CISC 181: DIGITAL SOCIETIES

UNIT 7: SOFTWARE SYSTEMS

BROAD DISTINCTION: OS VS APP

- As has been previously noted, early computers could execute only one program at a time.
- As computers became more sophisticated, they became capable of supporting multiple programs. It became expedient to segregate software into two categories:
  - application programs (now commonly called apps)
  - operating systems (OSs)

BROAD DISTINCTION: OS VS APP

- An application program performs some task or set of tasks for the immediate benefit of the user.
- Operating systems…
  - provide environments (user interfaces, or UIs) from which users can start apps;
  - provide apps with services that give them controlled, indirect access to the computer's hardware devices (RAM, disks, printers, etc.) and to the network;
  - with the support of appropriate hardware (e.g., multi-core CPUs)…
    - support simultaneous execution of various parts of programs;
    - support simultaneous execution of entire programs for one or more users.

BROAD DISTINCTION: OS VS APP

- Note that early OSs, notably those for personal computers, may have allowed apps uncontrolled, direct access to hardware and did not support simultaneous execution of multiple processes. More on this later.
- In any case, the distinctions between OSs and apps are weak. For example, many application programs are distributed with every OS. Some of these apps have been travelling with their OSs long enough that users may consider them part of the OS.

OPERATING SYSTEM FAMILIES

- There are many operating systems in use in today's computers. Those you are most likely to encounter have evolved from – or been inspired by – one of two foundational OSs:
  - Microsoft Windows NT, or
  - UNIX.

MICROSOFT'S OPERATING SYSTEMS

EARLY MICROSOFT OSs

- Microsoft's first PC operating system was called MS-DOS, where the MS was short for the company's name and the "DOS" (rhymes with "moss") stood for "disk operating system".
- MS-DOS became famous when it was licensed by IBM for use on its first, very successful desktop personal computer, the IBM PC, released in 1981. IBM called the OS "IBM PC DOS". Most people ended up calling it "DOS".

EARLY MICROSOFT OSs

- The enormous success of the IBM PC line led to a large "PC clone" or "PC compatible" market, and Microsoft licensed MS-DOS to the makers of these machines so that they could run the same software as IBM's personal computers.
- MS-DOS (and PC DOS, by extension) had text-based user interfaces as shown on the screen shot on the next slide. Graphics programs like games or programs with graphical elements like spreadsheet apps were supported but were not integral to the OS.

EARLY MICROSOFT OSs

An IBM monochrome monitor sits on an early PC running PC DOS. Note the two 5.25-inch floppy disk drives. These would have been known as A: and B: (pronounced "A-drive" and "B-drive").
Source.

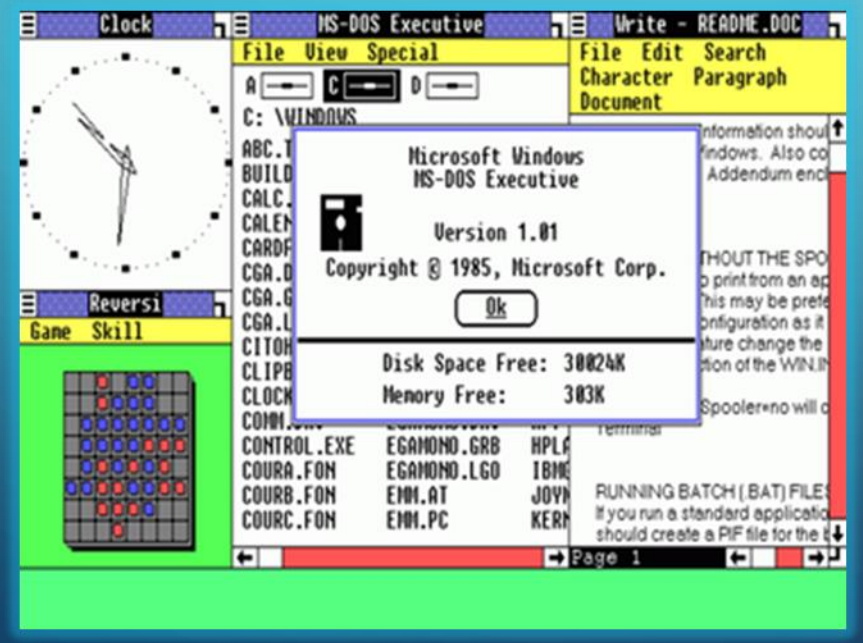
EARLY MICROSOFT OSs

- Microsoft started developing *graphical user interface* (*GUI*) apps for MS-DOS in 1981 but got serious about its efforts in this direction after Apple released its successful Macintosh desktop computer with its mouse and GUI in 1984.

Apple's first Macintosh came with 128KB of RAM.
Source.

EARLY MICROSOFT OSs

- Early versions of Microsoft Windows were apps that a user would typically start from DOS by typing a command ("win") and pressing "Enter." They could be used to start other apps and featured a GUI file manager.



Screen shot of a (very) early version of the Windows app running on MS-DOS. Source.

EARLY MICROSOFT OSs

- MS-DOS, and Windows versions 1, 2, 3, 95, 98, and Me, were all single-task systems. The OS handed complete control of the computer to a single application program which, on completion of some task, was supposed to hand control back to the OS.

EARLY MICROSOFT OSs

- This return of control wasn't guaranteed, and if the app failed in some way it would likely cause the computer to lock up and require a restart. This was done by the user holding down the Ctrl, Alt, and Del (delete) keys at the same time.
- The "Ctrl-Alt-Del" key combination became famous for this reason, and it is how one interrupts the normal operation of the Windows GUI to this day.

WINDOWS NT

- Windows NT, first released in 1993, was written to support simultaneous execution of programs and other processing tasks.
- Microsoft had teamed up with IBM to write such an OS earlier, but the partnership split up in 1990, and IBM was left to develop and market its OS/2 product by itself.
- OS/2 eventually fizzled into irrelevance. NT acceptance got off to a slow start (partly because on the hardware of the day it ran very slowly), but the product ultimately thrived.

WINDOWS NT

- Note that on machines with single processors – and often on machines with multiple cores – NT and other modern OSs permit each running process a *slic*e (short length) of time in which to execute, after which the OS suspends that app's execution while it allows another process its slice of execution time. The time slices are all very short, in human terms, and this rapid alternating between running processes gives an illusion of truly parallel execution. For further reading on this, see https://en.wikipedia.org/wiki/Preemption_(computing).

THE WINDOWS NT FAMILY OF OSs

- The NT name was retained by Microsoft through several major OS updates. The following Windows versions (or *releases*) have evolved from NT, and no doubt contain original NT code:
  - Windows 2000
  - Windows XP
  - Windows Vista
  - Windows 7
  - Windows 8
  - Windows 8.1
  - Windows 10
  - Windows 11

THE WINDOWS NT FAMILY OF OSs

- Most of these came in various "editions" (Home, Home Premium, Professional, Enterprise, Education, etc.). For a complete list, see Wikipedia's entry for Windows NT.
- From the NT days onwards, Microsoft has sold versions of its OS for use on servers, releasing new versions of Windows Server periodically, and roughly in parallel with the releases of personal versions. Like non-server versions of Windows, all are based on NT.

THE WINDOWS NT FAMILY OF OSs

- Windows Server provides specialized services for organizations, including
  - network-wide user authentication (user IDs, passwords) and
  - centralized file storage.
- Windows Server versions parallel most features – including user interfaces – of their contemporary non-server Windows editions.

UNIX, ITS PROGENY, AND ITS IMITATORS

UNIX

- UNIX (or Unix, or UNIX) is an OS that was developed by Ken Thompson, Dennis Ritchie – who also created the C programming language – and others (including Brian Kernighan) while they were researchers at AT&T's Bell Labs in the late 1960s and early 1970s.

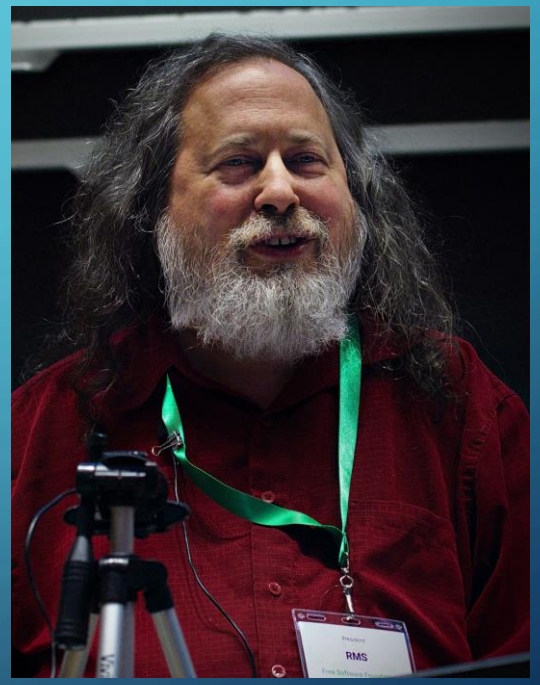
Ken Thompson (left) and Dennis Ritchie.
Source.

UNIX

- UNIX was written in the C high-level language.
- UNIX was created to support simultaneous execution of programs and other processing tasks for multiple users.
- UNIX quickly became a popular OS in research and industry; much less so on personal computers (at the time).

THE GNU PROJECT

- In the early 1980s, Richard Stallman, a programmer at Massachusetts Institute of Technology (MIT), grew resentful at being forced to use the proprietary, pre-compiled software then available to him.
- He felt that someone paying for software should be able to make improvements to it and resented having to purchase executable programs without access to original source code.



Richard Stallman. Source.

THE GNU PROJECT

- In response, Stallman launched the GNU Project, where *GNU* is a "recursive acronym," standing for "GNU's Not UNIX", to encourage the development of an operating system that worked just like UNIX, but used completely new, freely-available, and modifiable, programming code. (Note: "GNU" rhymes with "canoe.")

The GNU Project's gnu logo, designed by Aurelio A. Heckert. Source.

THE GNU PROJECT

- Stallman advocated for *free software*. Its original high-level language source code would be distributed with a program so that the person using it would be free to make changes to it. Any charges from the author of the software would be for making copies available.

THE GNU PROJECT

- To make sure that software developed under the GNU Project lived up to the GNU Project's ideals, Stallman created the GNU General Public License (GPL). This license dictated that any software developed using GNU Project tools, such as the GNU C Compiler (GCC), or any software derived from such software, would also be subject to the GPL and would likewise be freely available, with its source code, and be modifiable.
- Some would contend that the GNU Project was never completed because although much supporting software for the new operating system was developed, the core part of Stallman's proposed OS – the critical part called the *kernel* – never was. (More on that in a couple of slides.)

THE GNU PROJECT

- Stallman ultimately objected to the use of the term *open-source software* that most people now use to describe software distributed with its high-level language source code, as the term does not imply any sort of freedom to modify and reuse code. His disagreements on this and related matters – such as making once-free software proprietary – with people like open-source advocate Eric Raymond led to a schism in the free and open-source movement.
- But Stallman, as noted, doesn't object *per se* to charging for software; the acquisition of software is not necessarily the "free" part of the free software movement. However, much open-source software is also classified as *freeware*, because it *is* given away without charge.

UNIX AND UNIX-LIKE

- Operating systems that duplicate much of the functionality of UNIX are described as *UNIX-like*.
- UNIX and UNIX-like OSs are numerous. Most are based on one of two early creations:
  - Linux, or
  - The Berkeley Software Distribution (BSD, also called Berkeley Unix).

LINUX

- Many computers today run some version of Linux, a free, open-source, UNIX-like OS.
- The Linux kernel was developed by Finnish software engineer Linus Torvalds and released in 1991 when Torvalds was 22 years old.

Linus Torvalds. Source.

LINUX

- There are many hundreds of variants - called *distributions*, or *distros* – of Linux. Popular distros include:
  - Fedora: Distributed by a company called Red Hat. Red Hat makes money by selling corporate-level support for Fedora.
  - Debian: Well-suited for installation on desktop computers.
  - Ubuntu: Developed from Debian. Ubuntu is very popular as a desktop OS for those preferring not to use either Windows or MacOS.
  - Kali Linux: Another Debian-based distro. Fully customizable. Favoured by hackers and security professionals.

THE BERKELEY SOFTWARE DISTRIBUTION

- The Berkeley Software Distribution (BSD), a non-Linux OS, was first developed and released at the University of California, Berkeley (hence the name) in the mid-to-late 1970s.
- It incorporated original UNIX code from Bell Labs so, unlike Linux, it should be considered a true UNIX variant and not just "UNIX-like."
- Bell Labs released its UNIX source code and BSD, like Linux, is open-source, **but it was not released under the GNU General Public License**.

THE BERKELEY SOFTWARE DISTRIBUTION

- In fact, the license under which BSD was distributed makes it possible to reuse the code in both open-source and proprietary, closed-source settings.

THE BERKELEY SOFTWARE DISTRIBUTION

- Taking advantage of the flexible license, Apple co-founder Steve Jobs had BSD developed into a proprietary OS, called NeXTSTEP, after he was fired from Apple and had formed a rival company called NeXT in 1985.
- When Jobs returned to Apple in 1997, NeXT was folded into the larger company, and NeXTSTEP was further developed into what is now known as macOS (formerly Mac OS X).
- Its connection to BSD means that macOS may be considered a true UNIX OS.

MOBILE OSs

- Today's smartphones are computers, and they, too, depend on operating systems for much of their functionality. If an OS has been adapted or written for use on a smartphone, it is frequently categorized as a *mobile* OS.
  - Apple's iPhones and iPads run variants of the company's proprietary iOS mobile OS. According to Wikipedia, iOS is "Unix-like, based on Darwin (BSD)."
  - Most mobile devices today (smartphones and tablets) rely on Google's Android OS, which uses a modified Linux kernel but none of the usual GNU supporting code. The GNU components have been replaced with code developed at Google, at least some of which is based on BSD.

OSs FOR EMBEDDED COMPUTERS

- Devices including appliances and vehicles increasingly rely on embedded computer systems. These systems may be sophisticated enough to warrant having their own operating systems.
- Linux, being free, open-source, and highly customizable, is a popular choice for embedded OSs.

(SOME OF) WHAT OSs DO

MANAGING ACCESS TO THE CPU

- An OS controls programs' access to a computer's CPU, allowing them to do their work while preventing them from monopolizing the CPU to the exclusion of other programs. Programs may be prioritized for CPU access based on how critical they are to the functioning of the computer.

MANAGING ACCESS TO RAM

- An OS manages RAM, loading programs into memory so they can be executed, allotting them data space in RAM, and allowing that space to be reallocated to other programs when their execution is complete.
- The OS also enforces *memory protection*, that is, the RAM allocated to one program or process within a program may be used by that program or process alone while it is running, and another app may not have access to it. In this way, running programs and processes are protected from each other. (Naturally, the OS also takes care that its own share of RAM is protected from other programs.)

MANAGING ACCESS TO THE FILE SYSTEM

- An OS manages the file system, i.e., secondary storage, like hard disks, solid-state drives (SSDs), or flash drives.
- In situations where demand for RAM exceeds the installed supply, an OS might press part of a computer's secondary storage into service as a sort of RAM extension called *virtual memory*. Secondary storage access times are typically much higher than RAM access times, so programs in virtual memory run slowly, but this is usually preferable to having them not run at all or crashing when they exhaust available RAM.

MANAGING ACCESS TO ATTACHED DEVICES

- An OS manages the user interface (typically a GUI) and – with the assistance of other software – devices attached to the computer, like keyboards, mice, touchpads, touchscreens, printers, network connections, etc. The OS also controls programs' orderly access to these devices.

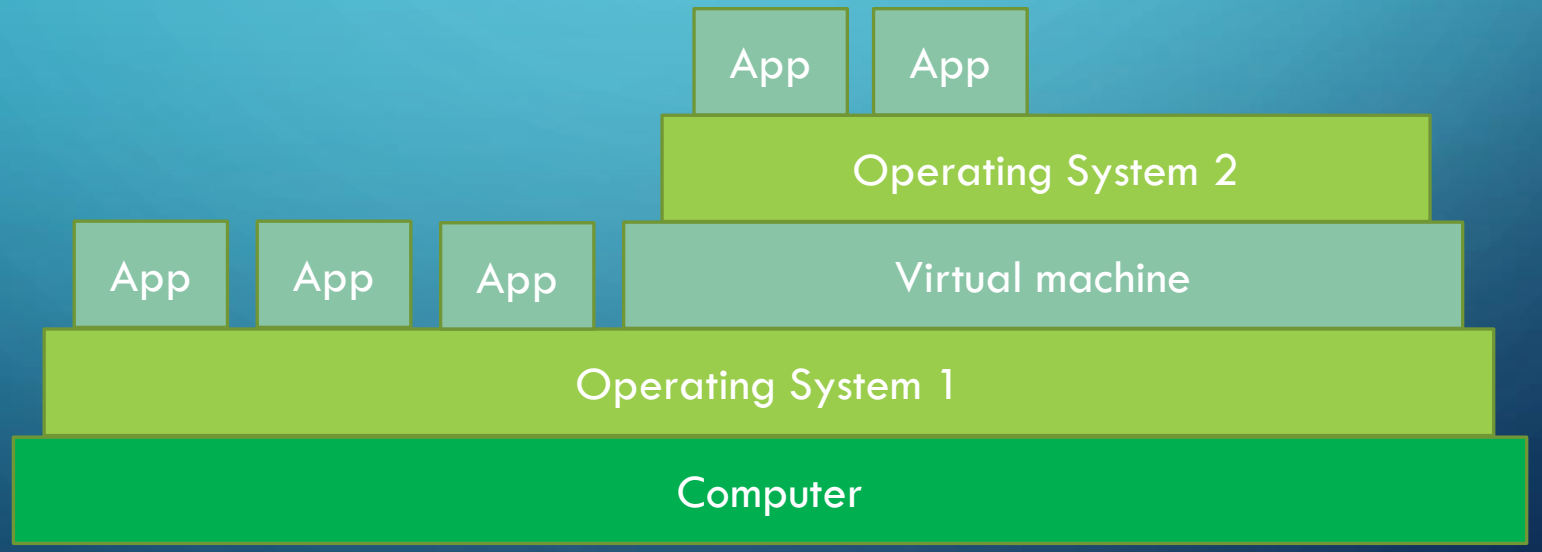
OTHER OS-RELATED STUFF

VIRTUAL MACHINES

- A *virtual machine* (*VM*) is an app that simulates another computer.
- A VM can support "guest" OSs that can then run their own apps.

VIRTUAL MACHINES

- This drawing depicts an operating system running on a computer that is supporting four executing apps, one of which is a VM. The VM is supporting a guest OS which is, in turn supporting two of its own executing apps.



VIRTUAL MACHINES

- A VM can protect an underlying machine and its file system from the misbehaviour of guest apps.
- *Virtual machines* (*VMs*) are also extensively used in software development.
  - A Windows or Mac user could develop Linux software on a Linux VM.
  - A desktop or laptop user could develop and test phone apps on a VM running Android.
  - VMs can simulate remote servers, like web servers, allowing "remote" development to happen entirely on a programmer's machine. This has several advantages, among them the ability to test software on various simulated server configurations without the risk of accidentally interrupting the operation of a real server that people are depending on.

SYSTEM CALLS

- An app, or perhaps a code library being used by an app, requests the services of the system's OS by way of *system calls*. These are standardized software interfaces – like functions – built into an OS.
- System calls handle process requests for many services including
  - secondary storage access;
  - reading from input devices and writing to output devices;
  - receiving or sending information over a network connection.
- The number of system calls available varies by OS, but over 300 is typical.

DEVICE DRIVERS

- A *device driver* is software that provides an interface between a hardware device and the OS that needs to control it.
- Device drivers allow OSs to adapt to changes in the hardware configurations of computer systems.

DEVICE DRIVERS

- For example, when a printer manufacturer like Hewlett-Packard (HP) or Brother introduces a new model with a particular set of features, the company's programmers will simultaneously release drivers for it for various operating systems (MacOS and Windows at a minimum, but often Linux, too).
- The user's OS likely came with a set of drivers for printers that were around at the time of its release, but it won't know about the specialized features of any new model. The driver released by the manufacturer provides the necessary software, thus bridging the gap between the OS and the new printer.

DEVICE DRIVERS

- Thus, for example, when a user asks Microsoft Word to print a document…
  - Word makes a system call to the OS.
  - The OS processes the system call and passes the document to the printer driver for the selected printer.
  - The printer driver encodes the document for the printer and sends the document to the printer for printing.

DEVICE DRIVERS

- Device drivers were, for years, distributed along with the products they supported on optical discs (CDs).
- As optical discs became rarer, a shift was made to downloading drivers from manufacturer's websites. This has the obvious benefit of ensuring the most recent drivers are available and for a variety of OSs.

SUMMARY

IN THIS UNIT WE LOOKED AT

- Software categories
  - Operating systems (OSs)
  - Application programs (apps)
- Microsoft Windows NT and later versions of Windows
- Bell Lab's UNIX
- The GNU Project
- Linux and its distros
- BSD

IN THIS UNIT WE LOOKED AT

- Some of the many roles of an OS
- Virtual machines (VMs)
- System calls
- Device drivers

A reminder that Quiz 4 happens on Friday which is also the due date for Written Assignment 2.

CISC 181: DIGITAL SOCIETIES

UNIT 8: NETWORKING (AND ENCRYPTION)

INTRODUCTION

- We begin a multi-week look at the ties that bind our devices together and allow us to connect in ways that have redefined how societies interact.
- There is much good that has come from these connections, and much that is not so good, too.

INTRODUCTION

- In coming weeks, we'll look at the internet and its apps, including the World Wide Web.
- We'll also look at how these technologies have affected and continue to affect human society.

INTRODUCTION

- In technical terms there is a broad division between the technologies that connect devices on our home, school, and work networks, and the technologies that connect those small networks into a world-wide network (the internet). This week, we'll take a (mildly) technical look at both sorts of connections, focusing mostly on the small networks around us.
- But first, some terminology.

NETWORKING TERMINOLOGY

BANDWIDTH

- *Bandwidth* (also called *digital bandwidth* and *throughput*) is the rate at which a communications system transmits information from one place to another.
- You can think of bandwidth as being the speed of a connection. It is expressed as some number of transmitted bits per second (bps) with units increasing in multiples of a thousand, i.e., Kbps (kilobits – or thousand bits – per second), Mbps (megabits – million bits – per second), Gbps (gigabits – billion bits – per second), or possibly Tbps (terabits – trillion bits – per second).

BANDWIDTH

- Note that internet service providers (ISPs) frequently refer to something quite different when they advertise "bandwidth." Their meaning is what most computer administrators would call a monthly *quota*, that is, the amount of data, typically some number of gigabytes, that your devices may send or receive in a month before your service is deliberately slowed (*throttled*) or additional charges apply.
- So, to your ISP, "unlimited bandwidth" may simply mean that users pay a fixed monthly rate, regardless of how much use they are getting out of their internet connections, or how fast or slow that connection is. We will not use this definition.

LATENCY

- *Latency* or *delay* is the length of time, typically measured in milliseconds (ms), that it takes for a data element to be transmitted between its source and its destination.
- Latency may not affect perceived bandwidth, depending on the reliability of the network being used, but it may become noticeable in other ways. For example, geostationary satellites sitting at altitudes of several tens of thousands of kilometers may provide somewhat reliable bandwidth between two points on earth, but a voice or video call over one may well suffer from noticeable gaps in the flow of conversation owing to the distances involved. This has led, as we shall see, to a different approach to building satellite-based networks.

JITTER

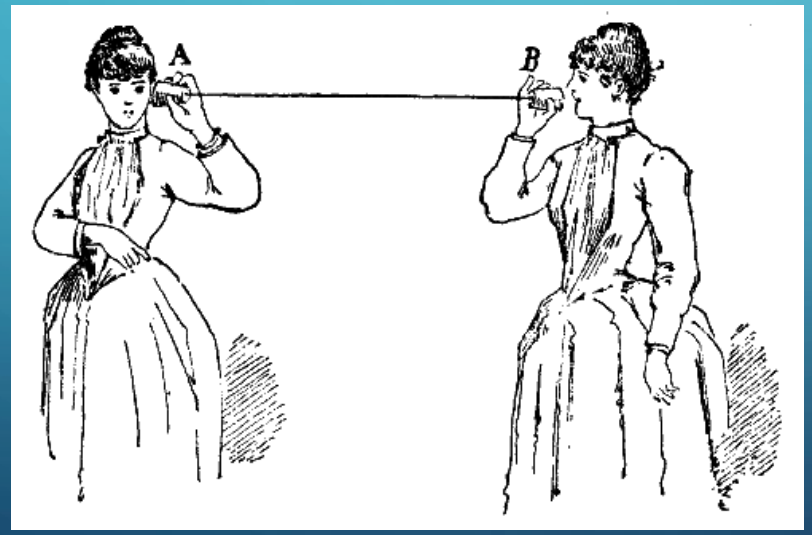
- *Jitter* is a measure of variation in latency. Its effect on bandwidth is usually undesirable, that is, it slows data transmission down.
- Jitter might be caused by competing demands on available bandwidth, defective equipment, electronic interference, weak wireless signals, etc. Some of these degrade the quality of a communications stream. While some forms of communications can tolerate such degradation to a degree (I'm thinking of voice communications, for example, where the listener's brain can compensate for limited levels of distortion), others that rely on accurate reception of data may require occasional retransmissions, thus lowering effective bandwidth.

RANGE

- *Range* is the distance over which information may be reliably sent and received using a specific network technology.
- For example, a home wireless router has an effective range of several dozen metres beyond which there will be a significant drop in signal strength. Its range may be further restricted in some directions owing to interfering objects, such as masonry (bricks and concrete) and metal in walls, floors, and ductwork.

POINT-TO-POINT

- *Point-to-point* communications are those that are restricted to two parties or between a specific source and a specific destination. If a path of communication is used to connect two and only two devices, we'd say those devices have a point-to-point connection.



Point-to-point communication using two cups and a string. Source.

BROADCAST

- In *broadcast* communications, one sender is transmitting to multiple receivers. A familiar example is the radio broadcast. A wireless home router is a radio broadcasting device.
- With programming, it is possible to create virtual point-to-point communications when the underlying network technologies use broadcast communications. This frequently involves the sender's machine encrypting its transmissions in a way that can only be decrypted by the intended recipient's machine. More on encryption at the end of this unit.

LOCAL AREA NETWORKS

- *Local area networks* (*LANs*) are small groups of connected computers and devices. A home network is a LAN. Queen's University has many LANs, some under the direct control of IT Services and others managed by various departments.

OTHER "AREA NETWORKS"

- The LANs at Queen's are connected in what is known as a *campus area network* (*CAN*).
- In a corporate setting, a similar network might be called a *corporate area network* (also a *CAN*).
- CANs may be part of a wider *metropolitan area network* (*MAN*).
- Any network larger than a MAN is a *wide area network* (*WAN*). Arguably, the internet is a WAN.
- Note that the distinctions between these categories is not always clear.

MODULATION

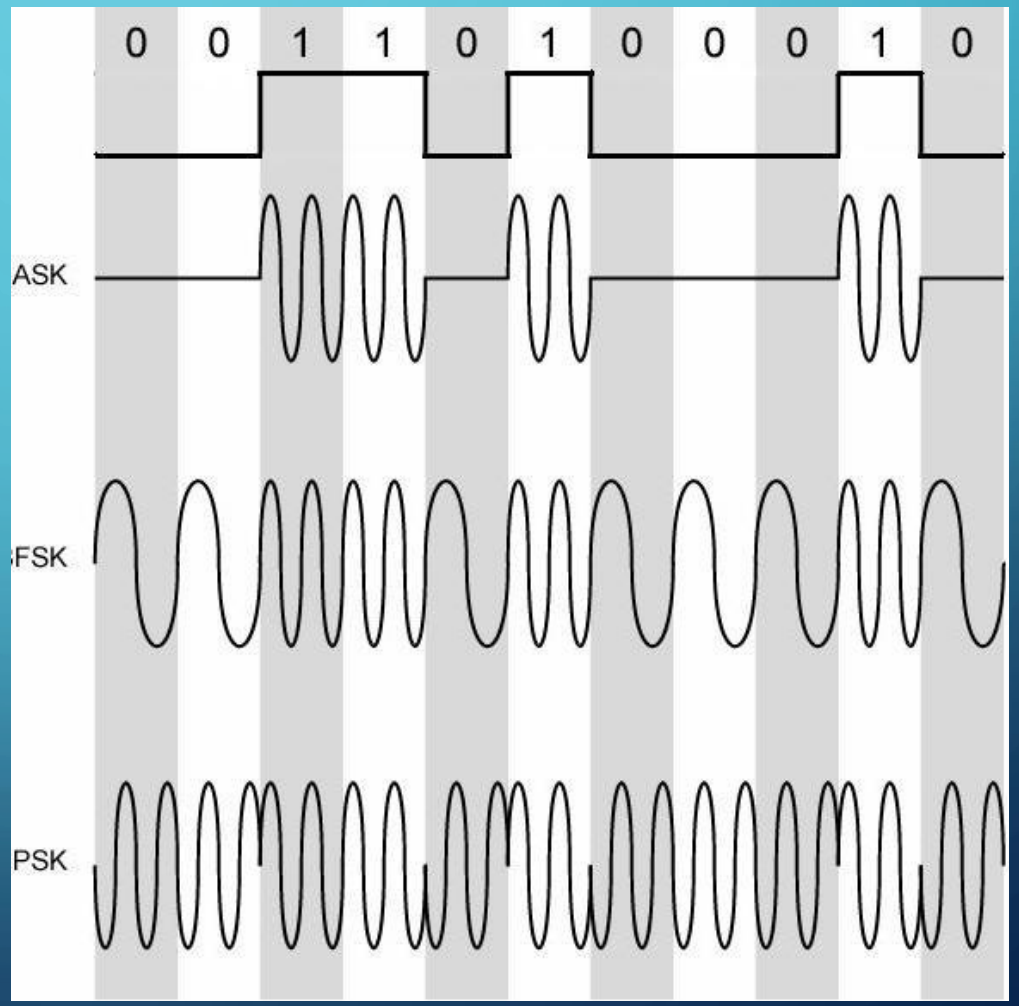
- *Modulation* is the modification of an analog signal to carry digital information. It's an example of a *digital-to-analog* (*D-to-A*, or *D/A*) conversion.
- Modulation is important because a computer's information is digital but network transmission media – typically wire, fibre-optic cables, or radio – rely on electromagnetic energy which travels in analog waves.

MODULATION

- Thus, modulation is the process of taking digital information, and imposing it in some way on an analog waveform so that it can travel across a network.
- Modulation changes an analog *carrier wave*, by altering the wave's frequency, amplitude, or phase, to carry a stream of bit values (ones and zeroes) from one device to another.

MODULATION

Three methods of modulating a stream of digital bit values (top) onto an analog carrier wave: Altering the carrier wave's amplitude (called amplitude shift keying, or ASK), its frequency (FSK), or its phase (PSK). Source.



DEMODULATION

- *Demodulation* is the undoing of modulation, that is, it is the extraction of digital information encoded on an analog signal. It is an *analog-to-digital* (*A-to-D*, or *A/D*) conversion.
- A computer receiving a pattern of bits that has been piggy-backed onto an analog carrier wave needs some way to reclaim the bits from that wave, and this is done through demodulation.

MODEM

- *Modem* is a *portmanteau* that, like *bit*, combines and shortens two words, in this case mo*dulator* and dem*odulator*.
- A modem is a device that sits between a digital device and an analog communications medium (a phone line, a coaxial cable, optical fiber, a radio transmitter/receiver, etc.) to allow the former to communicate over the latter.
- A modem modulates digital information onto outgoing analog waveforms and demodulates incoming analog waveforms to extract their digital information.

ROUTER

- Formally, a router is a device that connects similar networks to one another.
- In the home, a small office, or a lab, a router is a computer to which all devices on a LAN connect. This type of router manages network tasks and acts as a bridge across which all traffic in and out of the LAN is routed.
- Router is also the term used for computer systems that convey data across the internet, but that's a topic for our internet unit.

ROUTER

- Routers may be configured to protect a connected LAN from unwanted intrusions from the outside while still permitting legitimate two-way data traffic.
- The router in your home, if you have one, certainly doesn't look like a computer, but it likely is an embedded computer that runs some Linux distro as an operating system and lets you connect to it from a web browser to configure it.

GATEWAY

- You may also come across the word *gateway* when configuring a home network. Formally, a gateway is a specialized (often embedded) computer that connects dissimilar networks to one another. For example, the device which connects a wired LAN to a larger optical fibre network is a gateway.

SERVER

- A *server* is a computer that supports connections from other computers and provides those other computers with services and facilities such as email, web access, file sharing, and cloud storage.

CLIENT

- A *client* is a computer that get services from servers. Network-connected phones, tablets, laptops and desktop computers are examples of clients.

DOWNLOADING AND UPLOADING

- *Downloading* is the act of receiving a file or files from a server.
- *Uploading* is the act of sending a file or files to a server.
- A network across which uploading and downloading happen at the same speed is called *symmetric* (or *symmetrical*).
- A network across which upload and download speeds differ is called *asymmetric* (or *asymmetrical*). Many home internet connections are asymmetrical with much higher download than upload speeds because users tend to download more than they upload.

LAN CONNECTIVITY

WIRED AND WIRELESS

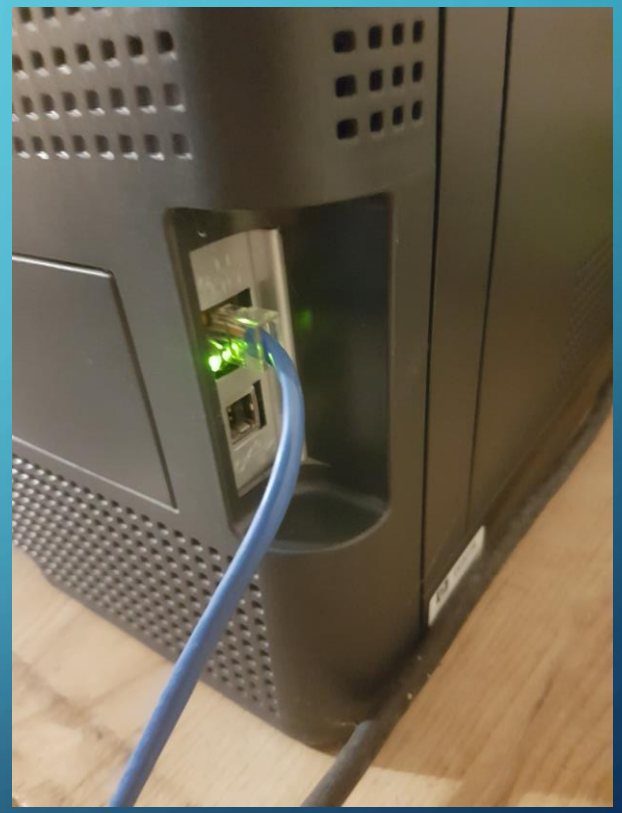
- Within a typical LAN, most communication is accomplished using one of
  - wired Ethernet;
  - wireless (Wi-Fi).
- Segments of LANs may also use
  - fibre-optic cable for high bandwidth communications between network devices;
  - Bluetooth wireless for communications between devices (for example, between a computer and a mouse or between a computer and a set of speakers).

ETHERNET

- *Ethernet* is the technological specification now employed almost everywhere for wire-connected LANs.
- Ethernet was invented by Robert (Bob) Metcalfe and David Boggs at the Xerox Palo Alto Research Center (PARC) in 1973.
- Ethernet gradually came to replace competing wired LAN technologies from other companies.

ETHERNET

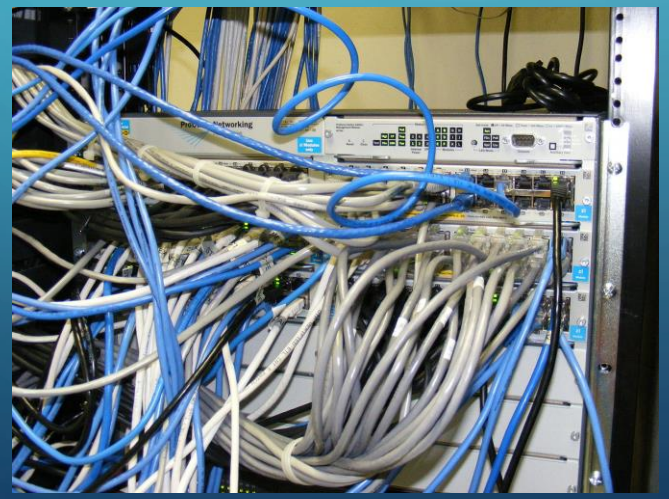
- Ethernet was also adopted as a communications standard by the prestigious *Institute of Electrical and Electronics Engineers* (*IEEE*, pronounced "I triple E"). The formal name for the standard is *IEEE 802.3*, but its popular name is still Ethernet.



An Ethernet cable connected to a networked printer.

ETHERNET

- The range of an Ethernet (i.e., maximum length data can reliably be sent over an Ethernet cable) is a few hundred metres, but this can be extended with devices that relay data from one network segment to another.
- The device usually used to extend the range of an Ethernet and to share an Ethernet connection with many devices is called a *network switch*, or, more commonly, a *switch*.



Some rather busy commercial-quality Ethernet switches in a rack. Source.

ETHERNET

- The bandwidth of a typical wired Ethernet connection is between 1 and 10 Gbps, depending on the ratings and quality of the cables and connecting hardware.

WI-FI

- Wi-Fi (wireless LAN) connections are made using radio. Each device that supports Wi-Fi contains a radio transmitter/receiver (transceiver).
- The IEEE specification for wireless LANs (802.11) was adopted for Wi-Fi to mimic the way Ethernet works.

WI-FI

- The effective range of Wi-Fi is limited by metal and concrete obstructions but is often around the same as wired Ethernet. Wireless range extenders, wireless access points, and mesh Wi-Fi are hardware solutions for working around these limitations.
- Wi-Fi is also subject to radio interference from other devices.

A wireless range extender.

A 3-node mesh WIFI system. Source.

WI-FI

- Because Wi-Fi is a directionless technology – broadcasting to and receiving from all directions – a Wi-Fi network is much more susceptible than a wired Ethernet network to security breaches by unwanted intruders. Strong encryption at the router of all Wi-Fi traffic is the usual solution to this, but concerns remain.

THE NETWORK INTERFACE CONTROLLER

- Each device on an Ethernet or Wi-Fi network connects to it by way of a hardware device called a *network interface controller* (*NIC*).
- An Ethernet cable plugs into a NIC by way of a standardized Ethernet port (socket). Wi-Fi NICs use radio antennas instead.
- Each NIC is uniquely identified on its LAN by a 48-bit *medium* (or *media*) *access control* (*MAC*) *address*.

THE NETWORK INTERFACE CONTROLLER

- NICs communicate with one another by way of *network packets*, commonly just called "packets."
- A packet is a formatted collection of bits that includes transmission information and a *frame*.
- The parts of a packet that do not comprise the frame are used for synchronization between devices and for marking the start of a transmission.
- The frame includes the MAC addresses of the intended recipient (destination) and sending (source) NICs, data that the sending machine is trying to convey to the receiving machine (the *payload*), and some error-checking information (a *frame-check sequence*) that the destination NIC can use to determine any transmission errors.

THE NETWORK INTERFACE CONTROLLER

Layer	Preamble	Start frame delimiter	MAC destination	MAC source	802.1Q tag (optional)	Ethertype (Ethernet II) or length (IEEE 802.3)	Payload	Frame check sequence (32-bit CRC)	Interpacket gap
	7 octets	1 octet	6 octets	6 octets	(4 octets)	2 octets	46-1500 octets	4 octets	12 octets
Layer 2 Ethernet frame			← 64–1522 octets →						
Layer 1 Ethernet packet & IPG	← 72–1530 octets →								← 12 octets →

Here's a Wikipedia view of an Ethernet packet with its frame and "interpacket gap" (IPG). **You do not need to remember the various parts of a packet for any quiz.** Note that an octet is the same as a byte, so each packet may contain a data "payload" of between 46 and 1500 bytes. That isn't very much, so the transmission of, say, a large file requires the generation of multiple packets that are sent in sequence.

CONNECTING TO THE WORLD

DIAL-UP

- For many years, the only network technology available to the average home computer user was a modem that worked by imposing or extracting digital information on or from analog electrical signals transmitted by the telephone system between two similarly-equipped computers.
- Data was transmitted as a regular land line phone call, at the same range of frequencies used for vocal communication, and a session would end when one side disconnected. We now call this technology *dial-up*, a reference to the rotary dial on old telephones.

DIAL-UP

Two generations of dial-up modems. The model on the left uses "acoustic couplers" that emphasize the technology's dependence on voice frequencies. On the right is the back view of a later modem with connections (left to right) for power, a computer's (pre-USB) RS-232 serial port, a cable to the phone company's wall receptacle, and a cable to the user's phone. Source and source. Later dial-up modems were built into laptops and desktops.

DIAL-UP

- A dial-up connection tied up a land line for the duration of its use and had technological restrictions that limited it to about 56 Kbps bandwidth maximum (about 24 MB/hour), often less. This was all but useless for doing something as elementary as downloading regular security updates for a modern operating system.

DIAL-UP

- Dial-up was in widespread use on home computers before the internet became generally available. In those days, users made frequent use of so-called *bulletin board systems* (BBSs) that were dial-up servers run by corporations or computer hobbyists.
- BBSs typically offered file sharing and email for members in addition to providing text-based message repositories – the bulletin boards – where users could share posts on many topics. In time, all such services would migrate to the internet where the reach was universal rather than being restricted to small groups of subscribers.

BROADBAND

- *Broadband* is a term long-used by ISPs to describe communications technologies with average bandwidths better than those achievable with dial-up. I say "average" because some broadband technologies – notably certain wireless technologies – can have horrible problems with jitter.
- More recently, broadband has been more rigorously defined, but it is a definition that has varied over time and from country to country. Canada's minimum bandwidth standards for broadband tend to lag those of other G7 countries.

BROADBAND

- *Cable, Digital Subscriber Line* (*DSL*), and *fibre* are the three main broadband technologies used in urban and suburban environments.

BROADBAND

- Rural broadband has historically been less reliable and much more prone to jitter than cable, DSL, or fibre. It has typically afforded lower bandwidth than that available to city dwellers and may have been unavailable to many for reasons of distance or geography. Rural broadband technologies include wireless (dependent on radio signals from nearby transmitter/receivers – *transceivers* – on towers), satellite (requires line-of-sight connections with a transceiver satellite), and mobile wireless (a subset of wireless, dependent on cellular networks).
- A *digital divide* is created when groups of people have unequal access to technology, as is the case for urban and rural dwellers and internet services.

CABLE BROADBAND

- Cable broadband uses coaxial cable as a transmission medium.
- Though originally designed to provide one-way transmission of television to the home, the growing popularity of the internet in the late 1990s and early 2000s caused cable to be developed into a two-way technology and it quickly became a common way to provide broadband internet service.

A male connector on the end of a coaxial cable.

CABLE BROADBAND

- Cable signals are analog, so their use in broadband requires the presence in the home of a special *cable modem*.
- Cable access is shared among many users, and because of this the bandwidth available to a single customer is typically capped by the modem.

CABLE BROADBAND

- Sharing cable access also means that your data ends up in your neighbours' homes and vice versa. Some effort has gone into ensuring that data intended for one cable user is secured by encryption so that it can only easily be decrypted by that user's cable modem. See http://en.wikipedia.org/wiki/DOCSIS#Security.

CABLE BROADBAND

- It's hard to get a good feel for how fast one should expect a cable connection to be. Various sources give different answers.
- I checked the bandwidth of my TekSavvy internet connection (which uses cable installed by Cogeco) in the middle of a workday using a popular connection speed testing service. It reported a download speed of 72.01 Mbps and an upload speed of 10.9 Mbps meaning my connection is asymmetrical.

DIGITAL SUBSCRIBER LINE (DSL)

- Like dial-up, DSL uses land phone lines for two-way data transfer. It differs, however, in how those phone lines are used:
  - DSL is always on; no "dialing-up" is necessary.
  - Dial-up modems were restricted to using the same frequencies as regular voice phone calls. Phone companies place a rather low limit on the frequencies available for voice calls (for which sound quality requirements are not great), and this resulted in the 52 Kbps maximum bandwidth barrier for dial-up. This restriction was lifted for DSL which uses a much greater frequency range than voice/dial-up with a corresponding increase in bandwidth.

DIGITAL SUBSCRIBER LINE (DSL)

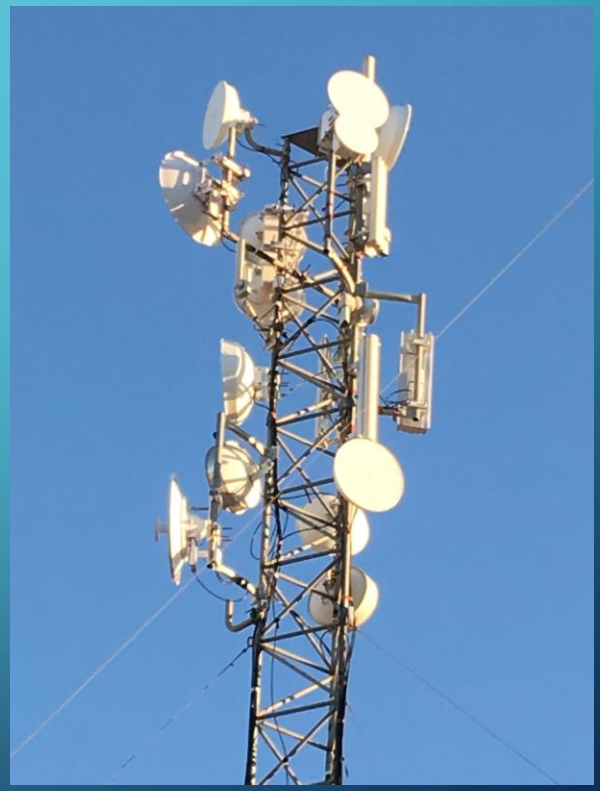
- DSL bandwidth, according to Wikipedia can vary between 256 Kbps to over 100 Mbps for downloads for typical connections. As is the case with my cable service, an *asymmetric DSL* (*ADSL*) connection provides its users with faster download speeds at the expense of slower upload speeds, but this is usually an acceptable trade-off.
- However, like a landline phone call, (and unlike a cable connection) a DSL connection is point-to-point; it is not broadcast to everyone in an area, it is reserved for a single customer's use.

DIGITAL SUBSCRIBER LINE (DSL)

- Because DSL makes use of a much greater frequency range than voice/dial-up connections, it is much more susceptible to signal degradation over long distances and can only be used within a few kilometres of a telephone company switching office. As these switching offices are expensive for a phone company to set up and maintain, it is far less likely that a rural customer is near one than an urban customer.
- A DSL connection requires a *DSL modem*.

FIXED WIRELESS BROADBAND

- *Fixed wireless broadband* is the term used for ground-based broadband networks that use a wireless technology, typically radio, as their communications medium.
- Fixed wireless is a popular method of connecting to the internet in rural areas, but only works for those within range of a service provider's ground station tower. Communications may be further limited by features of the landscape, like hills.



A fixed wireless broadband tower. Source.

FIXED WIRELESS BROADBAND

- Fixed wireless is typically asymmetrical. Available bandwidths vary widely, with download speeds ranging from 25 Mbps to 1000 Mbps (1 Gbps) and upload speeds from 7 Mbps to 25 Mbps.
- Fixed wireless is a broadcast technology, so data security is a concern that is mitigated by wireless encryption methods.
- In addition to a modem, a user of fixed wireless requires a directional antenna, one that is usually mounted on the user's home by a technician. This will likely push the installation cost higher than cable or DSL.

MOBILE BROADBAND

- *Mobile broadband* is the term used to describe a fixed wireless access system based on cellular network technologies.
- For years, it has been possible to use a smartphone as a mobile modem and router for personal computers in a process called tethering.
- Mobile internet plans are now available from many ISPs.

MOBILE BROADBAND

- Cellular networks that are advertised as *4G* or *4G LTE* can provide asymmetric bandwidth with download speeds up to 100 Mbps. This is the most common mobile broadband technology currently.
- The world is quickly shifting to *5G* mobile broadband, though there are many controversies – some political, some owing to conspiracy theories, some having to do with airliner safety, some having to do with health concerns – surrounding it.
- 5G promises download speeds up to 200 Mbps; generally, much faster than typical cable, DSL, and 4G connections.

SATELLITE BROADBAND

- From slow and sometimes failed beginnings in the late 1990s and early 2000s, satellite broadband has greatly improved and continues to improve.
- Satellite is the only broadband medium available to many people in rural areas.
- Satellite broadband has historically been very expensive but as technologies continue to evolve and competition grows, this is changing.

Satellite broadband dish in a rural setting.
Source.

SATELLITE BROADBAND

- Satellite broadband suffers from moisture or precipitation in the air (*rain fade*). It also, currently, requires that there be no obstructions (hills, trees, buildings) between the customer's dish on the ground and a satellite in orbit.
- As previously mentioned, latency may also be a concern with satellite broadband – particularly for those services using satellites in geosynchronous orbits – owing to large transmitter-to-satellite and satellite-to-receiver distances.

SATELLITE BROADBAND

- SpaceX, Amazon, and OneWeb each plan launch over 1000 satellites into low earth orbit to form *internet constellations* that should provide (much) better geographical coverage than can be afforded by a dish pointed at a single satellite. The great increase in numbers of satellites is a cause for concern among astronomers and space agencies worried about orbital debris ("space junk").
- Internet constellations operate in low earth orbit rather than in geosynchronous orbit to (greatly) reduce latency.
- SpaceX's StarLink internet constellation satellite service in Canada currently has a bandwidth that is comparable to or a bit higher than typical cable or DSL connections.

FIBRE BROADBAND

- The fastest available medium for providing network services to the public is *fibre-optic cable*, often abbreviated to *fibre*.
- Long available in commercial and academic settings, "*fibre to the home*" (*FTTH*) has become common, at least in urban settings.

FIBRE BROADBAND

- Fibre has the potential to provide bandwidths of 1 Gbps over a *symmetrical* connection (where the upload and download speeds are the same).
- Home wireless network technologies have traditionally outperformed incoming and outgoing broadband connections in terms of bandwidth. With fibre, our own equipment may become a bandwidth bottleneck.
- As a broadband technology, fibre is more expensive than cable or DSL, but in terms of bandwidth it certainly provides much higher return on investment (i.e., more "bang for the buck").

CRYPTOGRAPHY

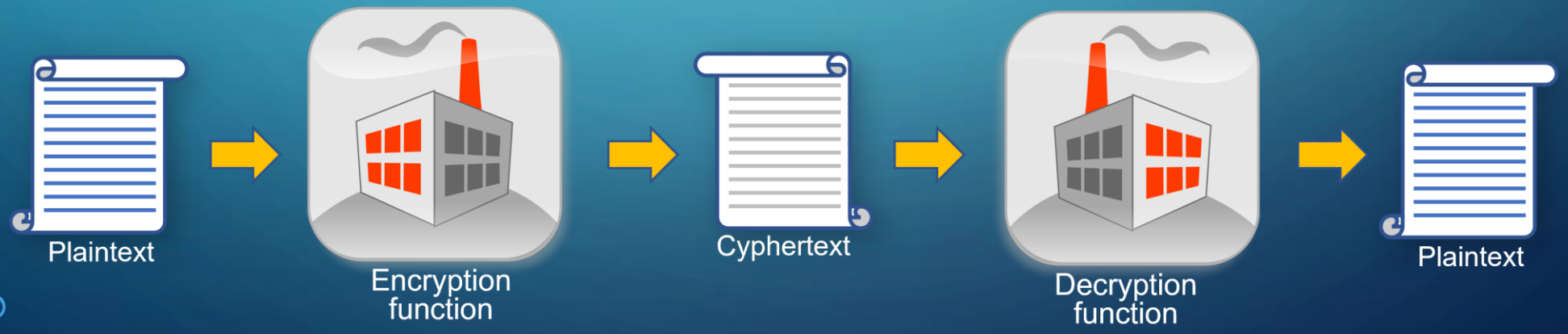
WHAT IS CRYPTOGRAPHY?

- Cryptography is the practice of securing data by transforming it into an unreadable format which, ideally, can only be restored to its original, readable form by authorized parties.
- Though cryptography has a long history, it has risen in popular awareness with the advent of computer networks and the need to secure data transmissions over those networks.

CRYPTOGRAPHY TERMINOLOGY

SECURED AND UNSECURED DATA

- *Plaintext* is a term applied to any data, **text or otherwise**, in its original form.
- *Ciphertext* is a reversible, obscured representation of plaintext.
- *Encryption* is the process of converting plaintext into ciphertext.
- *Decryption* is the process of restoring ciphertext to plaintext.
- Encryption and decryption methods are algorithms that may be expressed as functions.



KEYS

- A *key* in a cryptographic system is an item of data – typically a number – separate from the plaintext or ciphertext, that is used by the encryption or decryption algorithm to do its work.

KEYS

- A cryptographic system typically employs one or two keys.
  - In a *symmetric encryption* system, a single key is used for both encryption and decryption. The key must be kept secret as anyone who knows the key will be able to decrypt any generated cyphertext.
  - In an *asymmetric encryption* system, it's usual that one key– the *private key* – is kept secret and another – the *public key* – is not. In those systems, encryption is done with the public key and decryption is performed with the private key.
- The encryption and decryption algorithms in symmetric encryption systems involve less computation – and therefore less time – than those used in asymmetric systems, but at a potential security cost.

BACKDOORS

- A *backdoor* is a vulnerability deliberately built into an encryption system that will allow decryptions by parties not authorized by the cyphertext creator. These are typically created to allow government agencies, such as police services, access to encrypted data.
- In societies founded on principals of individual freedom of speech and privacy, backdoors are controversial. Their creation is generally resisted by technology companies fearful of losing customers who value privacy in their communications. See, for example, Apple, other tech companies continue to resist encryption backdoor proposals by FBI, U.S. DOJ | AppleInsider.

CRYPTANALYSIS VS. BRUTE FORCE

- *Cryptanalysis* is the practice of decryption using various analytical methods without benefit of keys or backdoors.
- A so-called *brute-force attack* on a ciphertext may be attempted when cryptanalysis fails. A brute-force attack involves trying every possible combination of characters or numbers to find an encryption key or possibly a password. This method obviously isn't efficient but may used as a last resort.
- To undo an encryption method is to *break* or *crack* it.

ALICE, BOB, EVE, AND MALLORY

- *Alice*, *Bob*, *Eve*, and *Mallory* are fictitious characters frequently appearing in abstract descriptions of cryptographic systems. In these descriptions,
  - Alice sends encrypted messages to Bob;
  - Eve (an eavesdropper) intercepts the messages and tries to read them;
  - Mallory is a malicious version of Eve who may choose to intercept and alter messages that Alice sends to Bob.
- The names are used in place of any sender of encrypted data (Alice), any intended receiver of that data (Bob), and a hostile party trying to break the encryption (Eve and Mallory).
- Other such characters have been invented over time to fill more specific roles. See https://en.wikipedia.org/wiki/Alice_and_Bob.

PERSON-IN-THE-MIDDLE ATTACK

- A *person-in-the-middle attack* has Mallory receiving Alice's messages then reading and possibly altering them before forwarding them to Bob. Neither Alice nor Bob suspect Mallory's presence in their communication.
- A good encryption scheme should anticipate the presence of a Mallory and take steps to ensure messages are
  - protected from being read by unauthorized parties and
  - that any unauthorized alteration to a message is readily apparent to the authorized receiver.

PERSON-IN-THE-MIDDLE ATTACK

- Symmetric encryption systems suffer from a weakness that asymmetric systems do not: How to securely communicate the single encryption/decryption key so that it can't be discovered in a person-in-the-middle attack? The answer to that is forthcoming.

AN INCOMPLETE HISTORY OF CRYPTOGRAPHY

CAESAR CIPHER

- The *Caesar cipher* is named for the Roman dictator Julius Caesar who used the encryption method in his private correspondence.
- It is a so-called *substitution cipher* which relies on a system of character substitutions in text messages.
- In it, a plaintext message has its characters rotated by some positive integer through the alphabet, i.e., with a key of 3 (favoured by Caesar), "A" becomes "D", "B" becomes "E" and so on. The last three letters of the alphabet are mapped to "A", "B" and "C". The plaintext English word "ZEBRA" would then become the ciphertext "BHEUD".

MARY, QUEEN OF SCOTS

- Mary Stuart (1542 – 1587), Queen of Scotland, was a Roman Catholic cousin of the Protestant Queen of England, Elizabeth I. While under house arrest in England, Mary employed various substitution ciphers in sensitive correspondence.
- Mary became involved in a plot to overthrow Elizabeth and claim the English throne for herself. She communicated with one of the authors of the plot by way of encrypted correspondence using one of her ciphers.
- Unfortunately for Mary, her correspondence was intercepted, deciphered, and used in evidence against her. She was ultimately convicted of treason and executed.

THE PROBLEM WITH SUBSTITUTION CIPHERS

- Substitution ciphers of the type used by Caesar and Mary Stuart are vulnerable to various eavesdropper attacks. For example:
  - The number of keys available in a Caesar cipher is limited. If the encryption method is known, it's easy to find which key was used to encrypt a specific message and decrypt it.
  - The frequency at which various letters appear in regular text is well understood. For example, "E" appears in English text more often than any other letter. A ciphertext based on a straightforward substitution of characters can be analyzed with this knowledge to make good guesses at the underlying message.
  - If a Mallory or Eve figure already possesses some decrypted messages, all further messages encrypted using the same substitutions are compromised.

POLYALPHABETIC CYPHERS

- *Polyalphabetic ciphers* offer improved security over substitution ciphers, all of which rely on a single "alphabet" of code characters or symbols. As the name implies, a polyalphabetic cipher is designed so that multiple alphabets of code symbols are used to encrypt messages.
- This might mean, for example, that no two adjacent characters in a plaintext message are encrypted in the same way, making it much harder for a would-be Eve or Mallory to decrypt cyphertext using techniques like letter frequency analysis.
- Rather than spend time here building an example of a polyalphabetic cipher, I refer you to this short video on the subject.

POLYALPHABETIC CYPHERS

- While an improvement on the older single alphabet substitution ciphers, polyalphabetic ciphers are vulnerable to cryptanalysis if the encryption method and the string representing the (typically lengthy) key can be discovered.

ENIGMA

- Prior to and during World War II, the German military used an encryption device called *Enigma* to encode its wireless (radio) text transmissions. Enigma implemented a sophisticated polyalphabetic cypher algorithm.

An Enigma machine.
Source.

ENIGMA

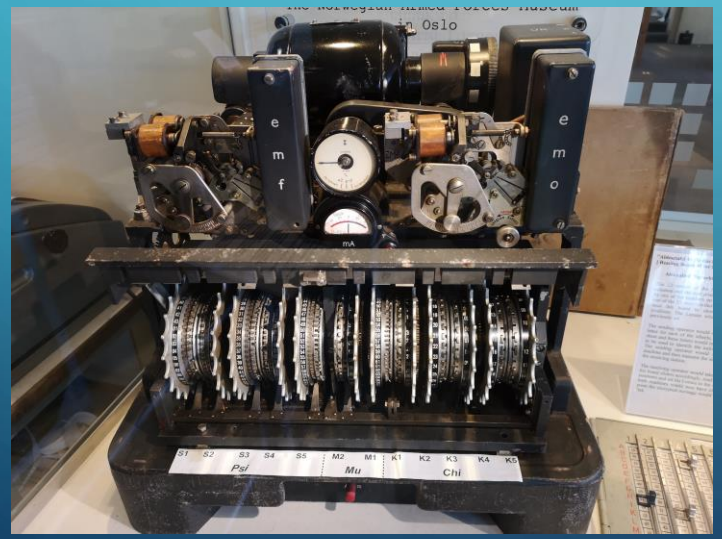
- Work on breaking the Enigma code began during the early 1930s in pre-war Poland under mathematician Marian Rejewski and continued as repeated improvements to Enigma were made.
- Fortunately for the Allies, before Poland fell to the invading forces of Nazi Germany and the Soviet Union in 1939, the Polish researchers shared their extensive knowledge of Enigma and the devices they had built to assist in their decryption efforts with Britain and France.
- This sharing of information gave Alan Turing and his team of specialists at Bletchley Park outside London a tremendous advantage in their own efforts to decrypt Enigma "traffic" as the steady stream of German ciphertexts was called.

ENIGMA

- Both the Polish and British built electro-mechanical devices to assist in their efforts to decrypt Enigma traffic. Rejewski devised a *bomba* (literally "bomb", for obscure reasons) that duplicated the operation of six Enigma devices, and Turing developed it into his *bombe*, the device featured in the film *The Imitation Game*.
- Though these devices were invaluable to Enigma cryptanalysis, the Allies also got lucky owing to the way Enigma was used and sloppiness on the part of some of the German encoders. It is likely that without these human weaknesses, Enigma would have remained secure.

TUNNY

- Though (much) less well known than the Enigma story, a quite separate cryptanalysis effort at Bletchley Park provided enormous advantages to the British and their allies. This was the successful decryption of traffic from a symmetric-key German cipher machine they called *Sägefisch* ("Sawfish") and the British called *Tunny* (derived from "tuna fish").



An SZ42 cipher machine, one of the devices manufactured in Germany by C. Lorenz AG codenamed *Sägefisch* and called *Tunny* by the British. Source.

TUNNY

- Tunny traffic, usually called Tunny or Fish, originated with the German high command and occasionally included messages signed by Adolf Hitler himself.
- Though judged a superior encryption machine to Enigma, cryptanalysis of Tunny was made possible by the same sort of procedural weaknesses and operator blunders that afflicted Enigma.
- Tunny was first cracked without mechanical assistance by a group of four German-speakers led by Ralph Tester set up in 1941 and called the *Testery*.
- Later cryptanalysis of Tunny was mechanized, ultimately by the Colossus computers described in an earlier unit.

PUBLIC-KEY CRYPTOGRAPHY

- *Public-key cryptography* refers to methods of encrypting and decrypting data that use two different keys – a public key and a private key – rather than a single, symmetric key for both functions.
- The concept of public-key encryption was first introduced in 1976 by US cryptography researchers Whitfield Diffie and Martin Hellman, building on work done by Ralph Merkle while the latter was an undergraduate at UC Berkeley.

PUBLIC-KEY CRYPTOGRAPHY

- Public-key encryption works by using a pair of mathematically related keys – a public key and a private key – to encrypt and decrypt data, respectively. The public key is made widely available, while the private key is kept secret. Anything encrypted using the public key can only be decrypted using the private key, thus helping to make the system resistant to person-in-the-middle attacks.
- The first widely used public-key encryption algorithm was the RSA cryptosystem, developed by Ron Rivest, Adi Shamir, and Leonard Adleman in 1978.

PUBLIC-KEY CRYPTOGRAPHY

- The complexity of the RSA encryption and decryption algorithms make it too slow for many applications, particularly network communications, but it is still used in so-called *hybrid cryptosystems* to securely transmit keys for otherwise symmetric-key cryptographic systems. Many other public-key encryption algorithms have been developed since its introduction.

PUBLIC-KEY CRYPTOGRAPHY

- The security of public-key cryptographic systems depends largely on three things:
  - The choice of encryption algorithms, since many prove vulnerable to various attacks.
  - The choice of keys. Keys are generated mathematically. Keys in RSA cryptosystems, for example, are calculated using two very large but otherwise randomly chosen prime numbers, multiplied together into a semiprime. Longer keys are often more secure than shorter keys, but optimal key length is affected greatly by choice of encryption algorithms.
  - Related to the choice of keys, the principle underlying the security of public-key systems is high computational difficulty in discovering the private keys. RSA, for example, relies on the tremendous difficulty of factoring very large semiprimes.

THE DEATH OF CRYPTOGRAPHY?

- It is not uncommon, now, to read news articles such as this one, The Death of Cryptography in a Post-Quantum World, that forecast the end of public-key cryptography with the advent of practical *quantum computers*, but we're not there yet.
- In anticipation of the demise of public-key systems, researchers are currently working on cryptographic systems that will not be vulnerable to quantum computer attacks.

IN THE MEANTIME…

- For now, public-key encryption and hybrid systems that employ it have become essential tools for securing communication and transactions over networks, including the internet which we'll be studying in more detail in an upcoming unit.

SUMMARY

IN THIS UNIT WE LOOKED AT

- Many networking terms
- LAN networking technologies
- WAN networking technologies (particularly broadband)
- Cryptography, including
  - Cryptographic terminology
  - Some cryptographic history
  - Public key cryptographic systems (as opposed to symmetric key systems)