The Digital Revolution and the Hackers Culture.

Elective course
3rd module (Feb-Mar) 2019

Fabio Grazioso

Lecture 11/12

summary

- Historical perspective
  - History of early networks and on-line culture
- Sociological perspective
  - Virtual reality, Augmented reality, Artificial Intelligence, Trans-humanism
- Technological perspective
  - Cryptography

History of early networks and on-line culture

Bulletin Board Systems

- A Bulletin Board is something where to put public messages, for a local community
- Out of this concept, we have the Bulletin Board System (BBS) which was the electronic (digital) version of this
- “Electronic” or “digital” means that you want to do this with a computer, over a **Computer Network**

Computer network

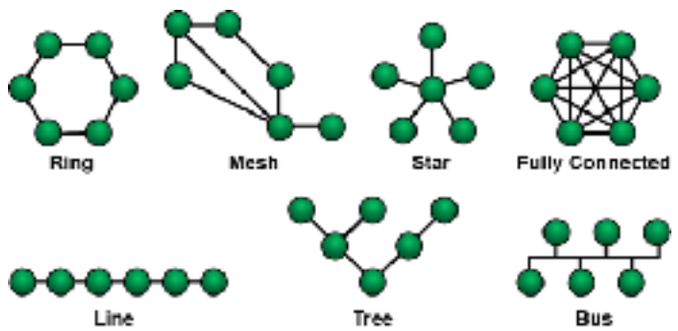
- What is a **Computer Network**? A network of computers, of course!
- But the question is: how do you *implement* this?

Computer network

- What is a **Computer Network**? A network of computers, of course!
- But the question is: how do you *implement* this?
- How do you make the connections?

Computer network

- What is a **Computer Network**? A network of computers, of course!
- But the question is: how do you *implement* this?
- How do you make the connections?
- What **topology**?



Bulletin Board Systems

- The earliest BBS can be considered “Community Memory”, started in 1973 in Berkeley, California running on a **mainframe** computer and accessed through terminals located in around San Francisco Bay Area.

So, with a mainframe we definitely have a “star” topology, with a central node ad several terminals

Modem connection

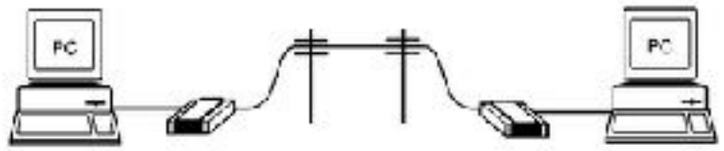
- Regarding the “medium” the way to implement a computer network, in the ‘70s, was through telephone lines

Modem connection

- Regarding the “medium” the way to implement a computer network, in the ‘70s, was through telephone lines
- To transmit data over telephone lines, a *modem* (modulator-demodulator) was used.

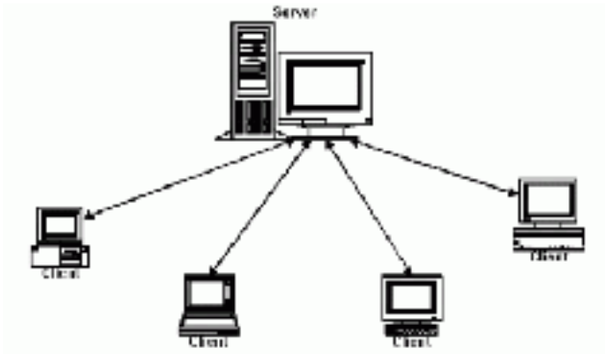
Modem connection

- Regarding the “medium” the way to implement a computer network, in the ‘70s, was through telephone lines
- To transmit data over telephone lines, a *modem* (modulator-demodulator) was used.
- Then, the connection can be done only point-to-point, because this is how the telephone system works



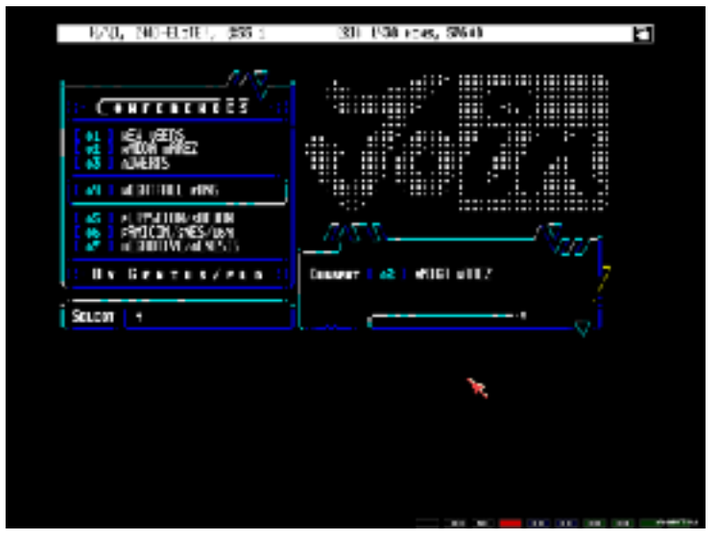
Modem connection

- Regarding the “medium” the way to implement a computer network, in the ‘70s, was through **telephone lines**.
- To transmit data over telephone lines, a ***modem*** (modulator-demodulator) was used.
- Then, the connection can be done only **point-to-point**, because this is how the telephone system works.
- And you have a star topology, where many clients connect to the same server. **One connection at a time.**



Bulletin Board Systems content

- The users connect to the BBS server, one by one, what do they find?
  - A collection of public messages
  - a collection of files
  - later, a private messaging system was developed



the content was alphanumeric, because of the limited “bandwidth”

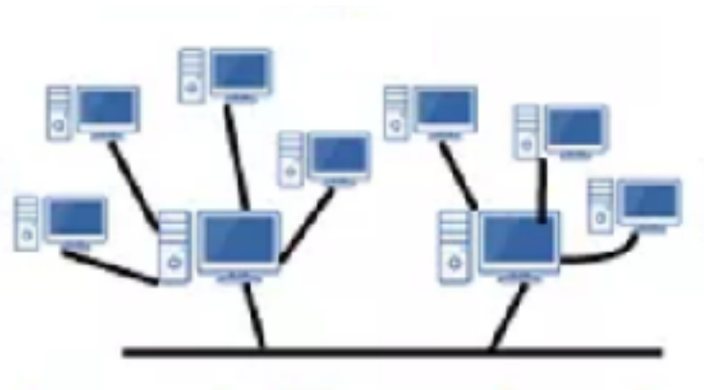
Bulletin Board Systems content

- The users connect to the BBS server, one by one, what do they find?
  - A collection of public messages
  - a collection of files
  - later, a private messaging system was developed

the content was alphanumeric, because of the limited “bandwidth”

Bulletin Board Systems content

- How do you send messages to other users?
- Either you are limited to the users of that BBS,
- or you implement a system where each server connects with other servers, and exchange data.

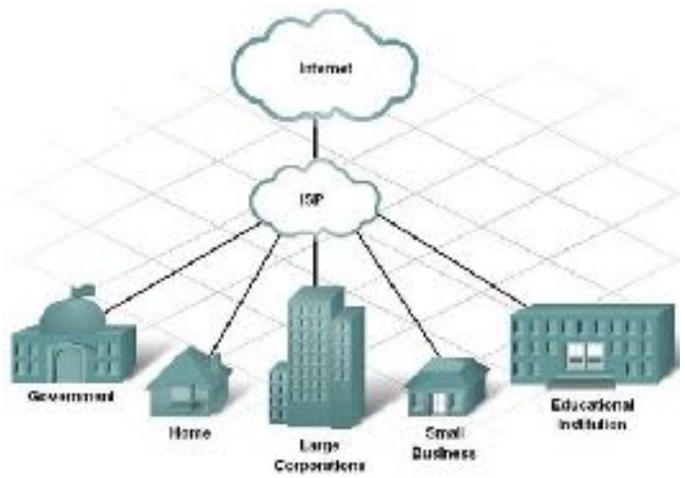


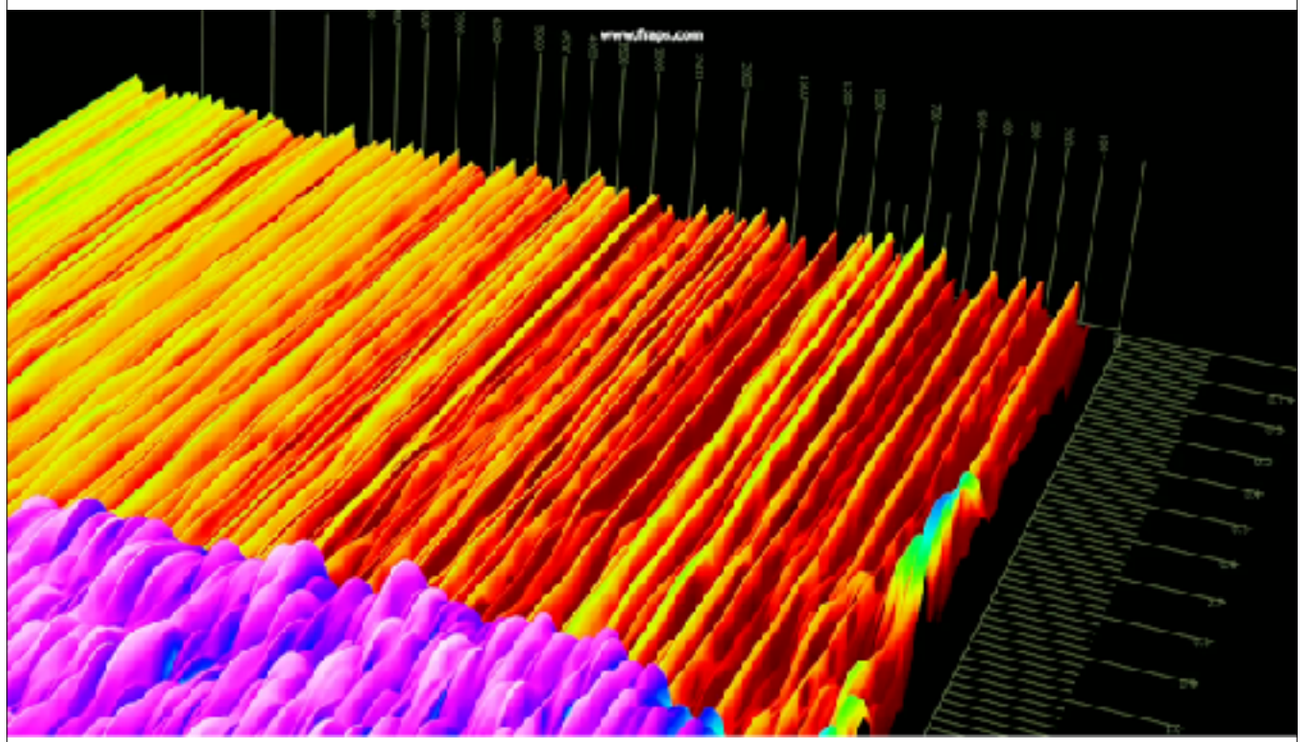
Academic networks

- DECnet, a network of mainly academic institutions, operated on VAX minicomputer networks

Internet Service Providers

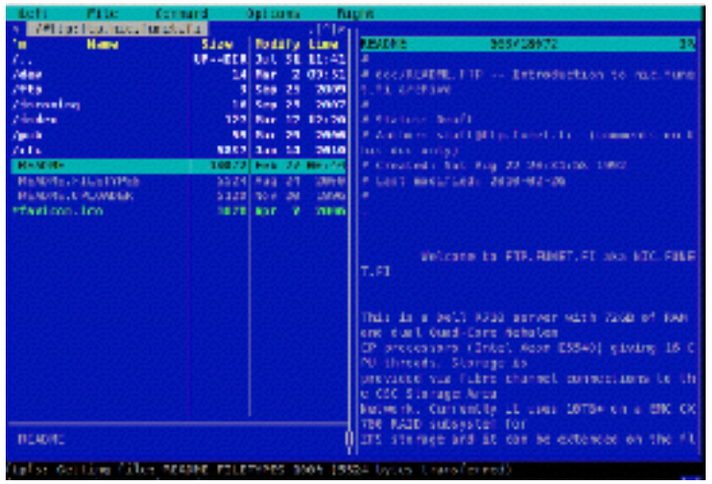
- In the ‘90s the “internet” started to became available
- The connection to the internet (interconnected network) was implemented through specialized physical connections (backbones) for big institutions (Universities, corporations etc.)
- To commercial users (households, offices, etc) the connection was implemented through Internet Service Providers, still using telephone lines
- A *point-to-point protocol* (PPP) was used, with a **modem**, to call a local server and, through that, to the internet.





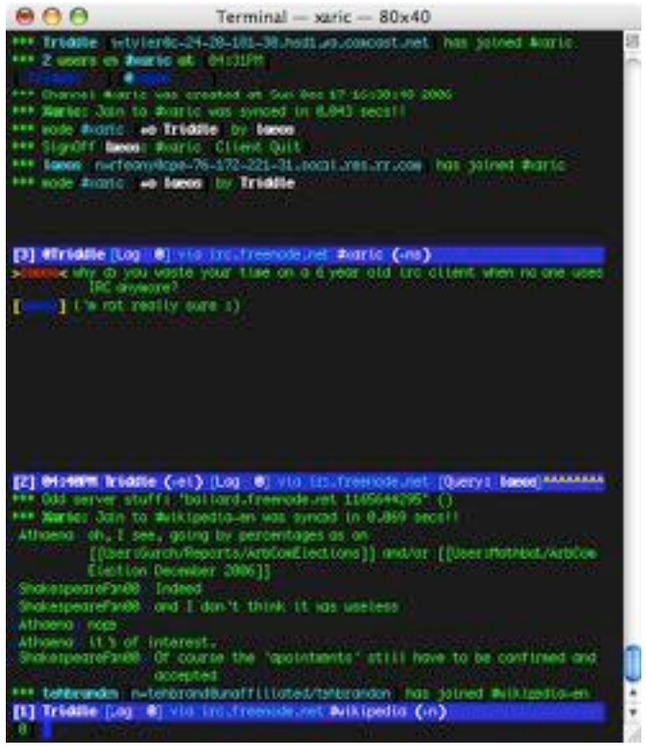
Anonymous FTP servers

- A host that provides an FTP service may provide anonymous FTP access. Users typically log into the service with an 'anonymous' (lower-case and case-sensitive in some FTP servers) account when prompted for user name. Although users are commonly asked to send their email address instead of a password, no verification is actually performed on the supplied data. Many FTP hosts whose purpose is to provide software updates will allow anonymous logins.



Internet Relay Chat

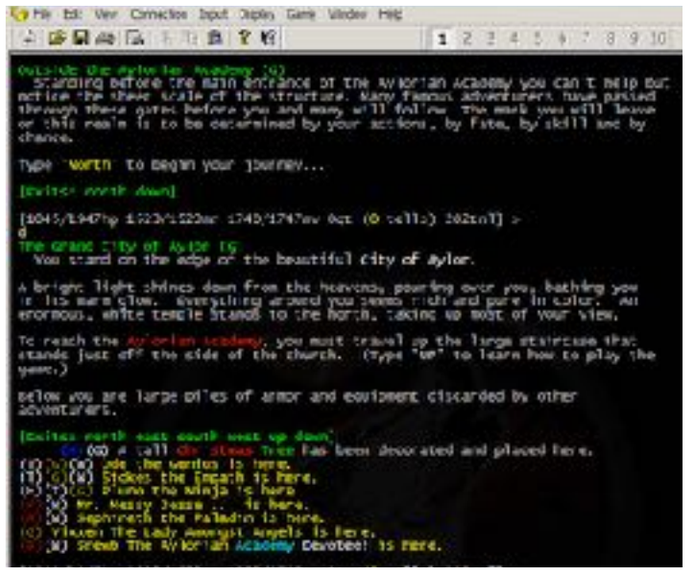
- Internet Relay Chat (IRC) is an application layer protocol that facilitates communication in the form of text.
- The chat process works on a client/server networking model. IRC clients are computer programs that users can install on their system or web based applications running either locally in the browser or on 3rd party server.
- These clients communicate with chat servers to transfer messages to other clients. IRC is mainly designed for group communication in discussion forums, called channels, but also allows one-on-one communication via private messages as well as chat and data transfer, including file sharing.



instant messaging

Multi-User Dungeon

- A MUD (Multi-User Dungeon) is a multiplayer real-time virtual world, usually **text-based**. MUDs combine elements of role-playing games, hack and slash, player versus player, interactive fiction, and online chat.
- Players can read or view **descriptions of rooms**, objects, other players, non-player characters, and actions performed in the virtual world. Players typically interact with each other and the world by **typing commands** that resemble a natural language.



instant messaging

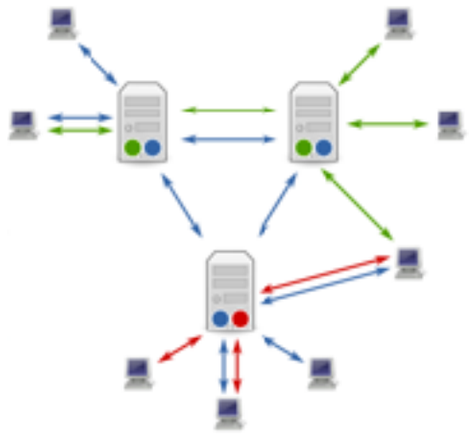
Multi-User Dungeon

- Traditional MUDs implement a role-playing video game set in a **fantasy world** populated by fictional races and monsters, with players choosing classes in order to gain specific skills or powers.
- The objective of this sort of game is to slay monsters, explore a fantasy world, complete quests, go on adventures, create a story by roleplaying, and advance the created character. Many MUDs were fashioned around the dice-rolling rules of the **Dungeons & Dragons** series of games.

instant messaging

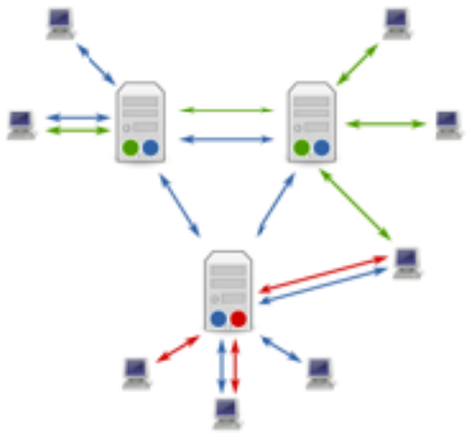
Usenet

- Usenet is a worldwide distributed discussion system available on computers. Tom Truscott and Jim Ellis conceived the idea in 1979, and it was established in 1980. Users read and post messages (called articles or posts, and collectively termed news) to one or more **categories**, known as **newsgroups**.
- Usenet resembles a bulletin board system (BBS) in many respects and is the precursor to **Internet forums** that are widely used today. Discussions are threaded, as with web forums and BBSs, though posts are stored on the server sequentially. The name comes from the term "users network".



Usenet

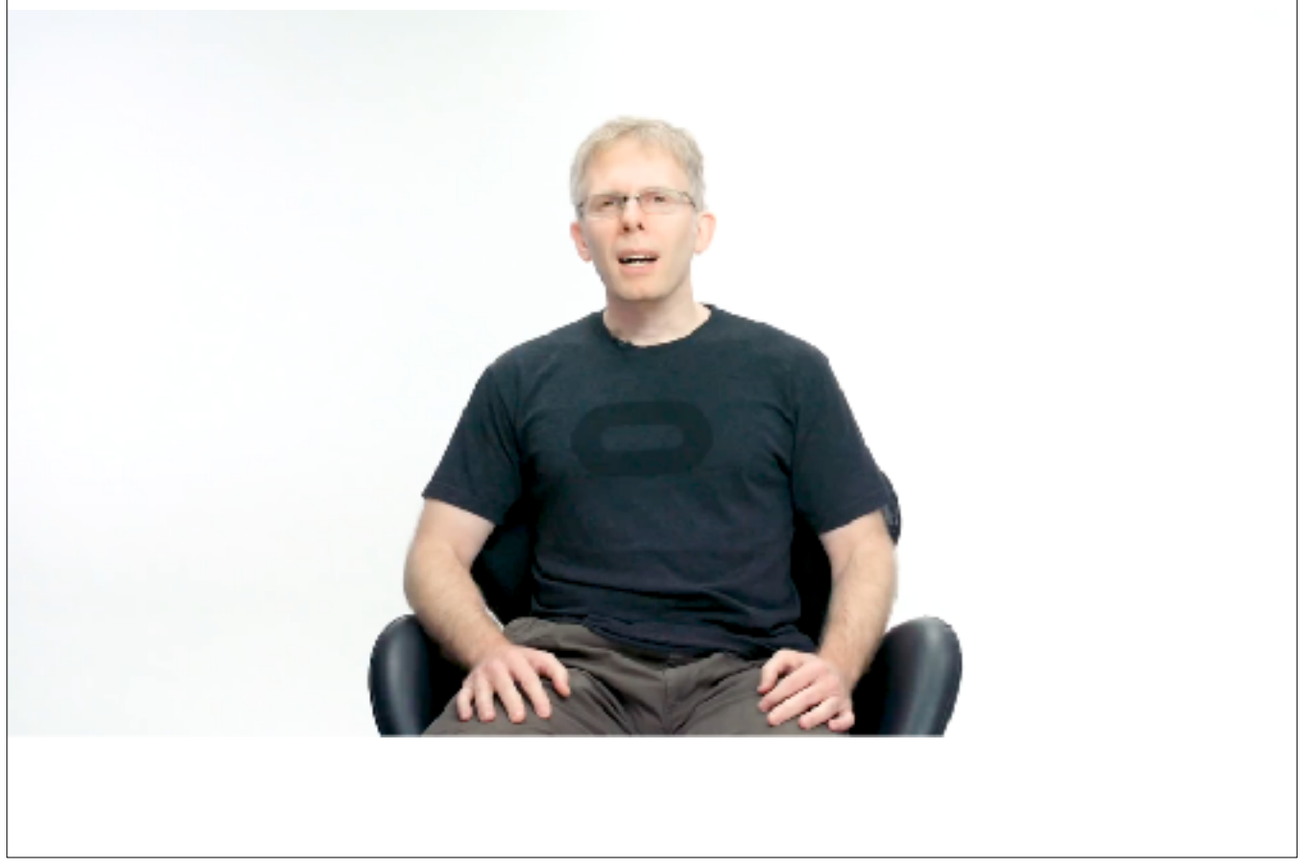
- A major difference between a BBS or web forum and Usenet is the absence of a central server and dedicated administrator. Usenet is distributed among a large, constantly changing conglomeration of servers that store and forward messages to one another in so-called news feeds.
- Individual users may read messages from and post messages to a local server operated by a commercial usenet provider, their Internet service provider, university, employer, or their own server.
- Usenet is culturally significant in the networked world, having given rise to, or popularized, many widely recognized concepts and terms such as "FAQ", "flame", and "spam".



Virtual reality, Augmented reality, Artificial Intelligence, Trans-humanism

Virtual Reality

- Virtual reality (VR) is an **interactive computer-generated experience** taking place within a **simulated environment**. It incorporates mainly auditory and visual feedback, but may also allow other types of sensory feedback like haptic.
- This immersive environment can be similar to the real world or it can be fantastical.
- Current VR technology most commonly uses virtual reality **headsets** or multi-projected environments, sometimes in combination with physical environments or props, to generate realistic images, sounds and other sensations that simulate a user's physical presence in a virtual or imaginary environment.
- A person using virtual reality equipment is able to "look around" the artificial world, move around in it, and interact with virtual features or items. The effect is commonly created by VR headsets consisting of a head-mounted display with a small screen in front of the eyes.



Augmented Reality

- Augmented reality (AR) is an interactive experience of a real-world environment where the objects that reside in the real-world are "augmented" by computer-generated perceptual information, sometimes across multiple sensory modalities, including visual, auditory, haptic, somatosensory, and olfactory.
- The overlaid sensory information can be constructive (i.e. additive to the natural environment) or destructive (i.e. masking of the natural environment) and is seamlessly interwoven with the physical world such that it is perceived as an immersive aspect of the real environment.
- In this way, augmented reality alters one's ongoing perception of a real-world environment, whereas virtual reality completely replaces the user's real-world environment with a simulated one.

Head-up display

Flight simulation

- A flight simulator is a device that artificially re-creates aircraft flight and the environment in which it flies, for pilot training, design, or other purposes.
- It includes replicating the equations that govern how aircraft fly, how they react to applications of flight controls, the effects of other aircraft systems, and how the aircraft reacts to external factors such as air density, turbulence, wind shear, cloud, precipitation, etc.
- Flight simulation is used for a variety of reasons, including flight training (mainly of pilots), the design and development of the aircraft itself, and research into aircraft characteristics and control handling qualities.

Flight simulation

- A flight simulator is a device that artificially re-creates aircraft flight and the environment in which it flies, for pilot training, design, or other purposes.
- It includes replicating the equations that govern how aircraft fly, how they react to applications of flight controls, the effects of other aircraft systems, and how the aircraft reacts to external factors such as air density, turbulence, wind shear, cloud, precipitation, etc.
- Flight simulation is used for a variety of reasons, including flight training (mainly of pilots), the design and development of the aircraft itself, and research into aircraft characteristics and control handling qualities.

Flight simulation

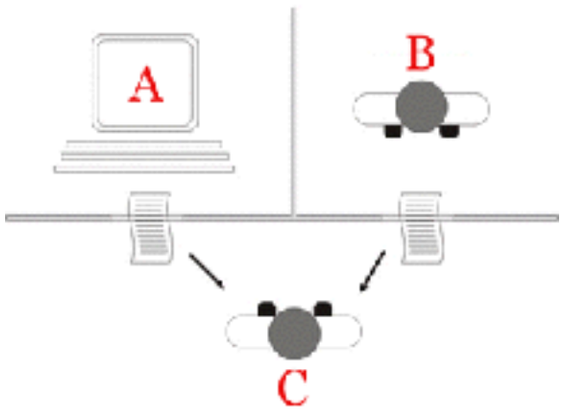
- A flight simulator is a device that artificially re-creates aircraft flight and the environment in which it flies, for pilot training, design, or other purposes.
- It includes replicating the equations that govern how aircraft fly, how they react to applications of flight controls, the effects of other aircraft systems, and how the aircraft reacts to external factors such as air density, turbulence, wind shear, cloud, precipitation, etc.
- Flight simulation is used for a variety of reasons, including flight training (mainly of pilots), the design and development of the aircraft itself, and research into aircraft characteristics and control handling qualities.

Artificial Intelligence

- In the field of computer science, artificial intelligence (AI), sometimes called machine intelligence, is intelligence demonstrated by machines, in contrast to the natural intelligence displayed by humans and other animals.
- Computer science defines AI research as the study of "intelligent agents": any device that perceives its environment and takes actions that maximize its chance of successfully achieving its goals.
- More specifically, Kaplan and Haenlein define AI as “a system’s ability to correctly interpret external data, to learn from such data, and to use those learnings to achieve specific goals and tasks through flexible adaptation”.
- Colloquially, the term "artificial intelligence" is used to describe machines that mimic "cognitive" functions that humans associate with other human minds, such as "learning" and "problem solving".

Turing test

- The Turing test, developed by Alan Turing in 1950, is a test of a machine's ability to exhibit intelligent behavior equivalent to, or **indistinguishable** from, that of a human.
- Turing proposed that a human evaluator would judge natural language conversations between a human and a machine designed to generate human-like responses.
- The **evaluator** would be aware that one of the two partners in conversation is a machine, and all participants would be separated from one another. The conversation would be limited to a text-only channel such as a computer keyboard and screen so the result would not depend on the machine's ability to render words as speech.
- If the evaluator cannot reliably tell the machine from the human, the machine is said to have passed the test. The test results do not depend on the machine's ability to give correct answers to questions, only how closely its answers resemble those a human would give.



Automatic Translation

- Machine translation, sometimes referred to by the abbreviation MT (not to be confused with computer-aided translation, machine-aided human translation (MAHT) or interactive translation) is a sub-field of computational linguistics that investigates the use of software to translate text or speech from one language to another.
- On a basic level, MT performs simple substitution of words in one language for words in another, but that alone usually cannot produce a good translation of a text because recognition of whole phrases and their closest counterparts in the target language is needed. Solving this problem with corpus statistical, and neural techniques is a rapidly growing field that is leading to better translations, handling differences in linguistic typology, translation of idioms, and the isolation of anomalies.[1][not in citation given]
- Current machine translation software often allows for customization by domain or profession (such as weather reports), improving output by limiting the scope of allowable substitutions. This technique is particularly effective in domains where formal or formulaic language is used. It follows that machine translation of government and legal documents more readily produces usable output than conversation or less standardised text.

Trans-humanism

- Transhumanism (abbreviated as H+ or h+) is an international philosophical movement that advocates for the transformation of the human condition by developing and making widely available sophisticated technologies to greatly enhance human intellect and physiology.
- Transhumanist thinkers study the potential benefits and dangers of emerging technologies that could overcome fundamental human limitations as well as the ethical limitations of using such technologies.
- The most common transhumanist thesis is that human beings may eventually be able to transform themselves into different beings with abilities so greatly expanded from the current condition as to merit the label of posthuman beings.

Ray Kurzweil

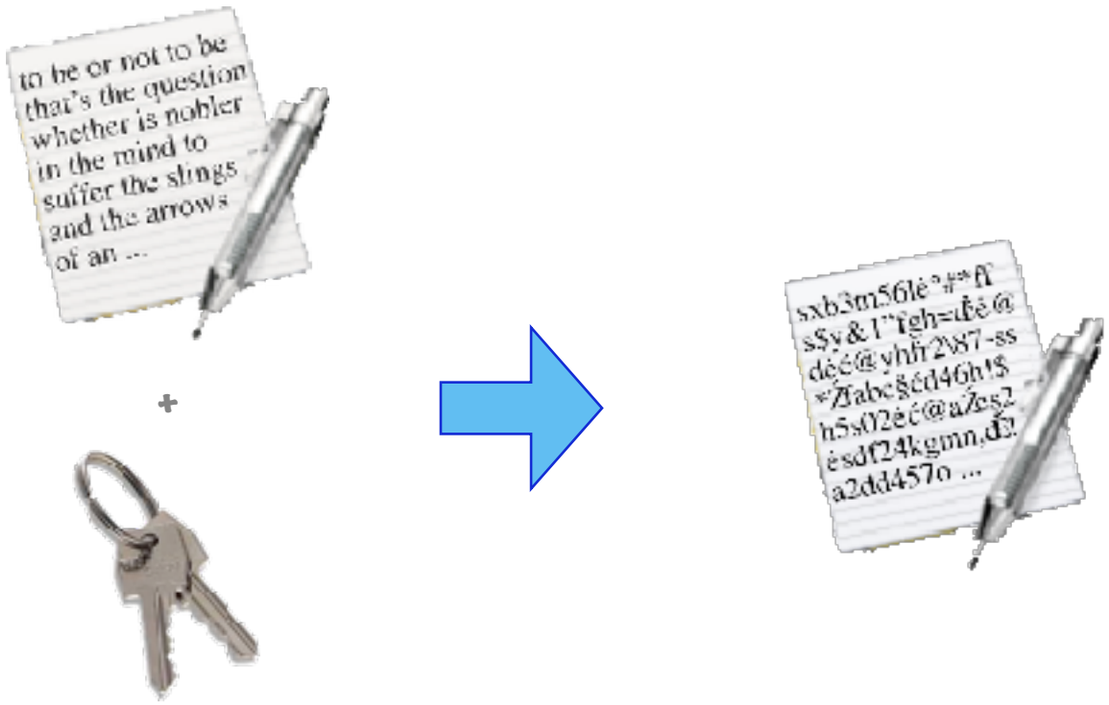
- Raymond Kurzweil is an American inventor and **futurist**. He is involved in fields such as optical character recognition (OCR), text-to-speech synthesis, speech recognition technology, and electronic keyboard instruments. He has written books on health, artificial intelligence (AI), transhumanism, the technological singularity, and futurism. Kurzweil is a public advocate for the futurist and transhumanist movements, and gives public talks to share his optimistic outlook on life extension technologies and the future of nanotechnology, robotics, and biotechnology.

- Kurzweil received the 1999 National Medal of Technology and Innovation, the United States' highest honor in technology, from President Clinton in a White House ceremony. He was the recipient of the $500,000 Lemelson-MIT Prize for 2001, the world's largest for innovation.[citation needed] And in 2002 he was inducted into the National Inventors Hall of Fame, established by the U.S. Patent Office.

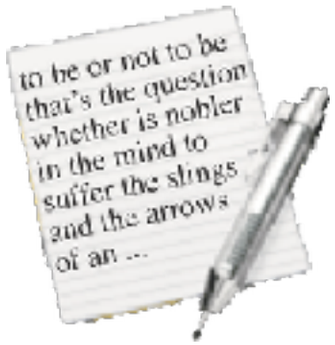
- He has received 21 honorary doctorates, and honors from three U.S. presidents. The Public Broadcasting Service (PBS) included Kurzweil as one of 16 "revolutionaries who made America" along with other inventors of the past two centuries. Inc. magazine ranked him #8 among the "most fascinating" entrepreneurs in the United States and called him "Edison's rightful heir".

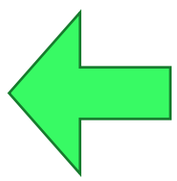
Cryptography

Cryptography in general



Cryptography in general





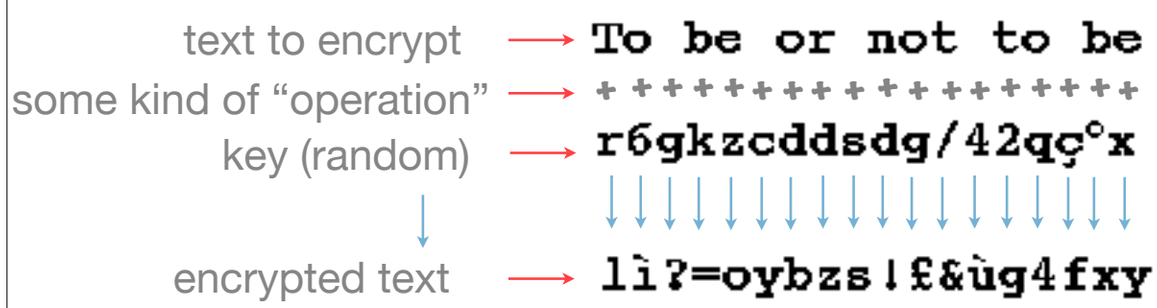
Cryptography in general

?

+

The Vernam protocol

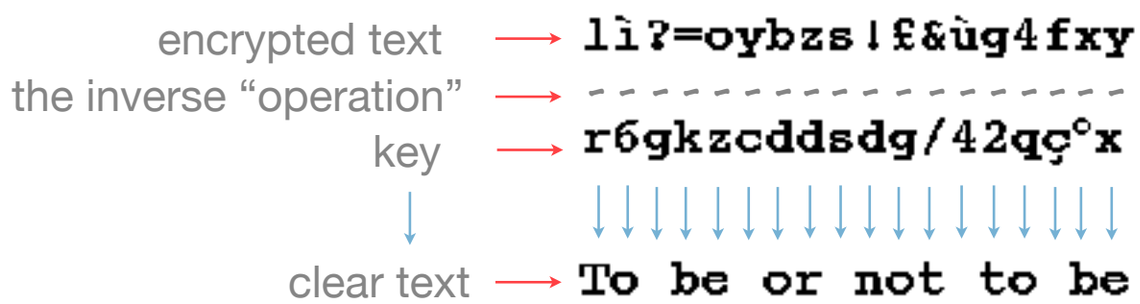
One example of cryptographic protocol is the **Vernam protocol**. It is proven to be 100% secure: the encrypted text has zero information content, in the Shannon sense



the “text characters” (text bits) are in a “1 to 1” relationship with “key characters” (key bits)

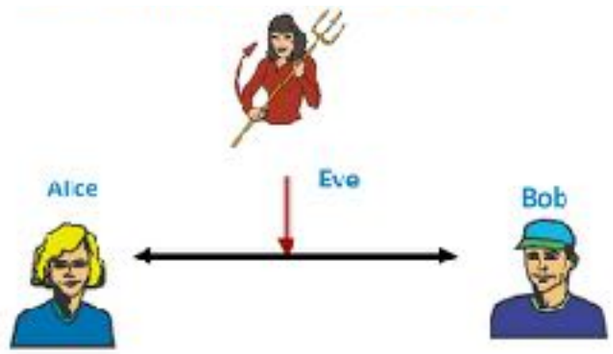
The Vernam protocol

One example of cryptographic protocol is the **Vernam protocol**. It is proven to be 100% secure: the encrypted text has zero information content, in the Shannon sense



Alice and Bob

- A message must go from “A” to “B”
- to help us think, let’s make it personal, and call the two parties “Alice” and “Bob”
- the goal of cryptography is for Alice to send a message to Bob without an *eavesdropper* to be able to read it
- We will call the eavesdropper “Eve” (she is evil!)



Public-key cryptography

- Public-key cryptography, or asymmetric cryptography, is a cryptographic system that uses pairs of keys
- a public key which may be disseminated widely, and a private keys which is known only to the owner.
- The generation of such keys depends on cryptographic algorithms based on mathematical problems to produce one-way functions.
- Effective security only requires keeping the private key private; the public key can be openly distributed without compromising security.

it is also called “asymmetric cryptography”

Public-key cryptography

- In an asymmetric key encryption scheme, anyone can encrypt messages using the public key, but only the holder of the paired private key can decrypt. Security depends on the secrecy of the private key.