计算好的哈希值，用以匹对明文密码。黑客可以通过彩虹表大量的尝试，从而得知明文密码的加密方式，以此反向破解(crack)整个加密系统。一台高性能的计算机破解一个弱加密的哈希值可能要花费数个月。现代的哈希算法也针对暴力破解进行了有效的防护措施，加盐算法(salt algorithm)就是主要手段之一。



### 扯扯闲话：加盐算法

加盐算法的设计理念听上去非常简单易懂。彩虹表不是包含大量提前算好的明文和其对应的哈希值吗？那我就在每次计算哈希值的时候在明文中随机添加一些信息，也就是“盐”。在保存的时候，我将哈希值和“盐”一起保存起来，方便下回比对使用。流程如下图<sup>78</sup>：

#### Password Hash Salting

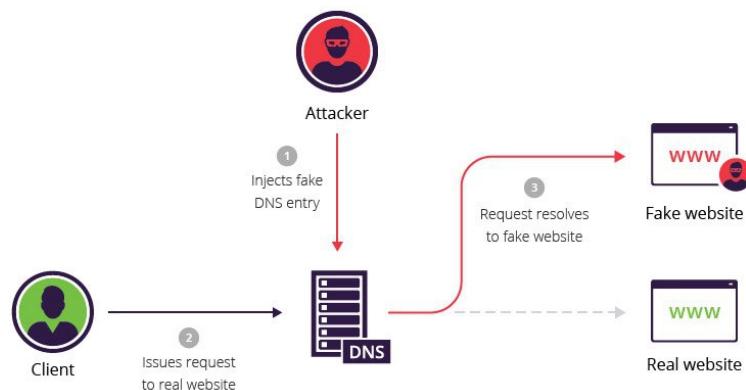


<sup>77</sup> 注意是白帽黑客！White **HAT** hacker! 而不是 white hacker!

<sup>78</sup> <https://cyberhoot.com/cybrary/password-salting/>

## DNS 欺骗

DNS 欺骗(DNS spoofing)是中间人攻击(man-in-the-middle-attack)的一种。黑客通过攻击网络连接中的“中介”——DNS 服务器<sup>79</sup>以达到非法目的。<sup>80</sup>例如，黑客可以通过篡改 DNS 服务器中指定域名对应的 IP 地址，从而将用户引入一个伪造的网站。如下图<sup>81</sup>：



## 身份盗窃

身份盗窃 (identity theft) 针对于个人。黑客会通过不同手段窃取个人信息，并用此进行违法活动，如使用盗取身份从银行账户中盗取资金。

<sup>79</sup> 参考第 2 章有关部分

<sup>80</sup> 准确来说，中间人攻击指的是在客户端和服务器的通讯之间插入一个“中间人”以达到非法修改或窃取数据的目的。在 DNS 欺骗中，黑客通过伪造一个 DNS 服务器进行攻击。以书为准。

<sup>81</sup> <https://www.imperva.com/learn/application-security/dns-spoofing>

# Social Networking security

社交网络安全

## 信息加密

日常生活中，我们几乎离不开社交网络。我们使用他们发送信息，进行社交活动。一些信息发送软件并不会对信息进行加密，比如 Facebook 公司<sup>82</sup>的 Messenger 软件，以及 Google 推出的 Hangouts 聊天软件。WhatsApp, Signal, 和 iMessage 会对信息进行端对端(end-to-end encryption)的加密。也就是说，你的信息会在你的手机上加密之后被发送出去，在对方手机接收之后才解密，从而最大程度的保证信息安全。国内的 QQ 和微信显而易见不是端对端加密。

## 大数据

现在的风口，或者说热门领域是人工智能。放到三四年前，那最热门的必然是大数据(big data)。随着互联网用户的增多，收集大量的数据变得可能，因此出现了各种大数据的应用。**简而言之，大数据就是通过收集巨量的数据进行分析，将它们转化为有价值结果的过程。**日常生活中最常见一个例子就是短视频推荐。科技公司使用大数据算法收集用户的数据，分析用户的喜好将不同的内容推荐给相应的用户，以满足用户的娱乐需求。

## 信息数字化

信息数字化(digitized information)是大数据分析的基础。历史上一个有名的数字信息化项目是 Google Print Library Project。其将 1500 万本书转换为了电子版。日常生活中，任何包含计算机芯片的东西，比如我们的电脑，手机和智能汽车都可以作为信息数字化的渠道，采集我们的信息。这也就涉及到了网络隐私问题。



### 扯扯闲话：你输入的验证码正在帮助古书修复？

Luis von Ahn 发明了网络验证码，用于进行人机验证。之后，他发现许多机构都在将古书数字化，但是古书中难免会有文字难以识别，于是，他创建了 reCAPTCHA 平台。reCAPTCHA 会首先判断用户是否为人类，确认之后会把难以识别的古书文字推送给用户。如果绝大多数用户给出的答案一致，就确认了单词的拼写。

<sup>82</sup> 现改名为 Meta

B 站上的一期视频对此进行了介绍：

<https://www.bilibili.com/video/BV1T54y1v74W>



## 大数据对社会的影响

大数据身为一种数据分析手段为科学的研究提供了新的思路。快速大量的信息收集和分析使得诸如人类基因图谱的绘制和长期气候预测等项目变为可能。在商业领域，大数据的应用使得企业可以更快速的进行分析决策，进而提高效率并节省成本。

但同时，对用户数据的大量采集带来了隐私安全问题。大数据推荐所产生的信息茧房效应也会加剧人与人之间的差距甚至是社会的分裂。



## 扯扯闲话：算法有价值观吗？

B 站上的这个视频很好的讨论了关于大数据算法的一些社会问题：

<https://www.bilibili.com/video/BV1nQ4y1q7gD>



## 网络隐私保护

隐私保护意味着公民可以不受到那些“不请自来”的监视(uninvited surveillance)。数据隐私问题包含了数据如何被收集，共享和使用。

随着网络的发展，世界上的各个国家或地区都立法保护用户的数据隐私安全。欧盟在 1995 年就建立了“黄金标准(gold standard)”，用以规范科技公司对用户数据的使用。

# Questions 练习

**1. Which technique is used by companies to try to avoid hacks?**

- A. Hashing algorithm
- B. Rainbow table
- C. Phishing
- D. DNS spoofing

**2. What is the name of software that shows unwanted “pop-ups” (弹窗)?**

- A. Virus
- B. Adware
- C. Ransomware
- D. Worms

**3. With regards to using technological devices for communicating and collecting data, what is meant by the term privacy?**

- A. The right for companies to store and withhold an individual's private information without the individual's knowledge.
- B. The right of the individual to be free from uninvited surveillance, governing how data is shared and stored.
- C. The right of the individual to freely communicate any information to anyone or any organization.
- D. The right of companies to use spyware to monitor what employees are doing, ensuring data security.

**4. Which is VPN, Virtual Private Network?**

- A. A network that is private and only used in a company
- B. A network that is completely owned by someone
- C. A network where information being sent is encrypted
- D. A network that uses a tunnelling protocol and the data being sent is encrypted

**5. You received an email from someone who pretends to be a well-known bank. You are asked to click a link and input some of your personal information. What is this called?**

- A. Phishing scam
- B. Internet scam
- C. DNS spoofing
- D. Worm Virus

**6. Which technology uses enormous amounts of information and transforms it into value?**

- A. Internet
- B. Information Technology
- C. Big Data
- D. Global Data

**7. What is the name given to information security experts who use their skills and techniques to test and bypass organizations' Information and Communications Technology (ICT) security to provide advice as to how should the organization strengthen its overall security?**

- A. Hacker
- B. Black hat hacker
- C. Security hacker
- D. Ethical hacker

**8. What is the technique that used to find out the password by trying every possible combination?**

- A. Hashing algorithm
- B. Man-in-the-middle attack
- C. Brute force attack
- D. Virus

**9. Which list contains malware?**

- A. rainbow table, brute force attack
- B. big data, virus
- C. trojans, worms
- D. malspam, maladvertising

**10. When a message is **scrambled** before sending and unscrambled after receiving, what is this called?**

- A. hypertext transfer protocol
- B. hashing
- C. encryption
- D. hacking

# Answers 答案

## Multiple choice:

1. A, 见第 77 页。
2. B, 见第 68 页, 请注意 pop-ups 一词!
3. B, 见第 83 页。
4. D, 见第 78 页。
5. A, 见第 68 页。
6. C, 见第 82 页。
7. D, 见第 80 页, 以及下面的扯扯闲话。
8. C, 见第 80 页。
9. C, 见第 71 页。
10. C, scramble 意指加密, 但感觉比较生僻, 放在这里增加印象。



### 扯扯闲话: 什么是 ICT security

当你看到这道题的时候, 是不是觉得眼前一黑。这么一长串题目, TOO HARD<sup>83</sup>! 其中主要的难点就是理解什么是 Information and Communications Technology (ICT) security。

要用官方一点的解释, 它指的是用于保护数字信息、系统和网络免受网络威胁、未经授权的访问、数据泄露及其他安全风险的策略、政策和措施, 旨在确保信息系统的机密性、完整性和可用性。(由 ChatGPT 生成)

其实说白了, 这就是指计算机系统的安全。无非说的高大上一点。

<sup>83</sup> 能使化学老师 Jason 立刻红温的咒语, 创始人为 Ethan Zhu

# Vocabularies 词汇

单词	释义	页码
<b>cyber crime</b>	网络犯罪	66
<b>malware</b>	恶意软件	66
<b>hijack</b>	劫持	66
<b>readable</b>	可读的	66
<b>plaintext</b>	明文信息	66
<b>cyber security</b>	网络安全	66
<b>unauthorized access</b>	未经授权的访问	66
<b>cyber privacy</b>	网络隐私	66
<b>abuse</b>	滥用(数据)	67
*zero-day vulnerability	0day 漏洞	67
<b>adware</b>	广告软件	68
<b>maladvertising</b>	恶意广告	68
<b>malspam</b>	恶意邮件	68
<b>phishing</b>	网络钓鱼	68
<b>social engineering</b>	社会工程学	68
*baiting	奖励诱骗	69
*pretexting	伪造	69
<b>spyware</b>	间谍软件	69
<b>ransomware</b>	勒索软件	70
<b>virus</b>	病毒	71
<b>malicious</b>	恶意的	71
<b>program</b>	程序	71
<b>code</b>	代码	71
<b>contract</b>	感染(电脑病毒)	71
<b>attachment</b>	(邮件)附件	71
<b>scam link</b>	诈骗链接	71
<b>shady</b>	可疑的	71
<b>trojans</b>	木马病毒	71
<b>legitimate</b>	合法的	71
*DoS	拒绝服务攻击	72
*DDoS	分布式拒绝服务攻击	72
<b>worms</b>	蠕虫病毒	72
<b>security update</b>	安全补丁	74

<b>pirated software</b>	盗版软件	74
<b>multi-factor authentication, MFA</b>	多重身份验证	74
<b>knowledge authentication</b>	知识验证	74
<b>possession authentication</b>	所有权验证	74
<b>biometric authentication</b>	生物验证	75
<b>fingerprint recognition</b>	指纹识别	75
<b>retina scan</b>	视网膜扫描	75
<b>encryption</b>	加密	76
*Caesar cipher	凯撒密码	76
<b>key</b>	密钥	76
<b>hash algorithm</b>	哈希算法	77
*one-way function	单向函数	77
<b>irreversibility</b>	不可逆性	77
*avalanche effect	高敏感型	77
<b>public key</b>	公钥	78
*certificate authority, CA	证书颁发机构	78
<b>virtual private network, VPN</b>	虚拟私人网路	78
<b>tunnelling protocol</b>	隧道协议	78
<b>mask</b>	掩盖(IP 地址)	78
<b>private tunnel</b>	私有管道	79
<b>drop out</b>	(私有管道)断裂	79
<b>firewall</b>	防火墙	79
<b>penetrate</b>	侵入	79
<b>internal network/intranet</b>	内部网络	79
<b>hacker</b>	黑客	80
<b>black hat</b>	黑帽(黑客)	80
<b>white hat</b>	白帽(黑客)	80
<b>ethical hacker</b>	道德黑客	80
<b>brute force attack</b>	暴力破解	80
<b>rainbow table</b>	彩虹表	80
<b>crack</b>	破解	80
<b>salt algorithm</b>	加盐算法	80
<b>DNS spoofing</b>	DNS 欺骗	81
<b>man-in-the-middle-attack</b>	中间人攻击	81
<b>identify theft</b>	身份盗窃	81

<b>end-to-end encryption</b>	端对端加密	82
<b>big data</b>	大数据	82
<b>digitized information</b>	信息数字化	82
<b>uninvited surveillance</b>	“不请自来”的监视	83
*gold standard	黄金标准	83
<b>pop-ups</b>	弹窗	84
<b>scramble</b>	加密	85

# 写给同学的 IT 书

到了 Foundation 阶段，IT 突然变成了一门正经学科，本来概念就难以理解，还是英文授课，根本听不懂，记不住啊！

这本书的出现就是为了解决这个问题。本书融会贯通了 PPT 和英文教材中的内容，添加了生动的解释，并结合考题突出了关键知识点。此外还有练习题和扩展内容，供想要了解更多的同学学习。

本书包含教材中所有理论内容：

- Lecture 2: How Computers Work
- Lecture 3: The Internet
- Lecture 4: Website Evaluation
- Lecture 5: Security and Privacy

作为 Peler 的好朋友，很荣幸为这本书写推荐语。从我个人角度来说，我从小对电脑技术只能说十窍通了九窍，一窍不通……但是在这本书中，再晦涩难懂的 IT 知识也有通俗易懂的解答，相信同学们一定可以通过这本书更好的理解课堂上的内容。

— Ovey

来自 2023 级商科班

**Peler**，本书作者。来自 2023 级，写作此书时是理科 2 班一名准预科学生。身为 Tommy 挑选的接班人，负责继续在机房制造事故。Peler 从幼儿园开始为乐高的 EV3 套件编写程序，逐渐沉迷于编写各种有趣的软件。在休闲时光里，他喜欢喝咖啡和打台球，并经常带着耳机发癫。他还对经济，摄影和骑车感兴趣，总是通过各种方式取悦自己的脑子以希望它正常运转。

**Tommy**，本书技术审核。来自 2025 届理科班，无数机房故事与事故的始作俑者。由于闲得慌开始给 Igor 写程序，由此一发而不可收拾。从小开始学计算机方面的知识，三年级从 Free Basic 入门，曾经在 Basic 编程班取得倒数第一的好成绩。前 Oler，现热衷于工程问题，希望掌握全栈能力。虽然决定不以计算机为专业，但是依然热爱这行业（跑去学化学+分子细胞生物学去了）。爱好广泛，还喜欢天文，摄影，帆船，出门旅游。时不时尝试研究点经济问题，总是希望自己多看点书。

本书（仅限文字内容）© Peler Yuan，采用 CC BY-NC-SA 4.0 许可。仅限非商业用途，相同方式共享。

本书使用的部分图片来自网络，其版权归原作者或来源网站所有。本书仅用于非商业用途，不对图片版权进行再授权。

若有任何疑问，请联系：[pelerlittlepig@gmail.com](mailto:pelerlittlepig@gmail.com)



本书电子版