

计算机网络安全技术



- 课程代号：40240572
- 课程对象：本科生
- 授课教师：尹 霞
- 开课单位：计算机系网络所

为什么学习计算机网络安全

无处不在的通信

- 通信是人类的基本需求
- 电信网的发展历程
- 计算机网络的发展历程

无处不在的网络安全

- 互联网是重要的社会基础设施
- 互联网中的攻击
- 互联网中的防守

揭开现象看本质

- 你应该知道的安全大师：阿瑟和阿兰
- 加密之王Enigma
- 上帝派来的数学黑客

无处不在的通信

通信是人类的基本需求

电信网的发展历程

计算机网络的发展历程



清华大学 110周年校庆
110th ANNIVERSARY
TSINGHUA UNIVERSITY

通信是人类的基本需求



通信是人类的基本需求

• 古代通信

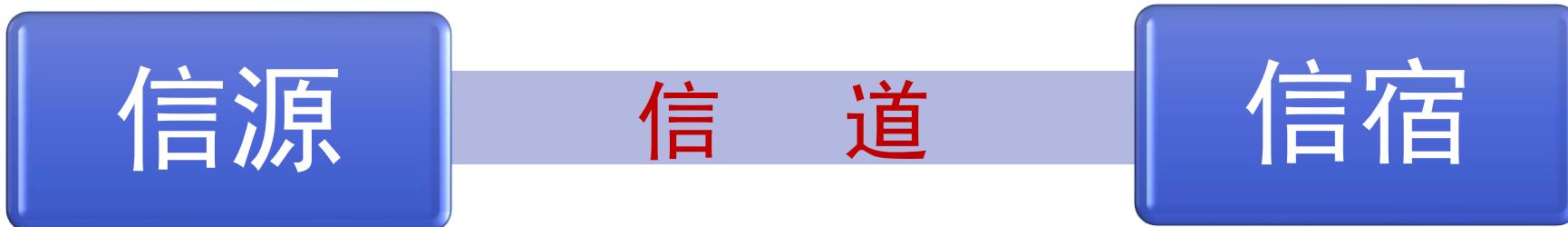
- 人类随着社会生产力水平的不断提高，活动区域不断扩大，信息交流的范围随之扩展，通信逐步成为基本需求
- 据文字记载，从西周开始，中国的“通信”组织不断完善，逐渐形成了两套官方“通信”系统
 - 一套是以步行、乘车为主的邮传“通信”系统
 - 一套是以烽火为主的声光“通信”系统：烽火戏诸侯

• 现代通信

- 感谢电的发现、电磁感应的发现、电磁波的发现
- 感谢计算机的发明

通信的基本要素

- 信源、信道、信宿
- 信源变成可传输的信号后，通过信道（媒介）传输给信宿的过程就叫通信



当今流行的通信技术

- 一个多世纪前，电信网开始出现，在政府的支持下渐渐形成规模，逐渐成为当时最流行的最先进的通信技术
- 半个多世纪前，计算机网络开始出现，并且以惊人的速度发展起来，成为当今最流行的最先进的通信技术
- 同时，现代生活中还存在着另外一种单向广播式的网络---有线电视网
- 所谓的“三网合一”中的三网就是计算机网络、电信网和有线电视网



网络的层次

电话
传真

新闻广播
电视节目

电子邮件
信息浏览
IP电话

电信网络

有线电视网络

计算机网络

通信基础传输网（光纤、卫星、微波等）



清华大学 110周年校庆
110th ANNIVERSARY
TSINGHUA UNIVERSITY

电信网的发展历程



电信网发展的里程碑

电报

电话

电磁波

无线电报

通信

无线电

寻呼机

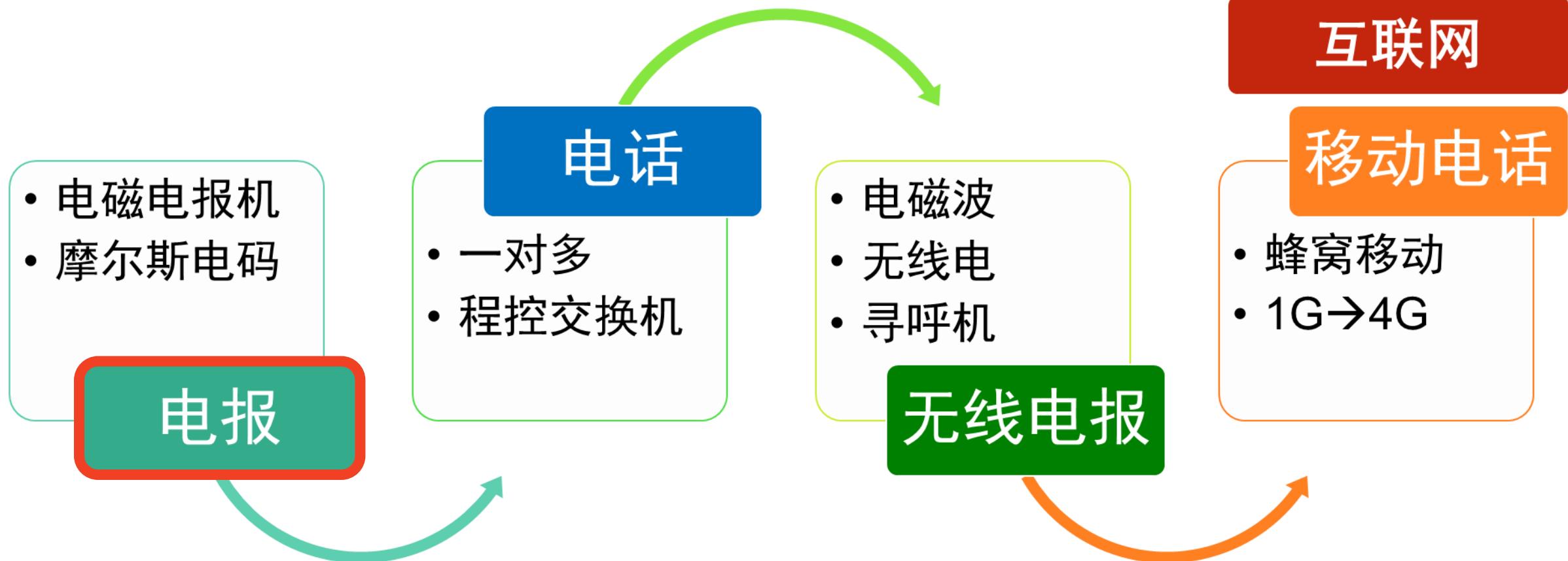
移动电话

蜂窝式

GSM手机

电信网的发展历程

- 三张网：电信网、计算机网、有线电视网



有线电视网

互联网

移动电话

电报

- 19世纪30年代，由于铁路迅速发展，迫切需要一种不受天气影响、没有时间限制又比火车跑得快的通信工具
 - 此时发明电报的基本技术条件也已具备：电池、铜线、电磁感应器
- 1836年，英国人约翰库克和惠斯通制成电磁电报机，于次年设计制造了第一个有线电报，并申请了专利
- 电报是19世纪30年代在英国和美国发展起来的
 - 电报信息通过专用的交换线路以电信号的方式发送出去，电信号用编码代替文字和数字，通常使用的是摩尔斯电码



摩尔斯电码 Morse Code

- 短促的点信号 “·”，读“滴”；
- 保持一定时间的长信号 “—”，读“嗒”
- 间隔时间：
 - 滴=1t
 - 嗒=3t
 - 滴嗒间=1t
 - 字符间=3t
 - 单词间=7t

International Morse Code

1. The length of a dot is one unit.
2. A dash is three units.
3. The space between parts of the same letter is one unit.
4. The space between letters is three units.
5. The space between words is seven units.

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	— — — • •

1	• — — — — — —
2	• • — — — — —
3	• • • — — — —
4	• • • • — — —
5	• • • • •
6	— — • • •
7	— — — • • •
8	— — — — • • •
9	— — — — — • •
0	— — — — — — •

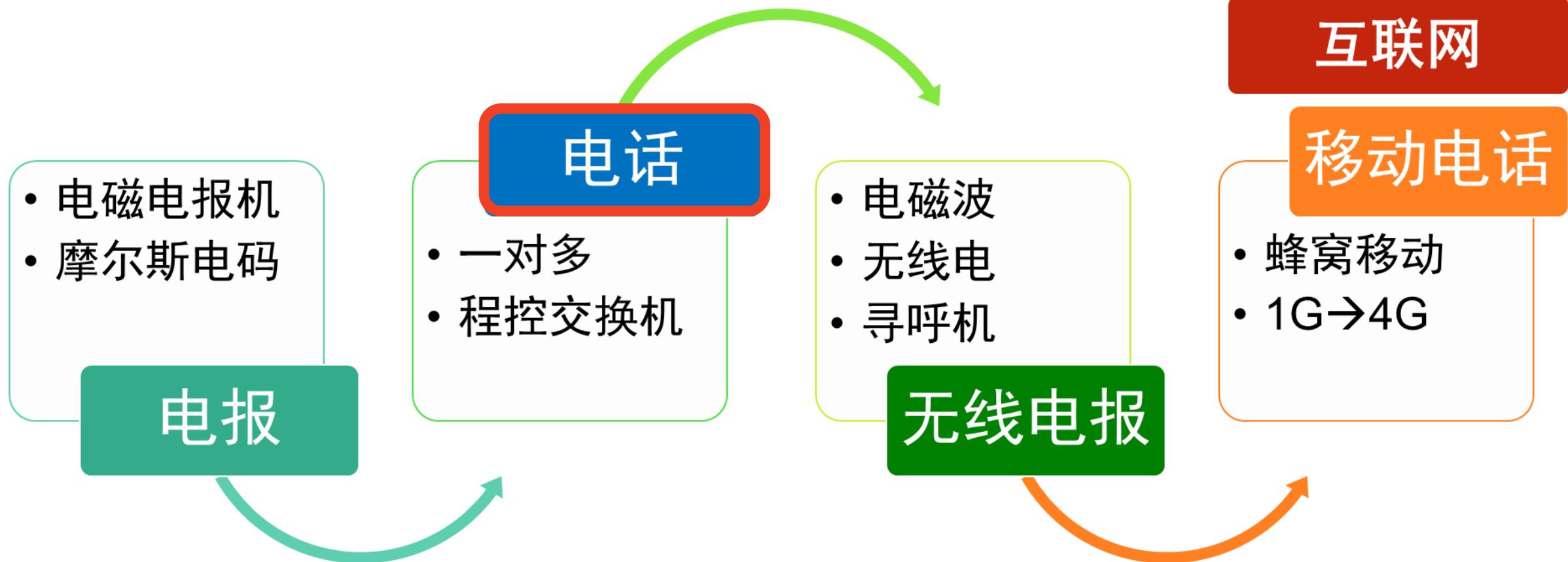
... .—.. —— ...— . —.— —.— .—

电报是工业社会的一项重要发明

- 电报大大加快了消息流通，是工业社会的一项重要发明
 - 早期电报只能在陆地上通讯，后来使用海底电缆，开展了越洋服务
 - 1858年8月5日，总长为3240公里的电缆敷缆完毕，第一份海缆电报横越大西洋
- 电报不仅手续麻烦，而且也不能进行及时双向信息交流
 - 发送一份电报，得先将报文译成电码，再用电报机发送出去
 - 收报方，要将收到的电码译成报文，然后送到收报人的手里
- 人们开始探索一种能直接传送人类声音的通信方式，这就是“电话”

电信网的发展历程

- 三张网：电信网、计算机网、有线电视网



有线电视网

互联网

移动电话

电话原理的形成

- 1753年，《苏格兰人》杂志首次提出来用电流进行通话的设想
- 1796年，英国人休斯提出了用话筒接力传送语音的办法，并将之命名为Telephone，这个名字一直沿用至今
- 1854年，法国人鲍萨尔设想了电话的工作原理：将两块薄金属片用电线相连，一方发出声音时，金属片振动，变成电，传给对方
- 问题是：
 - 怎样才能把声音这种机械能转换成电能，并进行传送？
 - 打电话的送话器和听电话的受话器如何构造？

实现电话需要解决的问题

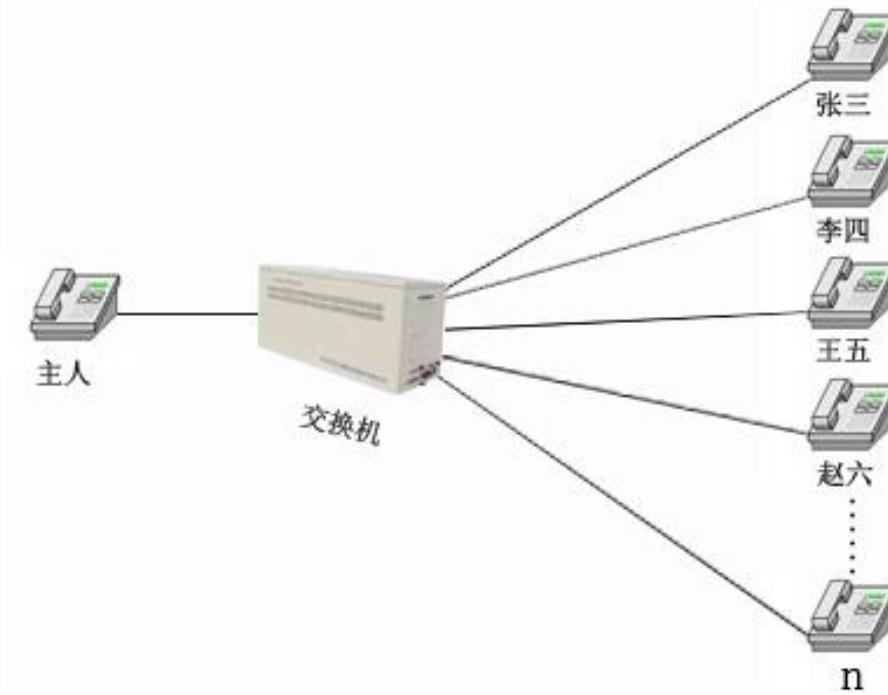
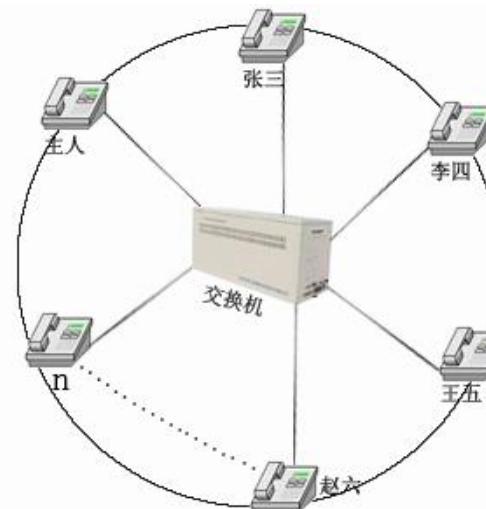
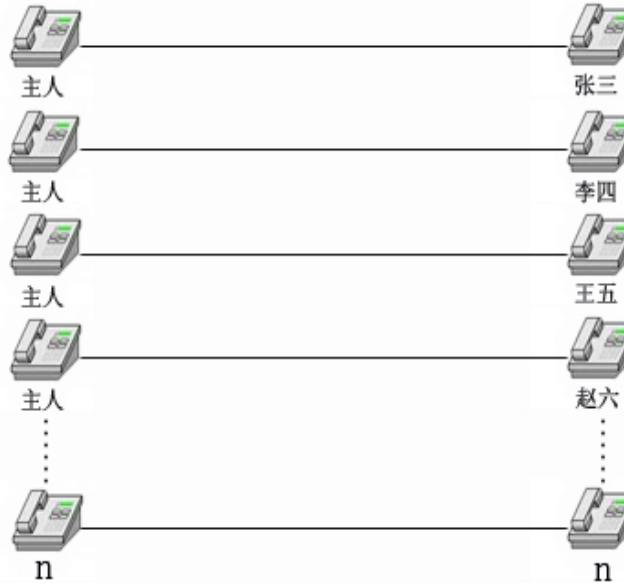
- 能把声音变成电信号的送话器
 - 贝尔送话器：利用电磁感应，声音不同造成金属片振动不同，从而产生的电场与磁场的场强不同
 - 格雷送话器：利用液体电阻的变化
 - 爱迪生送话器：利用活性炭的振动，后又发明了炭精送话器
- 传输导线：铜
 - 电阻小、惰性强、产量大、价格低
- 能把电信号变成声音的受话器：电磁感应
- 1876年3月7日，贝尔获得发明专利

电话的初步商用

- 1877年，贝尔架设了波士顿至纽约的300公里的长途电话线路，第一条电话线路开通了；有人第一次用电话给《波士顿环球报》发送了新闻消息，从此开始了公众使用电话的时代
 - 一年之内，贝尔共安装了230部电话，建立了贝尔电话公司，这是美国电报电话公司AT&T前身
- 1882年，电话线采用双绞线
- 1884年5月1日，世界上第一幢10层的摩天大楼在芝加哥建成
 - 正是电话使摩天大楼在大城市里相继涌现
 - 如没有电话，大楼里的信息都要靠人工来传递，那么供通信员使用的电梯是远远不够的

交换机的出现：实现一对多通话

- 最初的电话实现的是一对一的通话；要想实现和多人通话，那就必须同时安装多部电话
- 电话交换机的出现，解决了这个问题



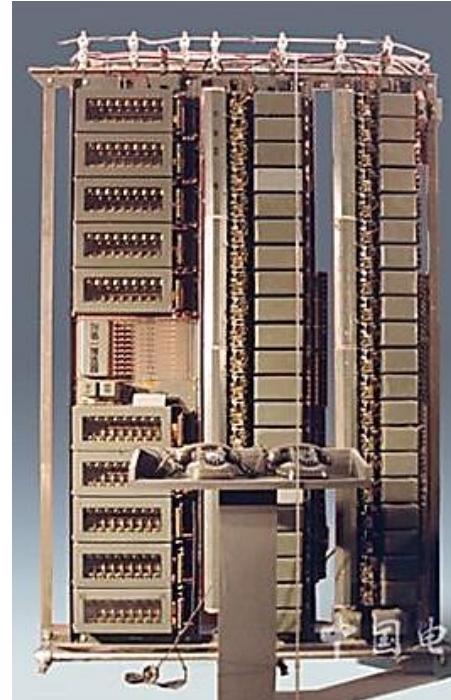
最初的交换机：人工供电制交换机

- 1878年，出现了人工供电制交换机
 - 它是借助话务员进行话务接续，效率很低
 - 1878年9月1日，埃玛.M.娜特成为世界上第一位女性接线员



自动接续的交换机

- 1879年底，电话号码出现了
 - 美国马萨诸塞州一位内科医师受马萨诸塞州流行麻疹的启发而提出：我们需要电话号码，否则一旦接线员病倒，全城电话岂非瘫痪
- 自动接续的交换机
 - 1893年，步进制交换机问世，它标志着交换技术从人工时代迈入机电交换时代
 - 1938年，纵横制交换机问世，解决了速度慢、效率低、杂音大与机械磨损严重等问题



程控交换机：计算机+交换机

- 1946年，世界上第一台电子计算机问世
- 1965年，第一部由计算机控制的程控电话交换机在美国问世，标志着电话新时代的开始

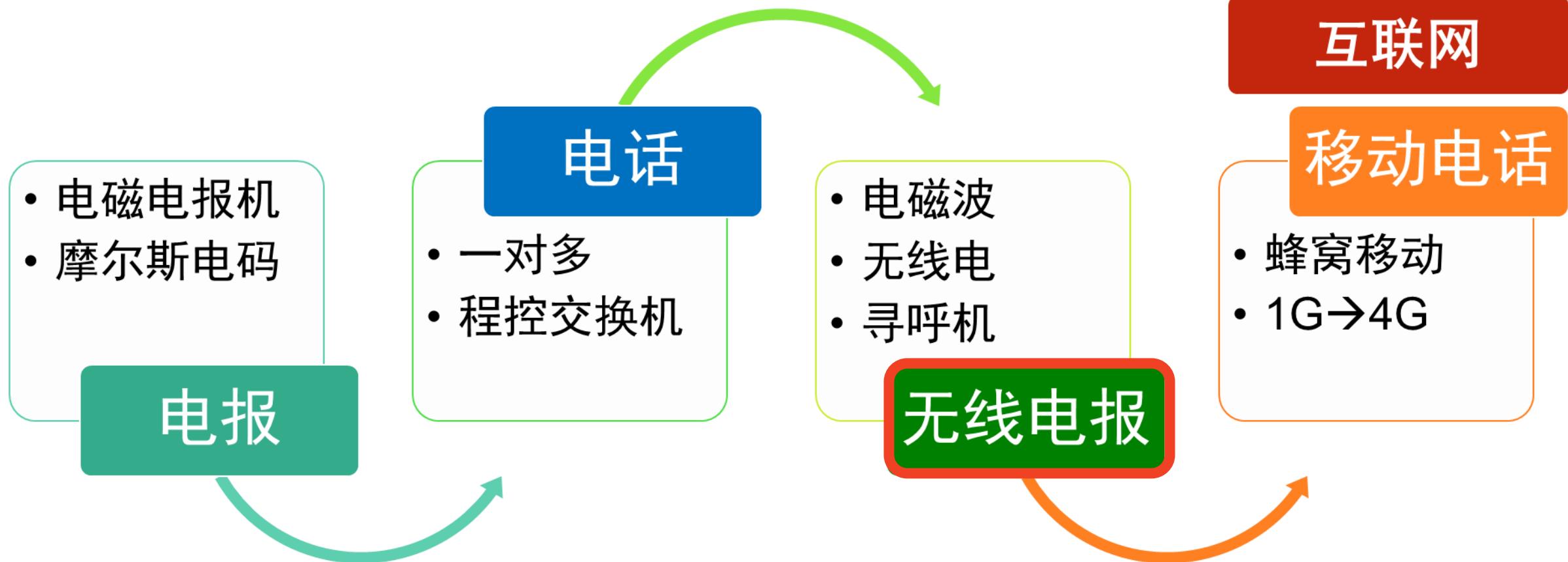
交换机类型	接续方式	控制方式	交换信息
供电制交换机	人工	环路电流	模拟话音业务
步进制交换机	自动	拨号脉冲	模拟话音业务
纵横制交换机	自动	布线逻辑	模拟话音业务
模拟程控交换机	自动	存储程序	模拟话音业务
数字程控交换机	自动	存储程序	数字话音、数据图文传真等

固定电话的局限

- 电报和电话的相继发明，使人类获得了远距离传送信息的重要手段
- 只要有电话，人人都能手拿一个“话柄”，和远方的亲朋好友谈天说地了
- 但是，电信号都是通过金属线传送的；线路架设到的地方，信息才能传到，这就大大限制了信息的传播范围。
- 面对大海、高山，有没有能让信息无线传播的办法？

电信网的发展历程

- 三张网：电信网、计算机网、有线电视网



电磁波和无线电

- 1864年，科学家麦克斯韦用数学公式表达了电磁感应，发表了电磁场理论，成为人类历史上预言电磁波存在的第一人
- 1887年，赫兹提出电磁能量可以越过空间进行传播，从而导致了无线电技术的产生
- 俄国人波波夫和意大利人马可尼各自独立发明了无线电，收音机即无线电接收机
 - 1896年，波波夫成功地用无线电传送了摩尔斯电码，距离250米
 - 1898年，马可尼在英国举行的一次游艇赛上，在离岸20英里的海上终点，用自己发明的无线电报机向岸上的观众及时通报了比赛的结果；这被认为是无线电通信的第一次实际应用，意义重大

实现无线话音传送

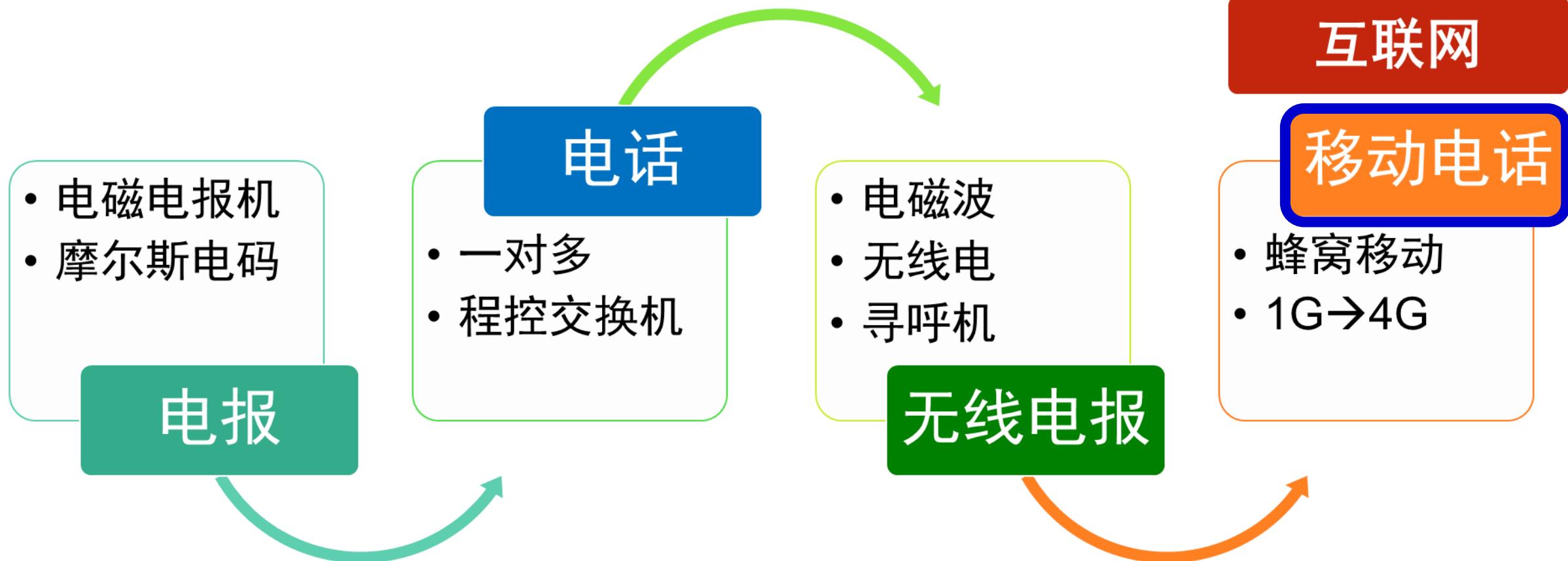
- 1902年，无线电广播之父，美国人巴纳特•史特波斐德，在肯塔基州穆雷市进行了第一次无线电广播
- 军用和商用船舶很快采用了无线电技术
 - 1912年，泰坦尼克号邮轮沉船事件中，利用无线电技术拯救了700多个生命
 - 1920年，美国匹兹堡的KDKA电台进行了首次商业无线电广播
- 第二次世界大战，也是基于无线电的信息战
 - 阿兰·图灵（英国） pk 阿瑟·谢尔比乌斯（德国）

对讲机和寻呼机

- 1941年，摩托罗拉生产出了美军参战时唯一的便携式无线电通讯工具：5磅重的手持对讲无线电样机
 - 设备是电子管的，使用的是短波波段
- 1956年，第一个无线电寻呼机在摩托罗拉公司问世
 - 寻呼机技术的改进史
 - 个体呼叫，向呼叫员询问信息；个体呼叫，打开机器听信息
 - 个体呼叫，打开机器看代码；个体呼叫，打开机器看文字
- 20世纪60年代，晶体管出现，专用无线电话系统大量出现，在公安、消防、出租汽车等行业中应用
- 但是，专用对讲机仅能在少数特殊人群中使用且携带不便，能不能有更小、更方便、适合大众使用的个人移动电话？

电信网的发展历程

- 三张网：电信网、计算机网、有线电视网



有线电视网

互联网

移动电话

无线电话的技术准备：载波

- 载波是传送信息(话音和数据)的物理基础和承载工具
- 载波(carrier wave)是由振荡器产生并在通讯信道上传输的电波，被调制后用来传送语音或其它信息
- 载波频率通常比输入信号的频率高，输入信号调制到一个高频载波上，就好像搭乘了一列高铁或飞机，然后再被发射和接收

无线电话的实现：蜂窝式移动电话

- 70年代初，美国贝尔实验室提出了在移动通信发展史上具有里程碑意义的小区制、蜂窝组网的理论，为移动通信系统在全球的广泛应用开辟了道路
- 1973年4月，一名男子站在纽约街头对着一个约有两块砖头大的设备讲话，引得过路人纷纷驻足侧目
- 1975年，美国联邦通信委员会FCC开放了移动电话市场，为移动电话投入商用作好了准备



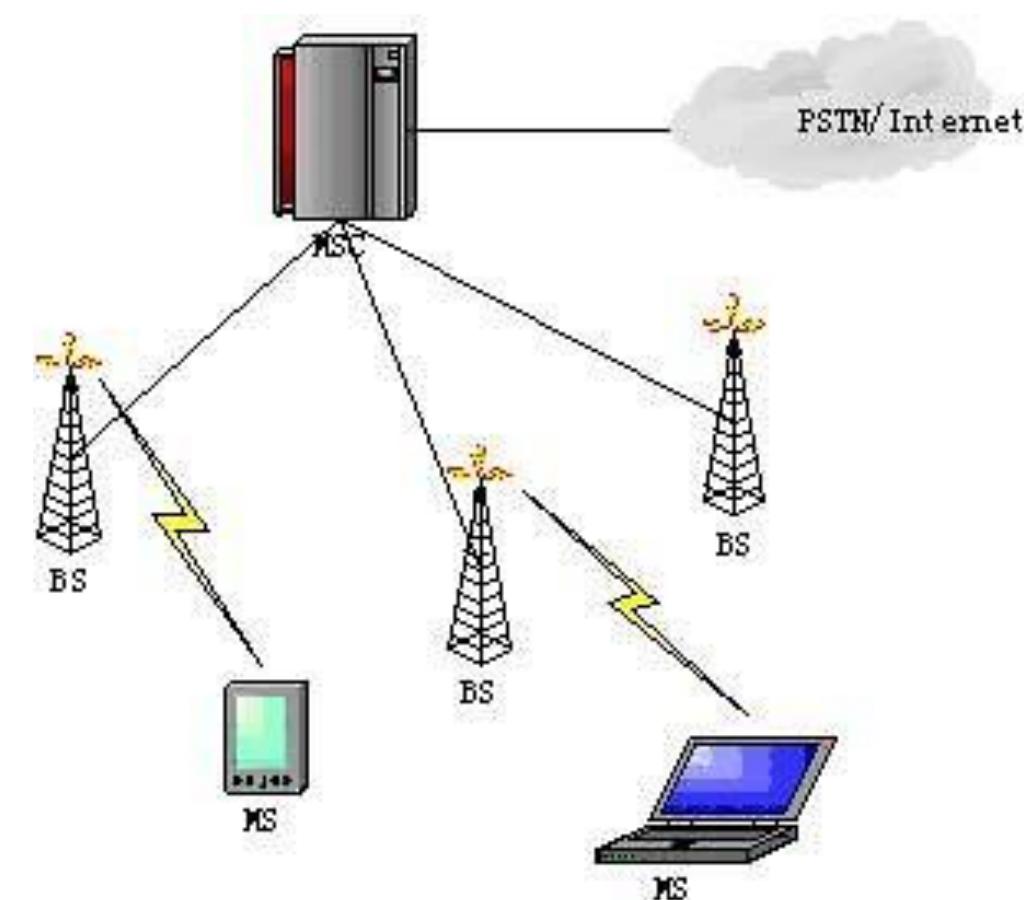
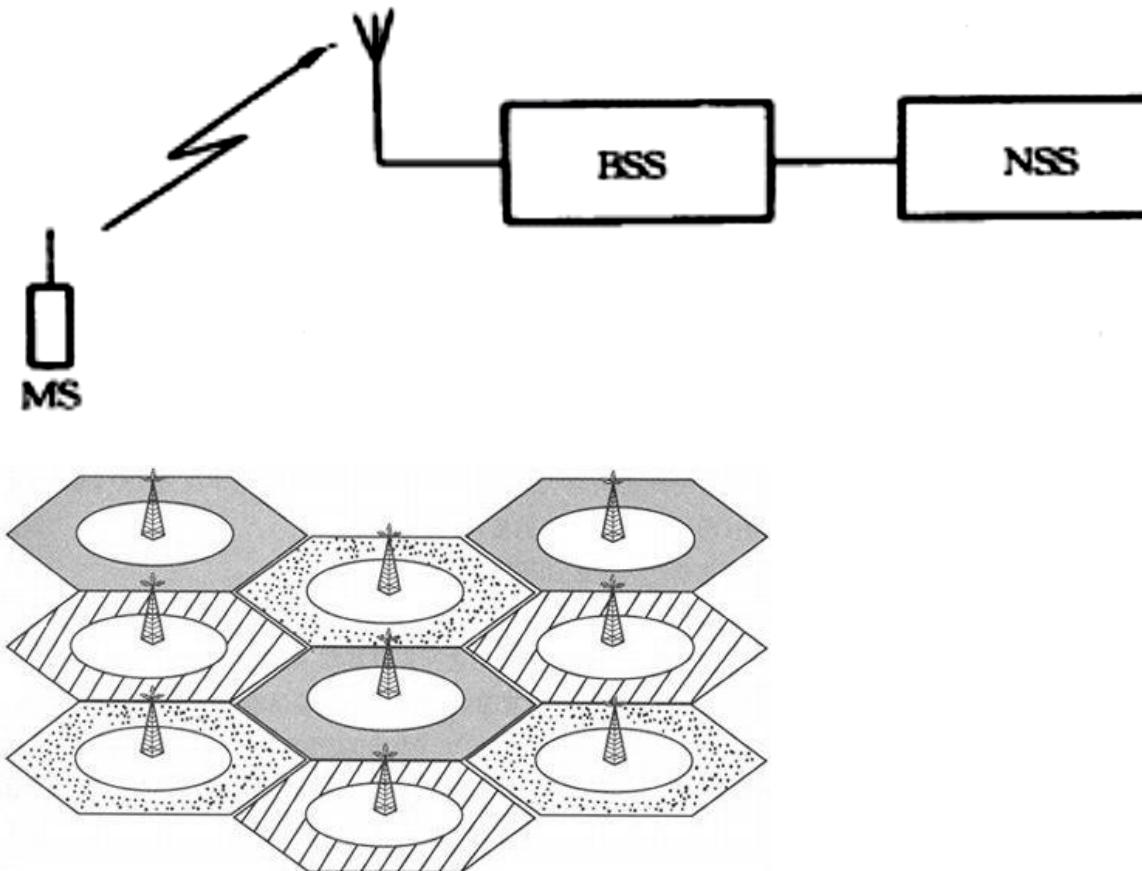
移动电话的发明者马丁·库帕

无线电话的实现：蜂窝式移动电话

- 1978年，美国贝尔实验室在芝加哥开通了“先进移动电话业务系统（AMPS）”，这是第一个真正的具有随时随地通信能力的大容量的蜂窝移动通信系统
- 1983年12月，AMPS在美国投入商用（1G）
- 移动电话在中国
 - 1993年9月18日，浙江嘉兴首先开通了我国第一个数字移动通信网
 - 1994年10月，第一个省级数字移动通信网在广东省开通，容量为5万门，从此GSM手机在国内迅速成长

蜂窝移动通信系统

- 蜂窝移动通信系统主要是由交换网路子系统（NSS）、无线基站子系统(BSS)和移动台（MS）三大部分组成



移动通讯1G→4G

- 1G：第一代移动无线网络是面向语音的模拟无线系统，使用FDMA技术实现
 - 典型的1G标准：美国的AMPS、欧洲的TACS
- 2G：第二代移动无线网络是面向语音的数字无线系统，使用TDMA或窄带CDMA技术实现。
 - 典型的2G数字蜂窝移动标准：欧洲的GSM、北美的IS-54和IS-95以及日本的JDC
- 3G：第三代移动无线网络把蜂窝电话、语音业务以及移动数据业务用各种分组交换数据业务综合在一个高语音质量、高容量、高速率的网络系统中
 - 典型的3G标准：W-CDMA、CDMA2000



移动通讯1G→4G

- 4G：第四代移动无线网络最初目的就是提高无线访问 Internet 的速率，最重要的特征就是更快的无线通信速度
 - 典型的4G标准是TD-LTE和FDD-LTE
- 从移动通信系统数据传输速率作比较
 - 1G：第一代模拟式仅提供语音服务
 - 2G：第二代数位式的传输速率只有9.6Kbps，最高可达32Kbps
 - 3G：第三代数字式的传输速率可达到2Mbps
 - 4G：第四代的传输速率可达到20Mbps，最高可达100Mbps
 - 5G：第五代的传输速率最高可达10Gbps；
低于1毫秒网络延迟，而4G为30-70毫秒

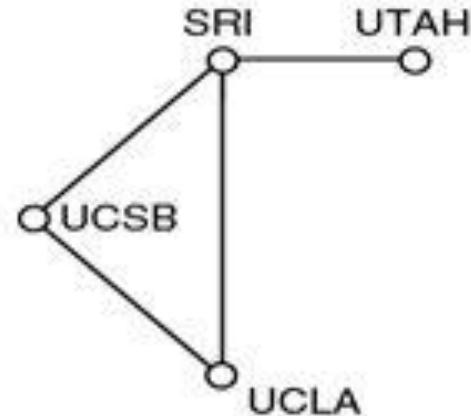
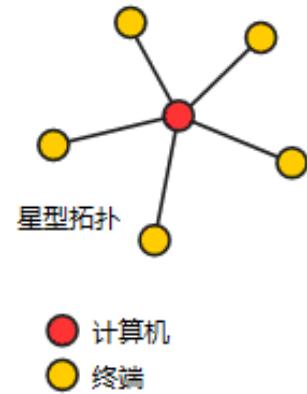


清华大学 110周年校庆
110th ANNIVERSARY
TSINGHUA UNIVERSITY

计算机网络的发展历程



计算机网络的发展历程

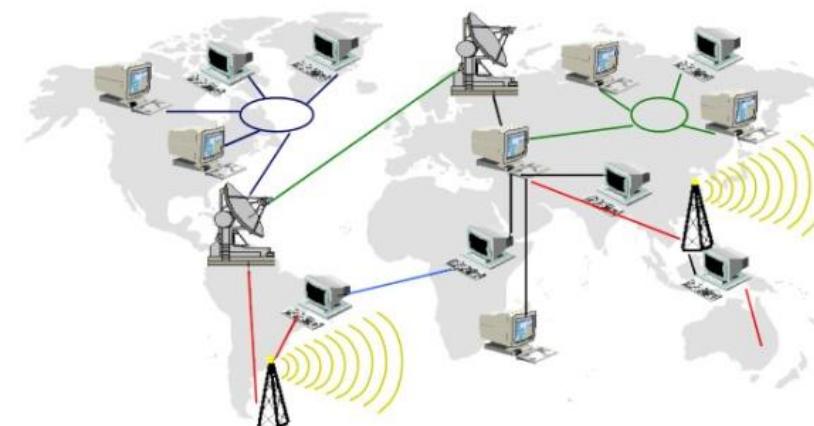


计算机孤岛

终端出现

计算机和
计算机互联

网络与网络
互联



1950年前：没有网络的时代

- 计算机体积庞大，没有终端，学生需要到数据中心交作业，作业的载体是打孔纸带或打孔卡
- 由于不同制造商生产的计算机所使用的数据格式不同，所以计算机之间不能彼此理解对方的数据格式，即便把计算机用数据线连起来，它们之间也不能交互



1950年前：没有网络的时代

ENIAC

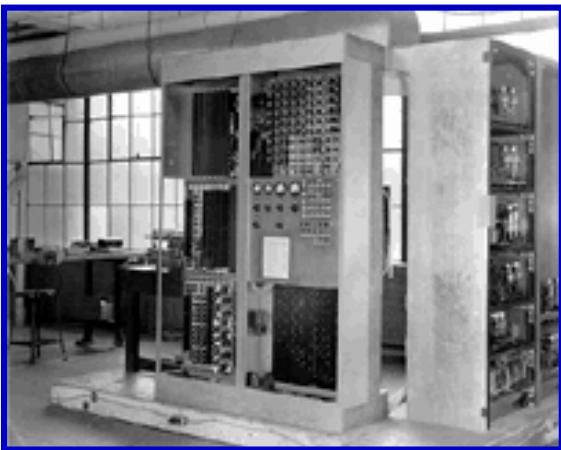


IBM S/360



体积庞大、
价格昂贵的计算成本
数据资源不能共享

EDVAC



DEC PDP小型机



1954年：终端出现

- 1954年，发明了收发器（transceiver）终端
 - 通过电话线传输，将打孔卡片上的数据发送到远地计算机上并接收结果



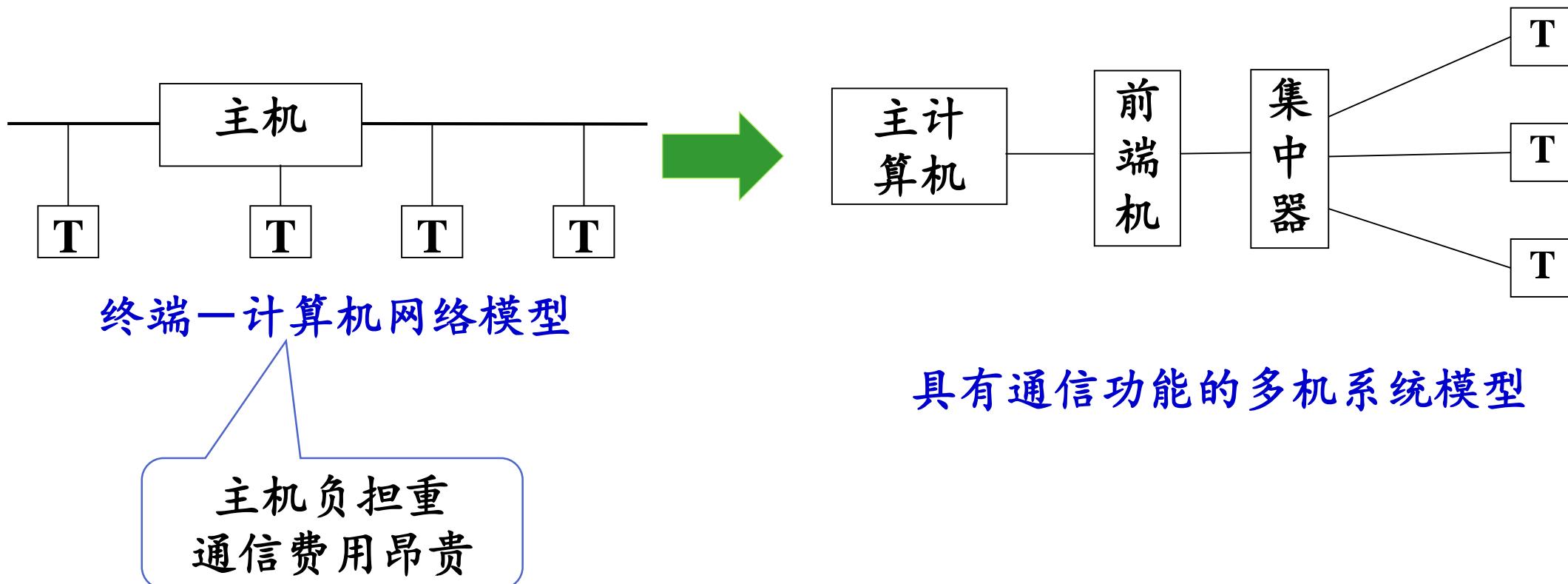
- 发明了电传打字机（teletype）
 - 用户在打字机上输入程序传递到计算机，打字机接收计算结果并打印出来
- 就是计算机网络的基本原型，星型拓扑结构（topology）



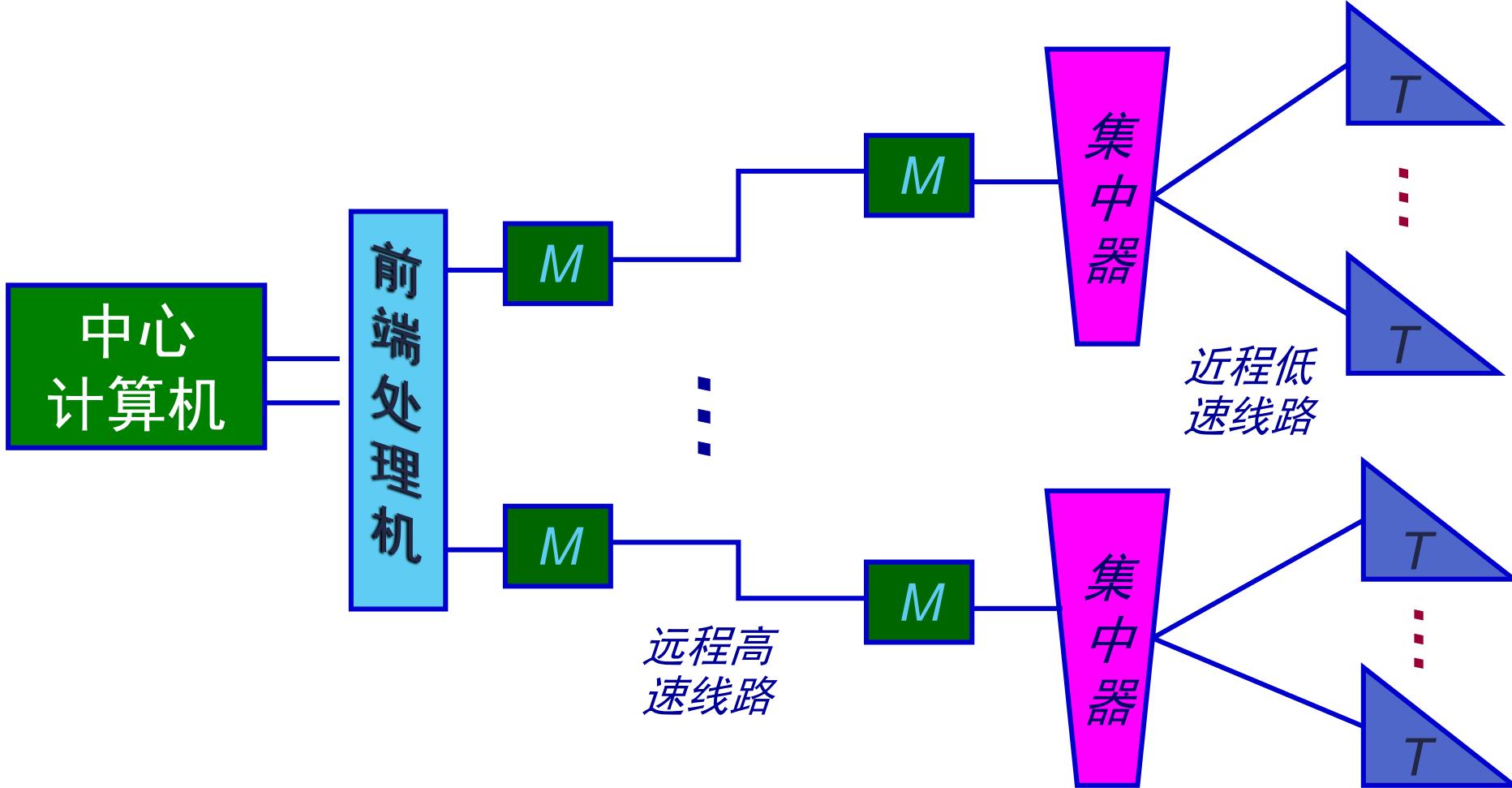
● 计算机
● 终端

50-60年代：计算机网络雏形

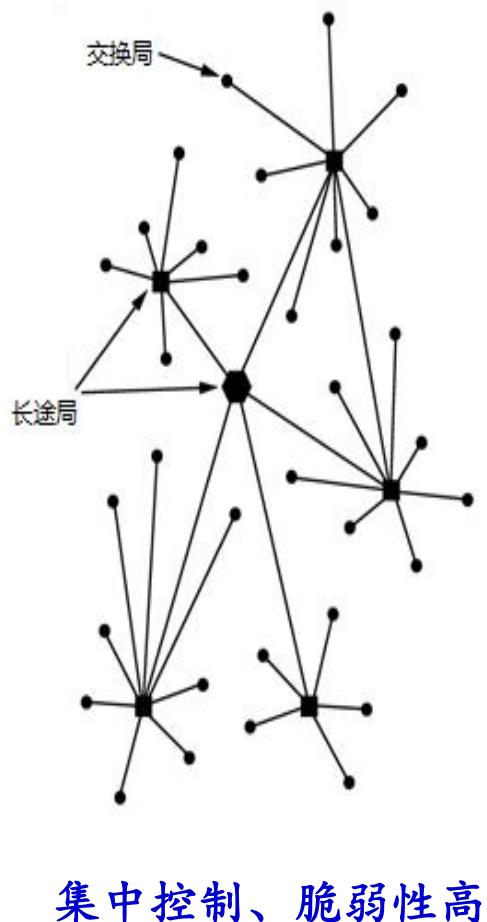
- 第一代计算机网络是由主机--通信线路--终端组成，算是计算机网络的“雏形”，多个用户可以共享资源服务



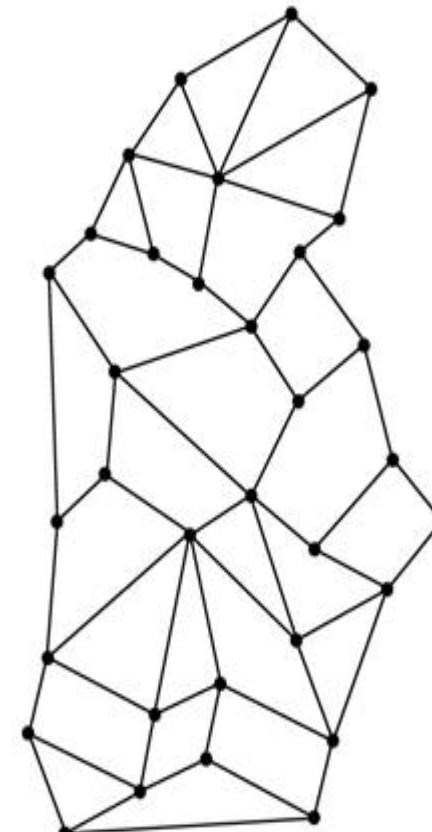
面向终端的计算机网络



1969年：冷战产物ARPANET



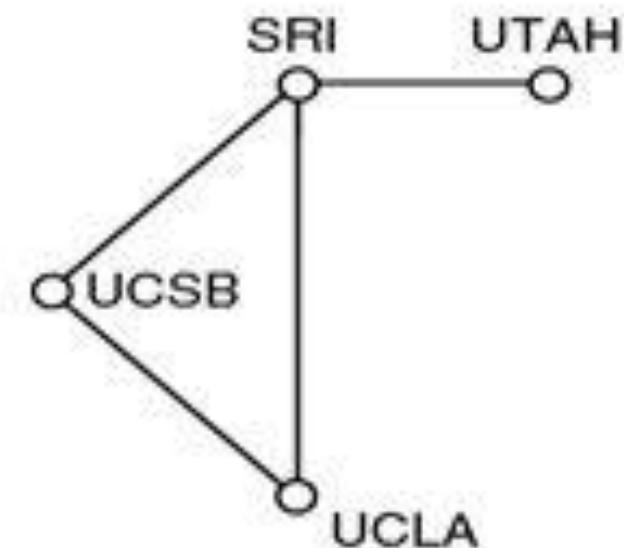
- 1960年左右，冷战高峰期，美国国防部希望建立一个命令和控制网络，即使在核战争的情况下也能够工作
- 为此，美国国防部下属的高级研究计划署（ARPA, Advanced Research Project Agency）筹措建立APRANET
- 不采用传统电话网的集中式结构，提出了分组交换技术的概念



Paul Baran的网络解决方案，提出了分组交换技术

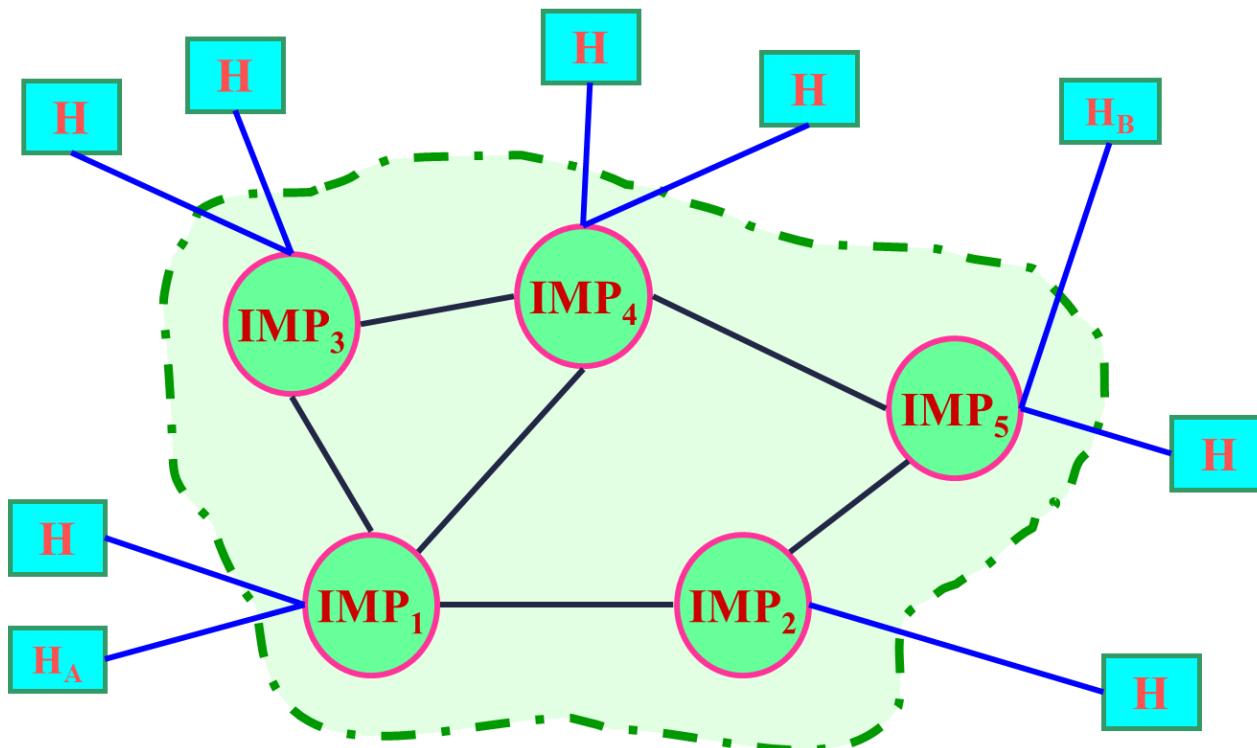
1969年：冷战产物ARPANET

- ARPA通过项目合同的方式，招募了技术思想比较活跃的四所大学来完成项目
- 1969年，在UCLA、SRI、UCSB和UTAH建立了有四个节点的实验网络



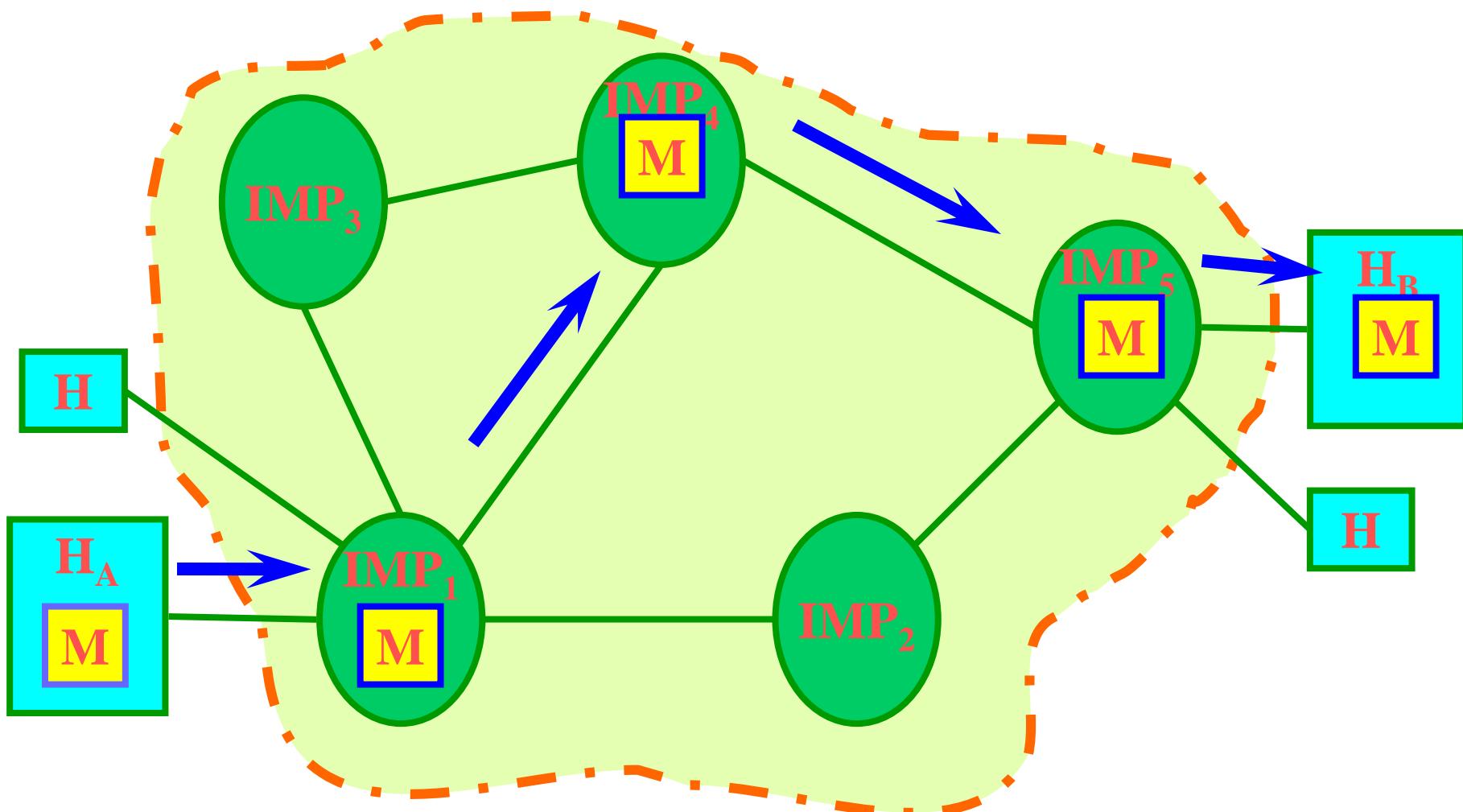
ARPANET：体系结构

- ARPANET的特征是采用分组交换技术实现计算机与计算机之间的通信，使计算机网络的结构、概念都发生了变化，形成了通信子网和资源子网的网络结构



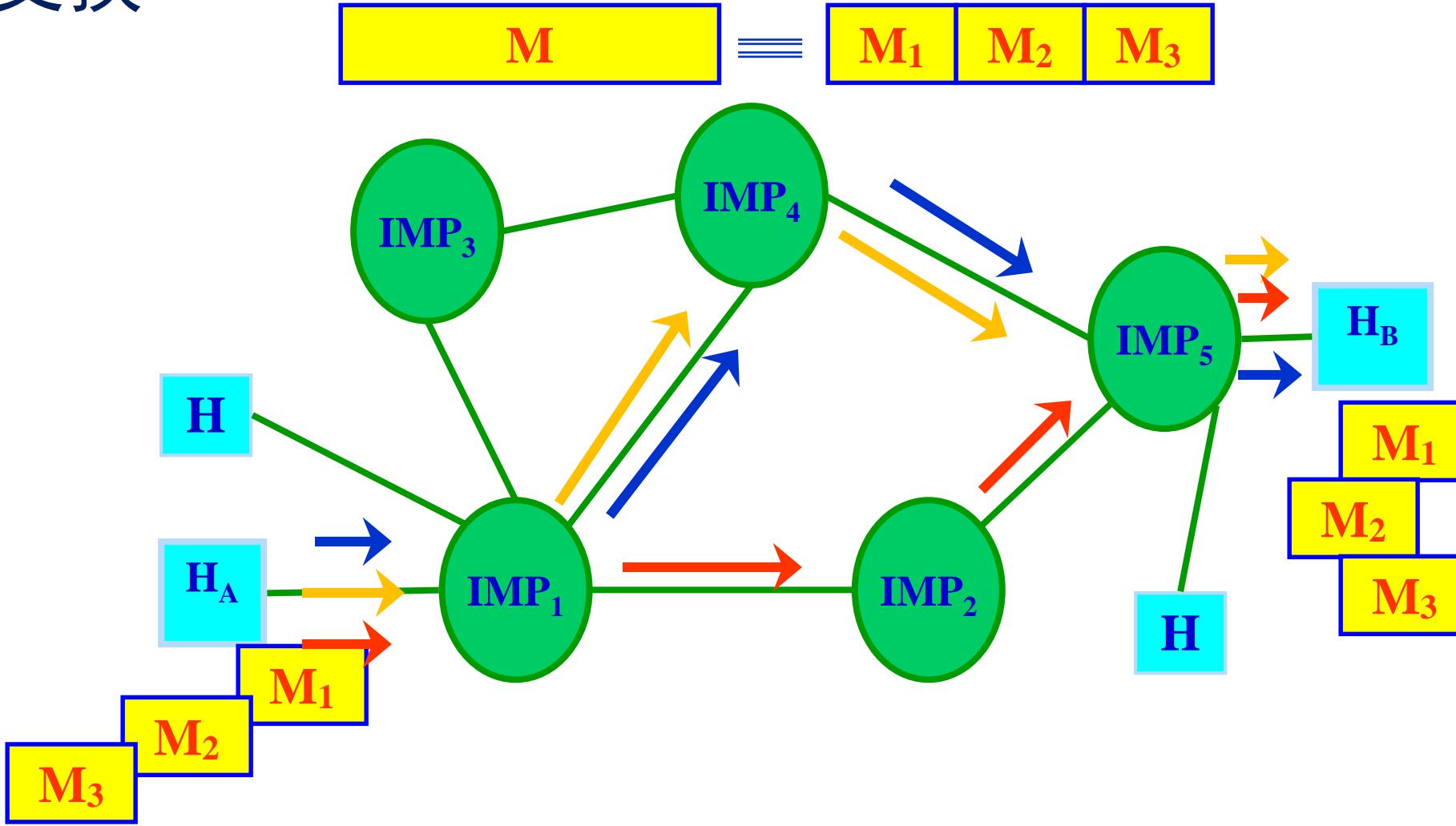
ARPANET：存储转发

- 传送方式 — Store and Forward 存储转发



ARPANET: 分组交换

- 分组交换



ARPANET：核心思想

- 组成元素

- IMP(Interface Message Processor)接口报文处理机
- 主机 H(Host)
- 分组 Packet

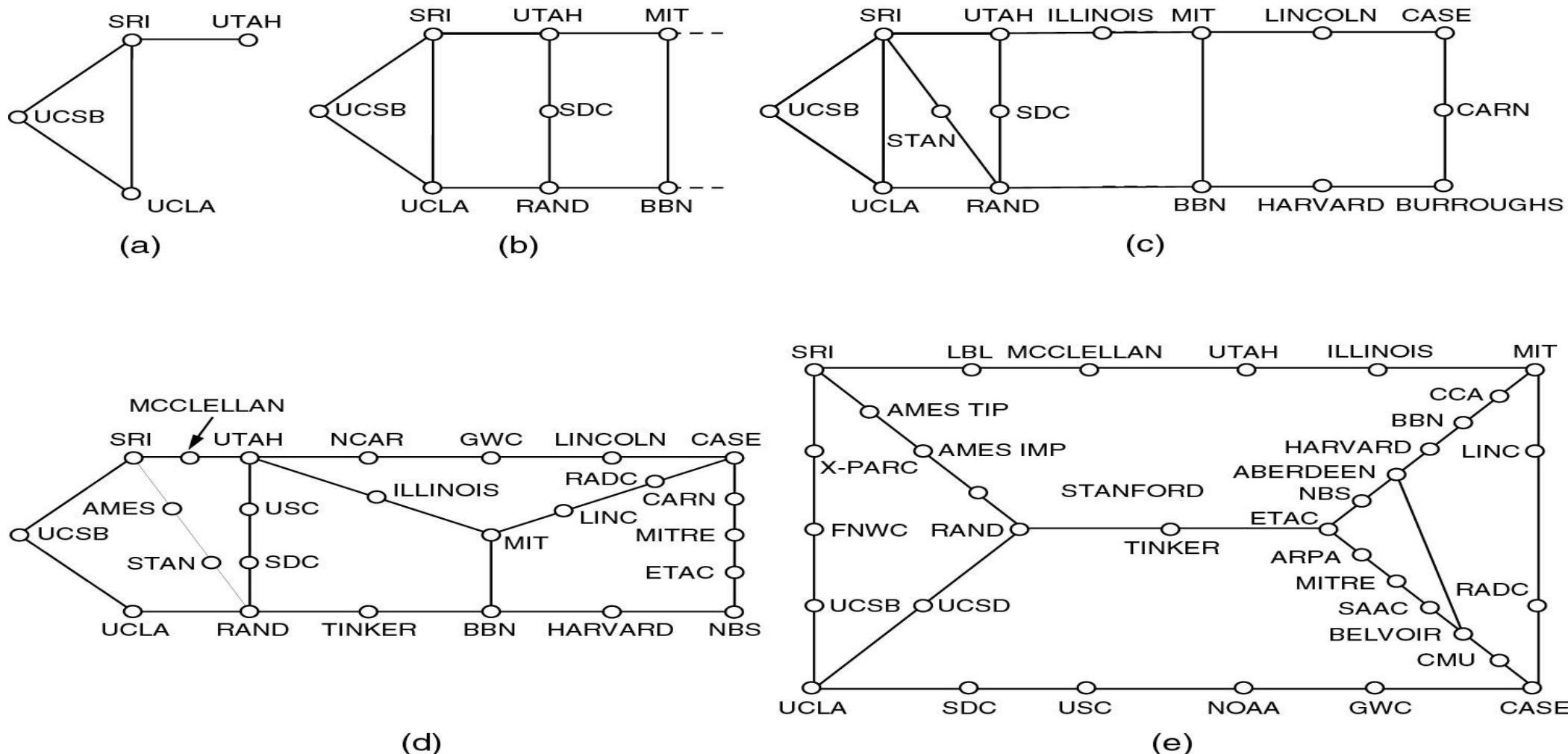
- 传送方式

- Store and Forward 存储转发

- 网络划分

- 通信子网、资源子网

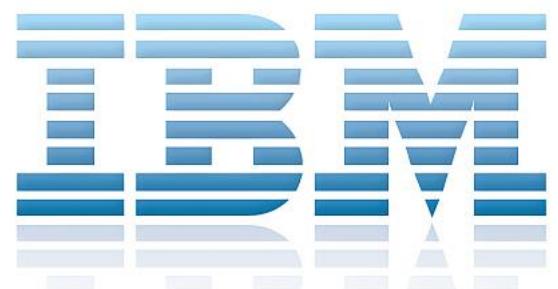
ARPANET：迅猛扩张



(a) 1969年12月； (b) 1970年7月； (c) 1971年3月； (d) 1972年4月； (e) 1972年9月

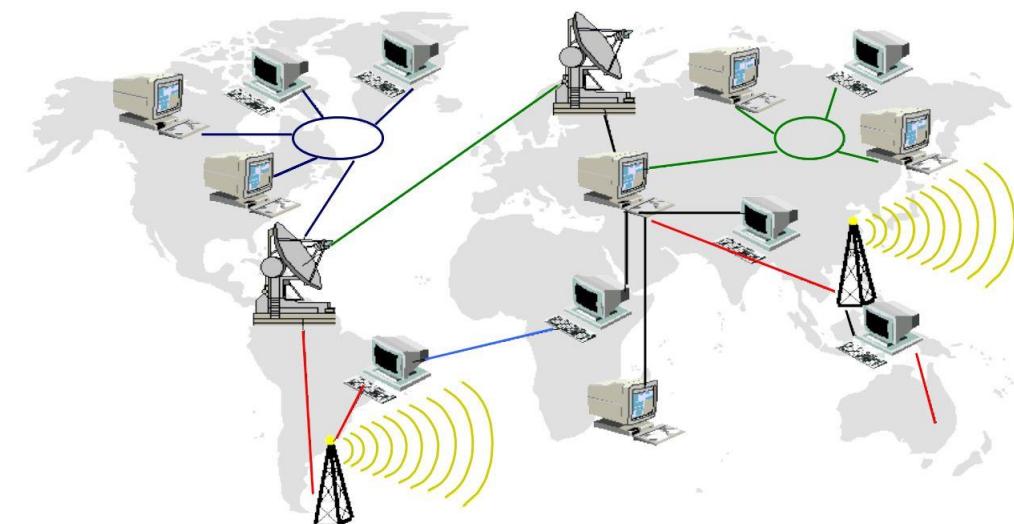
1970年代：网络之间无法互联

- ARPANET出现后，大学、公司和研究部门自行研发了各种不同体系结构的网络
 - IBM公司开发的SNA网络体系结构
 - DEC公司开发的DNA网络体系结构
- 这些网络从技术上到结构上有很大差异，网络与网络之间不能互联



1983年：Internet诞生

- 现代计算机网络互连阶段特征是网络体系结构的形成和网络协议的标准化；采用标准统一的TCP/IP协议，标志着互联网Internet的诞生
- 凡是支持TCP/IP协议的网络，便可以相互进行联接
 - 确定网络体系结构
 - 网络协议的标准化，建立全网统一的通信规则
 - 使计算机网络对用户提供服务



计算机网络的定义

A computer network is a collection of autonomous computers, interconnected by communication channels.

- 计算机网络是由地理位置分散的、具有独立功能的多个计算机系统，利用通信设备和传输介质互相连接，并配以相应的网络软件，以实现数据通信和资源共享的系统
 - 从物理连接上看，由计算机系统、通信链路和网络节点组成
 - 从逻辑功能上看，分成通信子网和资源子网两个子网
- 计算机系统进行各种数据处理，组成资源子网；通信链路和网络节点提供通信功能，组成通信子网



安全的逐步变革

- 在广泛使用数据处理设备之前，主要依靠物理和行政手段保证信息安全
 - 物理手段：将文件锁起来；行政手段：对人员的检查制度
- 信息安全的重大变革之一：计算机的应用
 - 需要自动工具保护存在计算机中的文件和信息，计算机安全
- 信息安全的重大变革之二：分布式系统、网络的应用
 - 信息在数据传输、处理和存储过程中需要安全保护
- 网络安全和计算机安全已没有明显的界限

无处不在的网络安全

互联网是重要的社会基础设施

互联网中的攻与防



清华大学 110周年校庆
110th ANNIVERSARY
TSINGHUA UNIVERSITY

互联网是重要的社会基础设施



互联网是重要的社会基础设施

- 互联网连接着商业、政府、教育、军事等社会各行业和部门，计算机网络已经深入到百姓的生活工作、学习和娱乐
- 互联网已经和电话、交通、水、电一样，成为社会重要的基础设施
- 如果互联网的安全可靠运行受到威胁，将会影响人们的工作、学习和生活；甚至影响整个社会的安全和稳定

网络安全问题已成为信息时代人类共同面临的挑战

- CNNIC发布《中国网民信息安全状况研究报告》：

- 整体上，我国信息安全环境不容乐观，有74.1%的网民在过去半年内遇到过信息安全问题，总人数达4.38亿

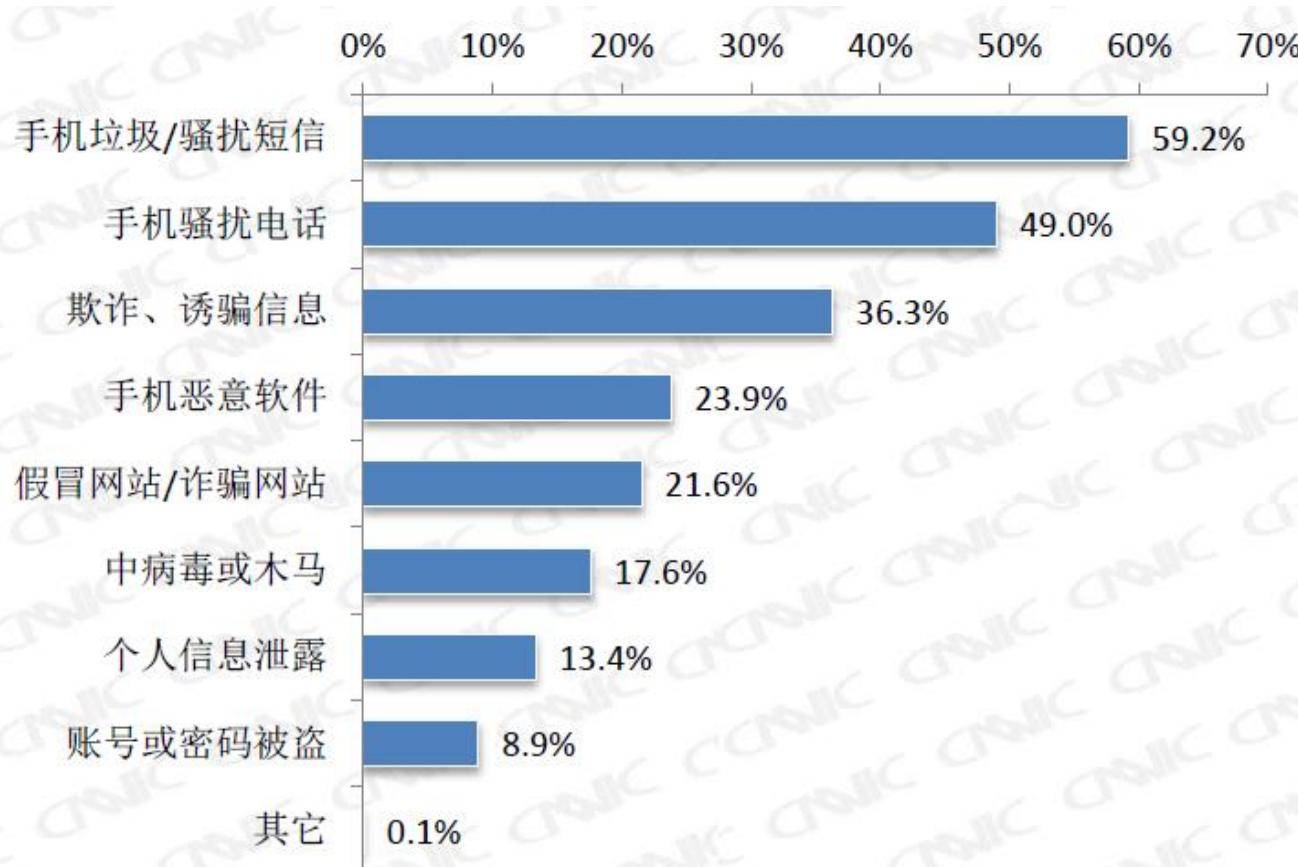


图 2 过去半年中国网民各种安全问题的整体发生率

网络安全问题已成为信息时代人类共同面临的挑战

- 信息安全事件对人们的影响较大
- 据不完全统计，半年内全国因信息安全遭受的经济损失达到了196.3亿
- 在遭受经济损失的人群中，平均每人损失509.2元

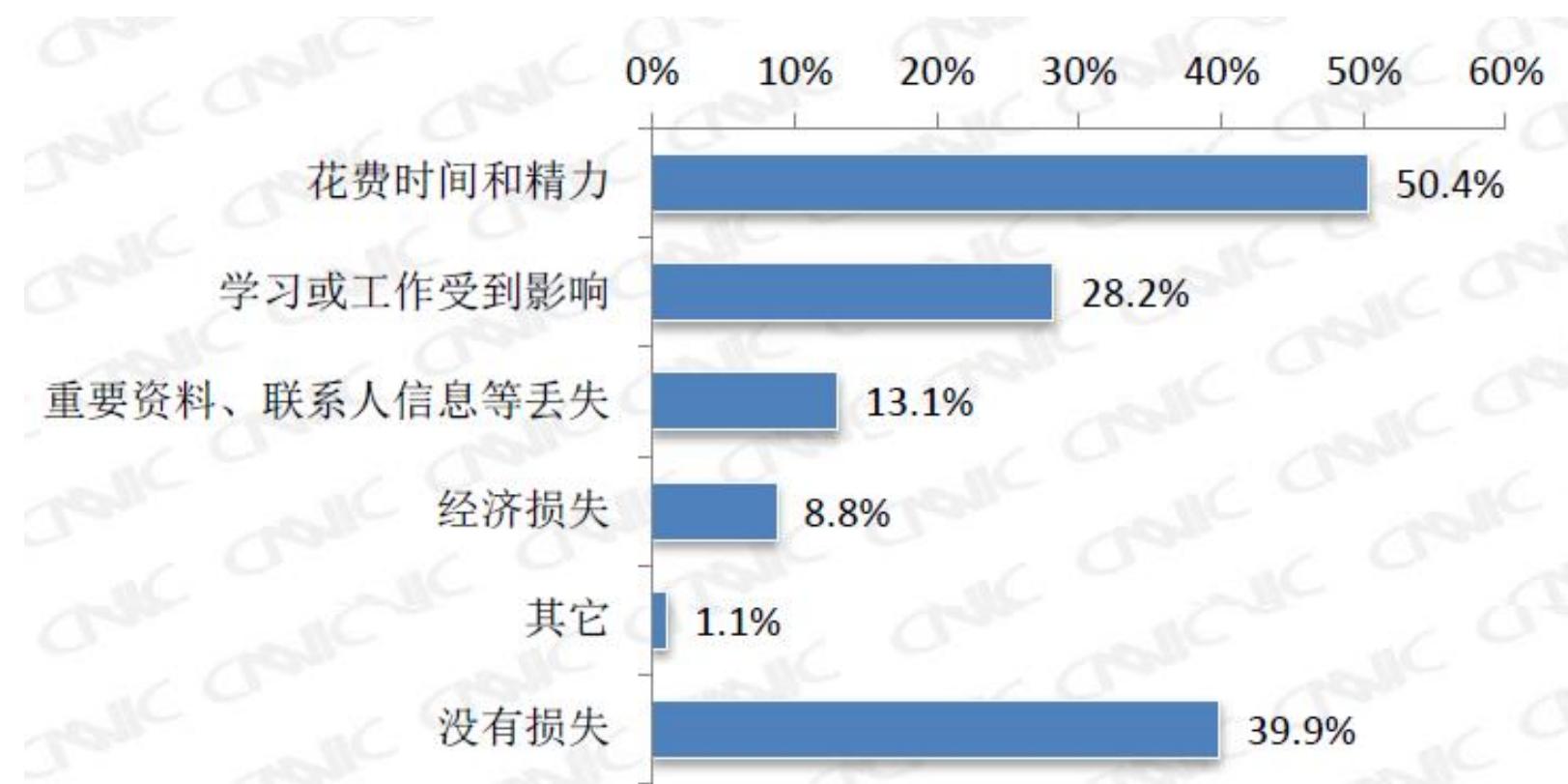
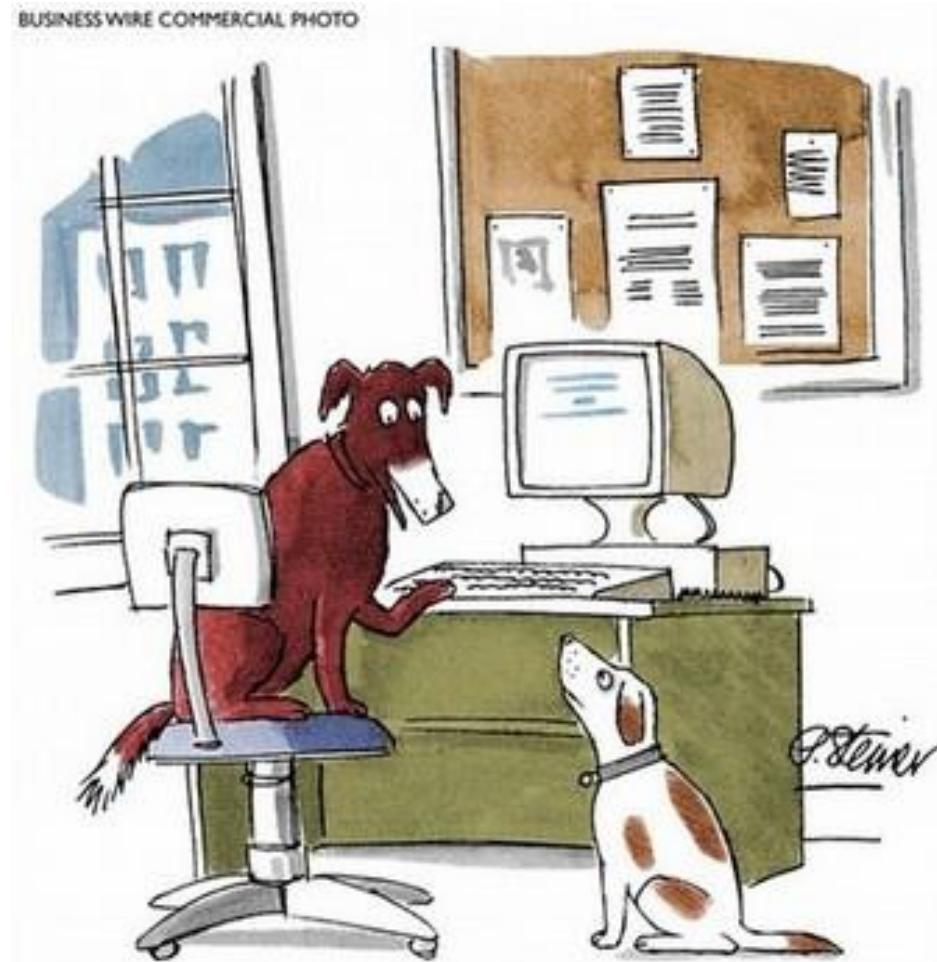


图 4 因安全事件造成的影响

互联网说：“诈骗不是我的错！”

- 骗子自古就有
- 互联网只是让骗子发现了新的行骗途径



On the Internet, nobody knows you're a dog.



清华大学 110周年校庆
110th ANNIVERSARY
TSINGHUA UNIVERSITY

互联网中的攻击



黑客“帝国”

- 互联网发展到今天已经与我们的生活息息相关，如今的互联设备上保存了大量的重要信息：银行账户、个人隐私、行业前沿技术等
- 随着互联网的发展，与互联网安全有关的黑客产业也在不断发展完善，逐步从个人单打独斗发展成现在的分工精细，上下游配合的产业链模式
- 每天在全球黑客产业网络中流转的交易额数以亿计，“年产值”已经过千亿，给企业和用户带来的危害不可估量

黑客“帝国”

- 第一代黑客的目的是验证技术
- 第二代黑客大多数是为了炫耀技术
- 但是随着互联网经济的发展，黑客的目标只有一个“盈利”，整个黑客产业也发展得越来越完善
- 就像组织严密的黑帮一样，网络黑客产业如今已经商业化得非常成熟，拥有很多条产业链
 - 其中对个人用户危害最大的是诈骗地下产业链
 - 其他还有暗链地下产业链、拒绝服务地下产业链等

争夺“信息”资产

- 整个黑客产业都是围绕着用户存放在网络上的数据信息展开的，到底哪些数据信息是我们需要保护的呢？
 - 网络帐号
 - 个人信息
 - 隐私信息
 - 与现实财产有关的信息
 - 在线银行的帐号、银行卡号、支付宝帐号等
 - 其他有用的数据信息
 - 包括各种存储在网络及系统中的文档、数据信等

窃取途径和攻击技术

- 窃取途径：

- 数据在网络传输过程中被窃取
- 数据存储在自身系统上被恶意软件（木马病毒）窃取
- 数据存储在网络系统上的数据被恶意攻击者通过攻击窃取
- 用户被钓鱼，自己泄漏的

- 攻击技术：

- 基于缺陷（漏洞）的攻击
- 中间人攻击
- 病毒木马
- 蛮力破解
- 社会工程学攻击
- 拒绝服务攻击

诈骗地下黑色产业链的分工

产业链最顶层——漏洞挖掘

- 研究和挖掘操作系统等各类系统的**程序漏洞**，并贩卖漏洞信息；在产业链最顶层，具有很高的知识含量

产业链第二层——代码编写

- 编写漏洞利用代码、**编写病毒程序**，贩卖木马病毒程序
- 属于产业链的第二层，从业者需要具备较高的编程技巧

产业链第三层——信息窃取

- 利用攻击代码去攻击网站系统，利用病毒去攻击普通用户，窃取大量的用户敏感信息；
- **蛮力破解、中间人攻击、拒绝服务攻击、病毒等**

产业链第四层——信息贩卖

通过网络贩卖第三层获取的用户信息；属于产业链的次底层，从业者无需专业知识，只需掌握基本的网络使用技巧

产业链第五层——窃取诈骗

- 利用买来的或者掌握的用户信息对用户及其身边的人进行诈骗；产业链的最底层，从业者无需任何网络专业知识，能够给用户带来直接经济损失：**社会工程学范畴**

信息窃取攻击1：蛮力破解

- 蛮力破解攻击 (brute-force attack) 使用数字和字母的任意组合，猜出用户名和口令
 - 口令有规律且比较短、多个系统共用一个口令的都容易被蛮力破解
- 蛮力攻击往往需要花费大量的时间，并且攻击的结果却往往不理想，为了提供攻击的成功几率，会衍生出字典文件
 - 将一些人们常用的密码组合作为探测口令，大大提高了攻击的效率
- 撞库攻击
 - 攻击者可以用获取的用户名和密码去尝试登录其它更大型的信息系统，这种攻击属于蛮力破解中的**撞库攻击**；如果用户在两个信息系统中使用了相同的用户名和密码，就会导致被攻击成功

信息窃取攻击2：中间人攻击

- 中间人攻击：在两个受害者网络链路之间进行数据监听和数据篡改的攻击方式
- 中间人攻击包括两部分：数据监听和数据篡改
 - 数据监听：因为网络中的数据都通过链路传输，因此可以获取用户与信息系统交互的相关数据信息
 - 数据篡改：在获取了链路中的数据信息后，攻击者还可以实时修改这些数据，欺骗链路两端的用户及信息系统

信息窃取攻击3：拒绝服务攻击

- 拒绝服务攻击：就是企图通过使计算机崩溃或把它压跨来阻止提供服务，一般是针对重要的大型网站的攻击行为
- 拒绝服务攻击是最容易实施的且最为有效的攻击行为，也是目前网络上存在最多的攻击
 - 用户一般不会直接成为拒绝服务攻击的目标，但是拒绝服务攻击会直接影响网络的可用性
- 常见的拒绝服务攻击有：
 - SYN洪水(SYN flood)、UDP洪水(UDP flood)、DNS反射攻击

信息窃取攻击4：病毒（恶意软件）



- 病毒作为一段程序想要在用户的系统上运行需要借助一定的传播手段，大多数时候会利用系统及软件的漏洞偷偷的在系统上运行，另一些情况则是伪装成正常程序欺骗用户来运行
- 病毒会通过以下这些途径进入系统：
 - 网络浏览
 - 电子邮件
 - 移动介质
 - 网络下载



清华大学 110周年校庆
110th ANNIVERSARY
TSINGHUA UNIVERSITY

互联网中的防守





常用的安全防护技术

- 加解密技术

- 对网络中的数据进行加密，降低中间人攻击带来的风险

- 访问控制和身份认证

- 有效的阻止非法的访问，让合法的用户能够执行相关操作

- 防火墙技术

- 以墙的模式阻挡了大部分外部来的非法请求

- 防病毒技术

- 能够识别病毒、木马、蠕虫等程序，并阻止其在系统上运行

- 补丁技术

- 能够有效的修补系统及软件中的漏洞



揭开现象看本质

加密之王Enigma：制造者和破译者



清华大学 110周年校庆
110th ANNIVERSARY
TSINGHUA UNIVERSITY

你应该知道的安全大师

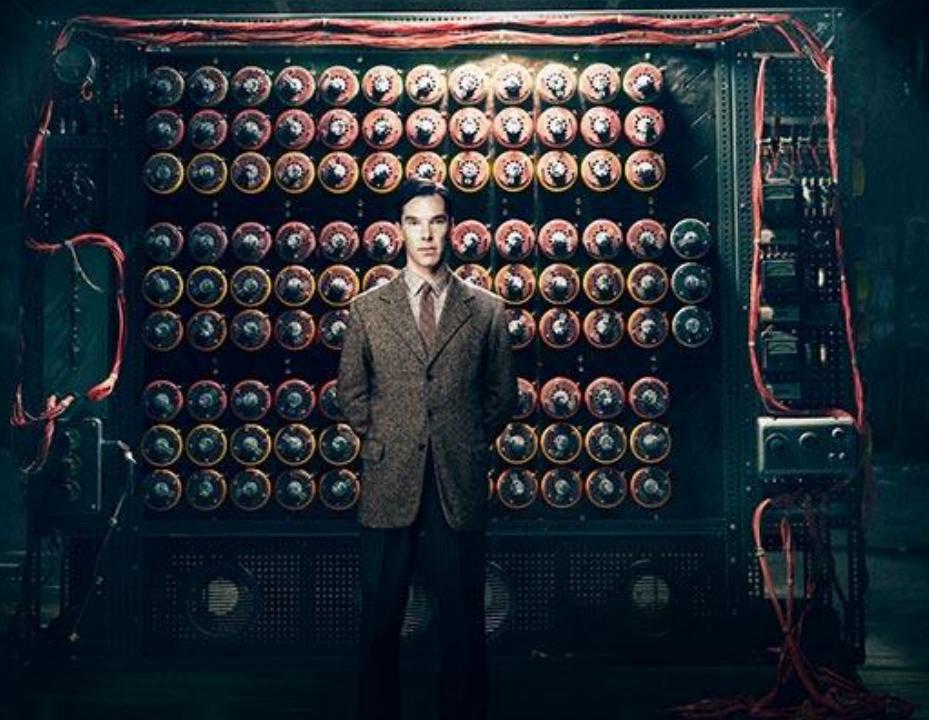
Enigma: 制造者和破译者

Arthur Scherbius

Alan Mathison Turing



THE TRUE ENIGMA
WAS THE MAN WHO CRACKED
THE CODE



BENEDICT CUMBERBATCH KEIRA KNIGHTLEY
THE Imitation Game

IMDb 7.8
Rotten Tomatoes 88%
Metacritic 75/100

豆瓣电影
danlan.org

8 项2015年第87届奥斯卡金像奖提名

最佳影片 最佳男主角 最佳女配角 最佳改编剧本
最佳剪辑 最佳导演 最佳原创音乐 最佳艺术指导

$S_A = \sqrt{p(p-a)(p-b)(p-c)} = p \cdot r \cdot b \cdot Y$

$\sin \alpha - \sin \beta = 2 \sin \frac{\alpha - \beta}{2} \cos \frac{\alpha + \beta}{2}$

$\log_b a = \frac{\log_a a}{\log_a b}$

$x = (-1)^k \arcsin(\alpha + \beta)$

$f(x) = \lim_{\Delta x \rightarrow 0} \frac{f(x + \Delta x) - f(x)}{\Delta x}$

5 项2015年第72届美国电影金球奖提名

剧情类最佳电影 剧情类电影最佳男主角 最佳女配角 最佳剧本 最佳原创配乐



模仿游戏
THE IMITATION GAME

7月21日 开启战争密码

英国惠威(C)影业公司 出品

中影电影集团公司 执印

华语电影发行有限责任公司 发行

长春电影译制片厂 译制

本尼迪克特·康伯巴奇
《星际迷航》
凯拉·奈特莉
《加勒比海盗》

Arthur Scherbius



Alan Mathison Turing

1918年，Enigma诞生

- 1918年，德国工程师Arthur Scherbius（阿瑟·谢比乌斯）申请了他设计的一种使用转子的密码机专利，这就是现代密码学历史上最出名的加密机Enigma（德文：谜）
- 但是Enigma在最初销售的时候，没有人对它感兴趣；不过随后英国政府发表了两份关于一次大战的文件使得德国军队开始对Enigma兴趣大增



1923年，两份重要的文件

- 《世界危机》，温斯顿·丘吉尔
 - 提到了英国和俄国在军事方面的合作，指出俄国人曾经成功地破译了某些德军密码。使用这些成果，英国的40局能够系统性地取得德军的加密情报，而德国几乎是在十年之后才知道这一真相
- 英国皇家海军发表的关于第一次世界大战的官方报告
 - 其中讲述了在战时盟军方面截获并破译德军通讯所带来的决定性的优势：由于无线电通讯被英方截获和破译，德国海军指挥部门就好象是把自己的牌明摊在桌子上和英国海军较量

1926年，Enigma被装备到德国军队

- 为了避免再一次因为文件被敌方破译，德军对阿瑟的发明进行了可行性研究，最终得出结论：必须装备Enigma这种加密机
- 1925年开始，阿瑟的工厂开始系列化生产Enigma，次年就装备到德军；同时还开始了Enigma商用型号的生产
- 之后十年，德国军队大约装备了三万台Enigma，使得德军在二战初期时，通讯的保密性在当时世界上无与伦比
- Enigma在的希特勒灭亡中同样扮演了重要角色

1929年

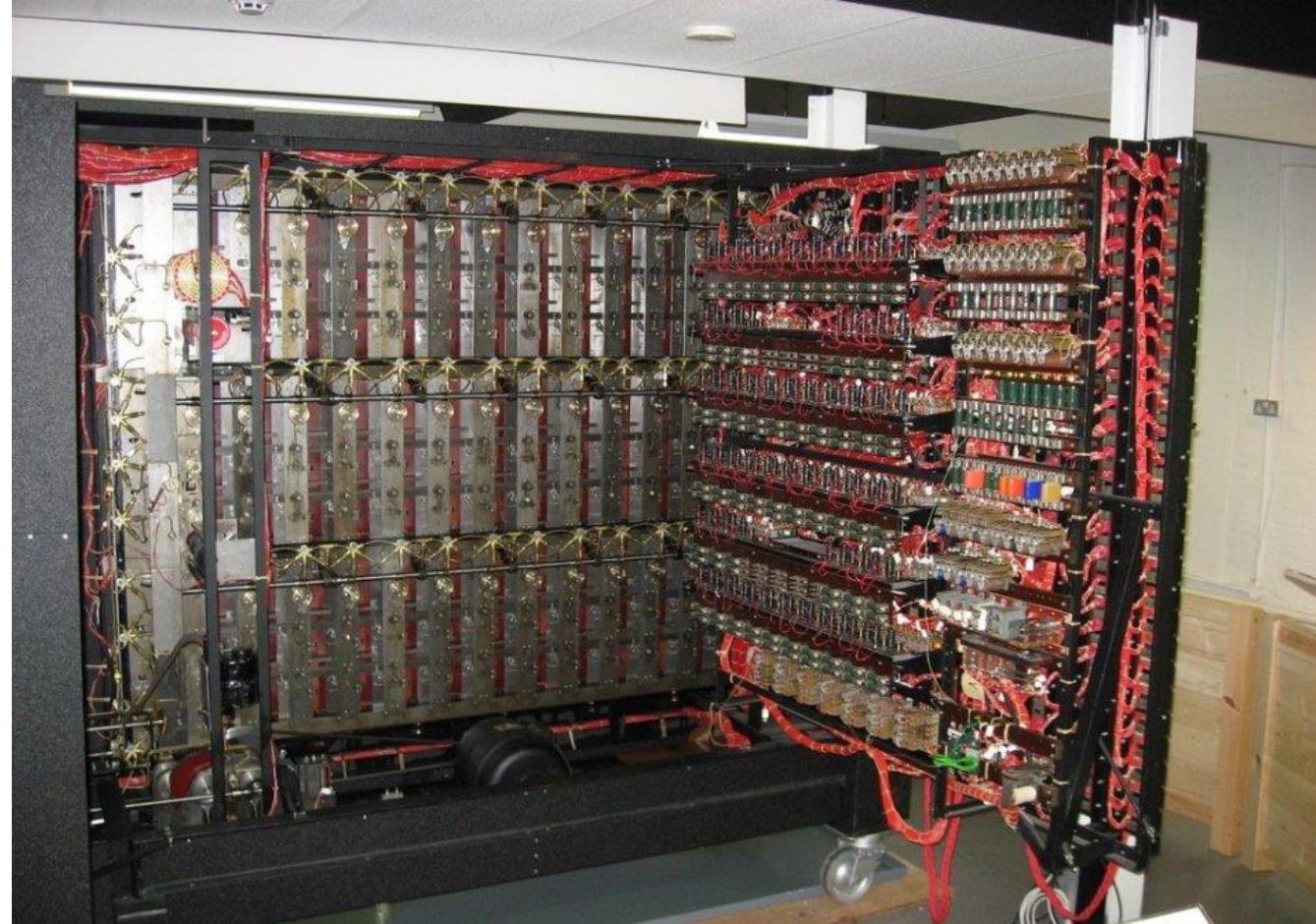
- 阿瑟于1929年5月13日死于内脏损伤



1929年

- 1929年，一位名叫Alan Mathison Turing（阿兰·麦席森·图灵）的17岁英国少年开始研究爱因斯坦的相对论，开始了他的数学生涯
- 在二战期间，图灵凭借着他的天才设想设计出了Enigma的破译机Bomber
 - Bomber主要由继电器构成，用了80个电子管，由光电阅读器直接读入密码，每秒可读字符2000个，运行起来咔嚓咔嚓响
 - 至今没人能搞懂图灵究竟如何指挥它工作，但是它确实能够屡次破译Enigma的秘密，让二战中的德国飞机和舰船一再落入圈套，死无葬身之地

Bomber: Enigma的破译机





清华大学 110周年校庆
110th ANNIVERSARY
TSINGHUA UNIVERSITY

加密之王Enigma



Enigma：二战中最大的军事秘密

- 1939年爆发第二次世界大战，历时6年，60多个国家和地区参战，波及20多亿人口，战争交战各方共动员军队1亿多人
- 二战中最大的军事秘密，除了原子弹外，就是纳粹德国的核心加密机——Enigma
 - 在这场人类有史以来最惨烈的战争中，决定最后战争命运走向的竟然是几台机器和制造它们的天才数学家们

Enigma的工作原理

- Enigma是一种转轮式密码机，原理并不复杂，但在第二次世界大战之前要破解它却基本上是不可能的
- 从外表看起来，Enigma似乎跟普通的打字机别无二致，通常有三个部分组成：键盘、转轮和显示器
 - 为了让密电尽量简短和难以破译，Enigma的键盘没有空格和标点符号
- Enigma使用的加密方法叫做代换密码算法（Substitution cipher）

转轮机

- 为了防止字频统计，阿瑟发明了Enigma最关键的加密部件——转轮机（Rotor machine）
- 转轮机是会自动转动替换对应字母的设备，单表代换密码变成多表代换密码，强度大大增加
 - 当在Enigma键盘上一个键被按下时，相应的密文在显示器上显示，转轮的方向就自动地转动一个字母的位置
 - 例如，当第一次键入a时，信号通过转轮中的连线，灯D亮起来，放开键后，转轮转动一格，各字母所对应的密码就改变了；第二次键入a时，它所对应的字母就变成了H；转轮又转动一格，第三次键入a时，灯K亮起来

反射器

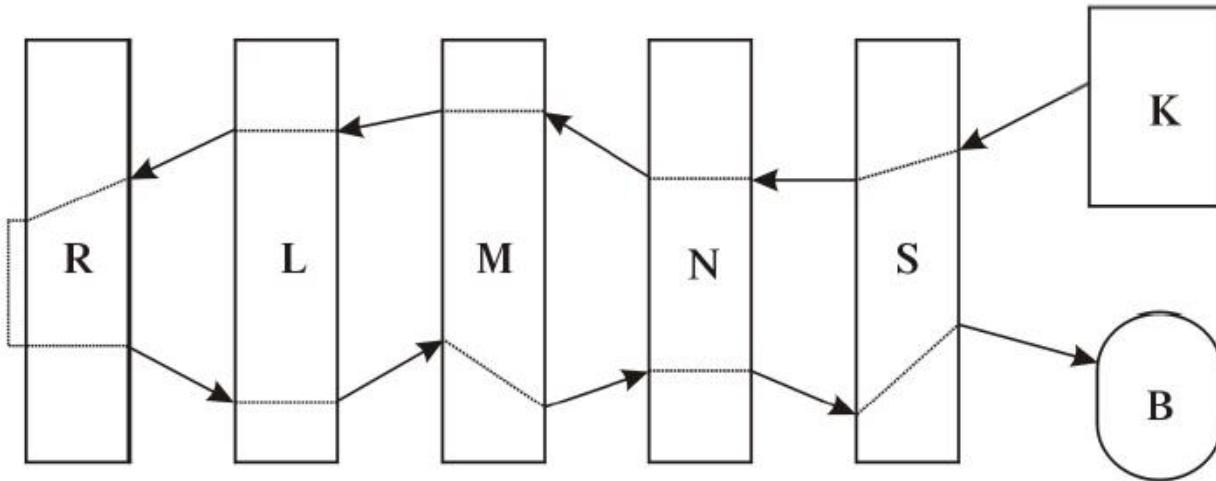
- 在此基础上，阿瑟更是十分巧妙地在三个转轮的一端加上了一个反射器
 - Enigma把键盘和显示器中的相同字母用电线连在一起；反射器和转轮一样，把某一个字母连在另一个字母上，但是它并不转动
 - 事实上它只是一个巧妙的开关：当一个键被按下时，通过三个转轮连成的一条线路，然后经过反射器再回到三个转轮，通过另一条线路再到达显示器上
- 反射器虽然没有像转轮那样增加可能的不重复的方向，但是它可以使译码的过程和编码的过程完全一样，大大的提高了使用的简洁性

Enigma的工作过程

- 开启一台Enigma，首先调节Enigma三个转轮方向，使它们出于初始方向
 - 转轮的初始方向就密匙，这是收发双方事前就预先约定好的秘密
- 按照明文敲打键盘，在Enigma的显示器中，每个被键入的字母的密文都依次闪亮并被记录下来，接着它把密文通过电报传出去
- 接收在接收到密文电报后，打开同样的Enigma，调节好三个转轮的初始方向，通过键盘键入密文，明文就依次显示在屏幕上，并被记录下来

Enigma密码机加密原理

Enigma M3型密码编码路径图



- **N、L、M**为**3**个不同的滚轮
- **R**为反射器
- **S**为接线板
- **K**为键盘
- **B**为灯板

Enigma: 滚轮和反射器的设置

N	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
N0	B	D	F	H	J	L	C	P	R	T	X	V	Z	N	Y	E	I	W	G	A	K	M	U	S	Q	O
N1	D	F	H	J	L	C	P	R	T	X	V	Z	N	Y	E	I	W	G	A	K	M	U	S	Q	O	B
N2	F	H	J	L	C	P	R	T	X	V	Z	N	Y	E	I	W	G	A	K	M	U	S	Q	O	B	D

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

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

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

Enigma举例

- 假设滚轮的顺序为N、L、M，而三个滚轮的初始位置为AAA，接线板上不用任何接线。试求输入明文为“AA”，则密文为“DH”。
 - 从键盘K按下第一个明文字母“A”，由于接线板无接线，字母“A”保持不变
 - 按键使得滚轮N向前滚动一格(即N1)，滚轮M和L皆保持不变
- 如果解密“DH”呢？

滚轮	字母
N	A→D
M	D→K
L	K→N
R	N→K
L	K→B
M	B→J
N	J→D

滚轮	字母
N	A→F
M	F→I
L	I→V
R	V→W
L	W→N
M	N→T
N	T→H

增加强度

- 三个转轮的初始方向共有 $26*26*26=17576$ 个选择，可以进行蛮力破译
 - 增加转轮个数：体积过大，易用性差
- 阿瑟提出了两个更巧妙的改进
 - 把Enigma的三个加密转轮制作成为可方便自由拆卸的形式，用户可以自行调整顺序
 - 在Enigma的键盘和第一个转轮之间增加了一个连接板，连接板能够让使用者用一根信号线将某一个字母和另外一个字母任意连接，这样这个字母的信号在进入转轮之前就会转变为另一个字母的信号。这种连线最多可以有六根甚至更多

增加强度

- 当然，转轮自身的初始方向，转轮之间的相互位置，以及连接板连线的状况都需要双方事先商定好，并严格保密
- 这样改动的Enigma一共到底有多少种组合加密可能性呢？
 - 三个转轮不同的方向组成了 $26 \times 26 \times 26 = 17576$ 种
 - 三个转轮间不同的相对位置为6种
 - 连接板上两两交换6对字母的可能性数目非常巨大，有100391791500种；
 - 于是总共有 $17576 \times 6 \times 100391791500$ ，大约为一亿亿种可能性



加密之王

- 强大的Enigma让德国军方的加密信心显得无比十足
- 造价却低廉的Enigma却具有如此强悍的加密方式，盟军第一次开始品尝到加密的噩梦
- Enigma成为了战争史上最成功的信息加密之王

<http://enigmaco.de/enigma/enigma.html>



阿瑟和阿兰告诉了我们什么？

加密解密是学习网络安全的
必经之路和坚实基础

计算机网络安全技术



*Activity is the only road to knowledge
Computer Network Security @ 2020Fall*