Jan. 15th

Samuel Hawks Caldwell

Born: Jan. 15, 1904;

Massachusetts
Died: Oct. 12, 1960

Caldwell was part of the team at MIT that developed and built Vannevar Bush's [March 11] Differential Analyzer [July 23], but after WWII his interests turned to digital computing. He led the development of the Rockefeller Electronic Computer (REC) and contributed to Project Whirlwind [April 20]. The two projects had similar goals, and the REC was eventually abandoned, and its personnel and resources reassigned to the Whirlwind.

In 1959 he and Lien-Sheng Yang began working on the "sinotype", a keyboard for composing Chinese characters from line strokes mapped to the keys. Yang had determined the stroke-by-stroke 'spelling' of 2,000 common words, and they ultimately settled on supporting 22 strokes. A novel feature was that a character could be 'guessed' after the entry of the first few lines for it – an early form of "autocomplete".

Caldwell was an accomplished organist, occasionally playing with the Boston Symphony Orchestra.

William (Bill) Cleland Lowe

Born: Jan. 15, 1941;

Easton, Illinois
Died: Oct. 19, 2013

Lowe was known as the "father of the IBM PC" [Aug 12], a title he shares with Don Estridge [June 23].

Lowe handled the managerial side of the SCAMP project led by Paul Friedl, which became the IBM 5100 [Sept 9], and arguably the world's first portable.

In early 1980, Atari [June 27] approached Lowe, when he was head of IBM's Entry Level Systems, with the idea of having IBM sell one of its home computers rebadged with the IBM logo. This was a canny move by Atari as it was well known that IBM was seeking a quick entry into the home computer market. Lowe took the proposal to management, who pronounced it "the dumbest thing we've ever heard of."

Instead IBM CEO Frank Cary tasked Lowe with creating a plan for bringing an equivalent IBM product to market within a year. It was an Herculean task, but a prototype was ready by [Aug 8] 1980.

In mid-October [Oct 20], the committee approved Lowe's full plan, turning his team into "Project Chess". The fruits of their labors became the IBM PC.

ABC in the News

Jan. 15, 1941

A brief article in *The Des Moines Tribune* (on p.14 to be precise) described the progress of the Atanasoff-Berry computer (ABC) being built by John Vincent Atanasoff [Oct 4] and Clifford Berry [April 19].

This was the earliest published piece about the ABC although Atanasoff had prepared a 35-page paper [Aug 14] about the machine in 1940.

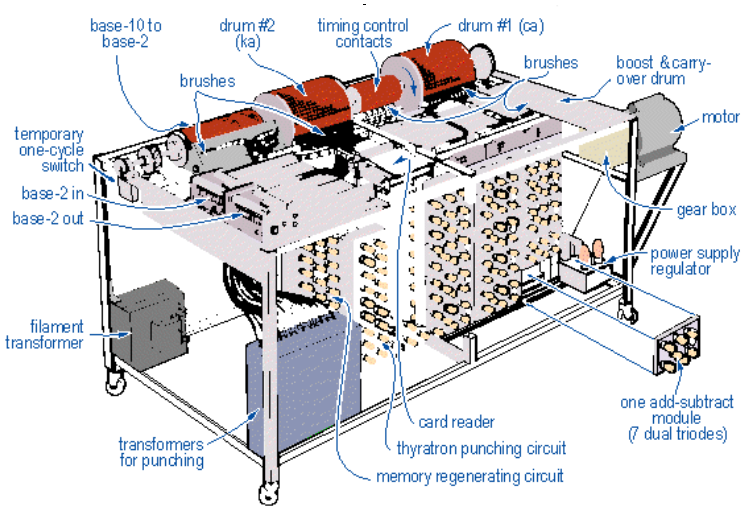


Diagram of the ABC. Ames Lab, Iowa.

The news item was accompanied by a photograph of Berry holding a large board of vacuum tubes under the caption "Machine Remembers." The text also included perhaps the first published comparison of a computer to a human brain.

Although the ABC had "computer" in its name, there's some debate about whether it deserves that title. It wasn't intended to be a general-purpose computer, focussing instead on solving simultaneous linear equations. This meant for example that it lacked stored program capabilities.

However, it did pioneer several important computing elements, including binary arithmetic, electronic switching, and drun memory that could store around 3000 bits. However, the original notion of drum storage was due to Gustav Tauschek [April 29], who patented his ideas in 1932.

The ABC was probably completed at the end of 1941, and George Snedecor, head of Iowa State's statistics department, was very likely its first user. This meant that he submitted his problem to Atanasoff who encoded and ran it.

Forrest Marion Mims III

Born: Jan. 15th 1944;

Houston, Texas

Mims was the author of the popular “Getting Started in Electronics” and “Engineer’s Mini-Notebook” series of instructional books that were sold by Radio Shack [Feb 2]. The notebook series was beautifully printed on graph paper, with hand-lettered text, copious line drawings, and schematics.

In 1960, Mims built an analog computer for a high school science fair that could translate twenty words in one language into another. Its memory was a bank of 20 screwdriver-adjustable trimmer resistors, which Mims dubbed the "Screwdriver-Programmable Read Only Memory" (SPROM).

In Dec. 1969, Mims co-founded Micro Instrumentation and Telemetry Systems (MITS) with Ed Roberts [Sept 13] . Their original aim was to produce miniaturized telemetry modules for model rockets. Later Roberts bought out Mims to refocus the company on calculators, which eventually led to the Altair 8800 microcomputer kit [Dec 19].

Knowing Mims' skills at writing, Roberts asked him to write the Altair's user manual in return for a free assembled machine.

Bruce Schneier

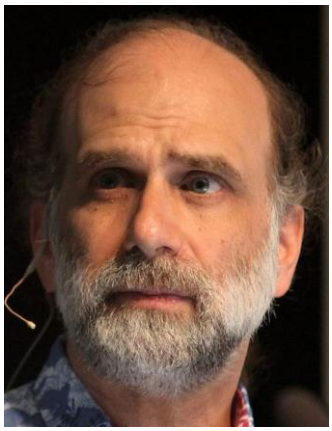
Born: Jan. 15, 1963;

New York City

In 1994, Schneier published “Applied Cryptography,” which expanded the cast of characters used to explain cryptographic algorithms and protocols beyond Alice, Bob, and Eve [Feb 00]. His dramatic personae included:

- Carol: a participant in three- and four-party protocols;
- Dave: the other contributor in the four-party protocols;
- Mallory: a malicious attacker;
- Peggy: a prover of protocols;
- Trent : a trusted arbitrator;
- Victor: a verifier of protocols;
- Walter: The warden who guards participants.

The well-known "Schneier’s law" was actually coined by Cory Doctorow [Jan 21] in a 2004 talk: “Any person can invent a security system so clever that he or she can’t imagine a way of breaking it.”



Bruce Schneier (2013). Photo by Rama. CC BY-SA 2.0 fr.

However, Schneier was the originator of the “movie-plot threat” – the way that governments sometimes justify their attacks on civil liberties by using scenarios reminiscent of the behavior of terrorists in action movies. A real-world example is the banning of baby carriers from subways because they might be packed with explosives. Between 2006 and 2015, Schneier ran an annual contest to create the most fantastic movie-plot threat. The results were posted to his blog.

A (rather depressing) quote: “I am regularly asked what the average Internet user can do to ensure his security. My first answer is usually ‘Nothing; you’re screwed’.”

Micral N

Jan. 15, 1973

The Micral N was the earliest commercial PC built around a microprocessor (the Intel 8008 [April 00]). The last part of this definition is important because the Kenbak-1 [Sept 00] from 1971 predates it as the earliest commercial PC **NOT** employing a microprocessor (it relied on transistors). Micral means “petit” in French slang.

Aside from the 8008, the Micral sported a bus (aka the pluribus), MOS-based memory, and serial and parallel IO cards. Its software included a rudimentary OS and an assembler.

The Micral N was designed by François Gernelle at the French company Réalisation d’Études Électroniques (R2E) as part of a one-off project funded by the Institut National de la Recherche Agronomique (INRA). Alain Perrier was planning to use the machine to analyze the water content of different soils for plant irrigation.

Work began in June 1972, with a deadline of December, which meant that Gernelle’s team were working 18 hours a day near the end, but the machine was delivered on this day.

In Feb. 1973, R2E started selling the Micral N commercially for just FF 8,500 (about $1,750), making it a cost-effective replacement for a minicomputer. Indeed, Perrier had originally thought to use a PDP-8 [March 22] for his project. Not surprisingly, it and later Micral models sold well.

In June 1973 the term “micro-ordinateur” (microcomputer) first appeared in print in reference to the Micral (although Isaac Asimov [Jan 2] had coined the English word in 1956). Gernelle was also awarded two patents, but neither mentioned micro-ordinateur since the patent agent refused to accept it as a real word.

By 1978 around 90,000 Micrals had been sold, but R2E never managed to crack the US market. In 1979 it sold the Micral brand to Bull [Dec 25], which used the name through the 1980's to label its PC clones.

A Micral was the first PC programmed by Philippe Kahn [March 16], but he may have been using a later 8080-based model, the Micral G or Micral S.

DES

Jan. 15, 1977

The Data Encryption Standard (DES) is a symmetric-key algorithm, meaning that it employs the same key to both encrypt and decrypt a message. DES was developed at IBM based on Horst Feistel's earlier Lucifer cipher.

DES was approved as a federal standard in Nov. 1976, and published on this day as FIPS PUB 46, making it the strongest legally exportable encryption software in the US. However, far stronger schemes were available in other countries. Indeed, critics argued that DES was too weak to be useful, and had probably already been broken by spy agencies. The main problem was that its key was only 56-bits long.

To prove the point, several US groups organized DES cracking competitions, such as the RSA Data Security challenges [Jan 28] [Feb 23]. DES Challenge III in 1999 broke a 56-bit key in just 22 hours 15 minutes.

On a positive note, Bruce Schneier [two entries back] has remarked, "DES did more to galvanize the field of cryptanalysis than anything else."

In 2005 DES was withdrawn, replaced by the Advanced Encryption Standard (AES). AES accepts keys of 128, 192, or 256 bits (which by today's standards are all pretty weak). AES is a subset of the Rijndael cipher developed by two Belgian cryptographers, Vincent Rijmen and Joan Daemen.

NCSA

Jan. 15, 1986

The National Science Foundation (NSF) opened the National Center for Supercomputer Applications (NCSA) at the University of Illinois, as one of the five new loci of the NSF's Supercomputer Centers Program. On [July 16], these institutions were linked together using the high-speed NSFNET.

Larry Smarr (1998). Photo by Dave Pape.

The Supercomputer program was initiated by Larry Smarr, who wrote an influential paper, "The Supercomputer Famine in American Universities" in 1982 after he'd been forced to travel to Europe to conduct his supercomputer-based research.

NCSA first gained prominence after its release of NCSA Telnet in 1986, which was followed by other useful networking tools; perhaps most famously, the Mosaic web browser [Sept 28 implemented by Marc Andreesen [July 9]. NCSA also hosted the HTTPd web server by Rob McCool, which later evolved into the Apache HTTP Server [Dec 1].

The AT&T Network Crash

Jan. 15, 1990

Over half of AT&T's long-distance network crashed for nine long hours, finally staggering back to life at 11:30pm, when the network loads were low enough to allow the system to stabilize. At the time AT&T carried over 70% of the US's long-distance phone traffic.

The cause was one of AT&T's New York switching centers after it performed a routine reset because it was nearing its load limits. As per standard procedure, the switch sent a message to nearby switches announcing that it would be taking no more calls until further notice. After the reset, (which took less than ten milliseconds), a second message was broadcast saying the switch was back in action.

Inexplicably, this closely-timed pair of messages caused the receiving switches to reset, which propagated the same deadly pairing to other switches. The network ended up being so busy repeatedly resetting itself that it couldn't do anything else.

The defect turned out to be due to a single line of buggy C code in some recently updated software: a `break` statement located within an `if` clause, that was nested within a `switch`. Worryingly, the update had passed through several testing stages before being deployed, and had worked fine throughout the busy Christmas holiday.

For more network outages, see [April 13], [April 20], [May 8], [Oct 4].

The Stealth Project

Jan. 15, 1991

Next: [April 8]

The first meeting of Sun Microsystem's "Stealth Project" (as named by Scott McNealy [Nov 13]) was held in Aspen, Colorado. Attendees included Bill Joy [Nov 8], Andy Bechtolsheim [Sept 30], Wayne Rosing, Mike Sheridan, James Gosling [May 19], and Patrick Naughton.

The project was the company's response to Naughton almost resigning to join NeXT [Sept 18]. Instead he circulated an e-mail detailing how he though Sun was going astray.

The meeting focused on brainstorming ways to build a network of consumer electronics devices that could be controlled with a handheld remote. In Feb., Naughton, Gosling, and Sheridan began working on the details: Naughton developed the "Aspen" graphics system,

Gosling concentrated on programming language ideas, and Sheridan on the business side.

In April the group moved out of Sun's headquarters, and was renamed the Green Project [April 8].

ZZT Released

Jan. 15, 1991

ZZT was an ASCII-based action-adventure puzzle game developed by Tim Sweeney, the first to feature a built-in game editor. In fact, gaming hadn't been Sweeney's initial aim; he had started out to write an MS-DOS text editor using Turbo Pascal [Nov 20], then decided to make the project more fun by adding game-like elements. He created the game engine and editor first, and then built his game worlds using them.

ZZT was sold as a shareware [May 29] title, consisting of one free world called the Town of ZZT. If players liked it, they could send money to buy more levels. Alternatively, thanks to the built-in scripting language called ZZT-OOP, creators could create their own worlds and even modify the behavior to produce games in different genres, from turn-based text adventures to a Lemmings clone [Feb 14]. Sweeney started a level designer contest for registered users; over 200 worlds were submitted.

The success of ZZT allowed Sweeney to found Potomac Computer Systems (named after his home town of Potomac, Maryland). He changed the name to "Epic MegaGames" in Oct. 1991 to make it sound more grandiose, but dropped the "Mega" in 1999 after the success of Unreal Engine [July 1].

The game's name was picked so it would be listed last alphabetically in shareware catalogs and on bulletin boards. A fan later suggested the backronym of "Zoo of Zero Tolerance".

USB

Jan. 15, 1996

The USB (Universal Serial Bus) 1.0 specification, supporting data transfer rates of between 1.5 and 12 Mbit/s, was released Seven companies (Compaq, DEC, IBM, Intel, Microsoft, NEC, and Nortel) had been involved in its development, which had started in 1994.

However, the first widely used version of USB was 1.1, released in Sept. 1998, and utilized by the iMac G3 [May 6]. The iMac was also the first computer to offer USB ports as standard, including for its keyboard and mouse. Earlier Mac peripheral connectors, such as ADB, SCSI [March 3], and the GeoPort, were discarded.

Memorably, USB 1.1 was showcased at the 1998 COMDEX [Dec 3] in Las Vegas. At a news conference, an Intel team attached 127 peripherals to one PC, with Bill Nye (the Science Guy) plugging in the last device. A document was then output to a stage full of different printers.

Many USB specifications have followed, each offering increased data transfer speeds. The USB 4 specification was published in August 2019, supporting a maximum transfer rate of 40 Gbit/s. One giant leap forward that debuted in the USB cable's type-C iteration was that it can be inserted into a port in any direction (i.e. it has a rotationally symmetrical connector) .

Wikipedia

Jan. 15, 2001

Wikipedia was launched by Jimmy Wales [Aug 7] and Larry Sanger who coined the name as a mashup of wiki [March 25] and encyclopedia. The domain wikipedia.org had gone live two days earlier.

Wikipedia's early entries were taken from Nupedia [March 9], Slashdot postings [Oct 5], and web search engine results, and by Aug. 8, had reached over 8,000 articles (which seemed big at the time). By comparison, the current English version of Wikipedia (Dec. 2020) holds 6.2 million articles, and if all the language versions are counted, this rises to nearly 56 million, in over 250 languages. In recent years, the number of new entries in English has been slowing, but the other languages have taken up the slack.

English Wikipedia reached 6 million entries on Jan. 24, 2020, with the addition of an item about Maria Elise Turner Lauder, a 19th-century Canadian school teacher. The article was written by Rosie Stephenson-Goodknight, a longtime Wikipedia editor.

On Jan. 12, 2021 (at around 1am), the billionth edit to an English language Wikipedia page was carried out by "Ser Amantio di Nicolao"; he modified information about Alec Empire's "Death Breathing" album. However, the patchy recording of edits from the early days of Wikipedia suggests that this milestone was actually reached a few days sooner.

As of Feb. 2021, Steven Pruitt has made over 4 million edits to Wikipedia's English content and 35,000 original articles under the "Ser Amantio di Nicolao" alias (a minor character in Giacomo Puccini's 1917 opera *Gianni Schicchi*). According to *Northern Virginia Magazine*, "Pruitt has not literally pressed the "edit" button 4.4 million times. One method he's used is a tool that allows a user to make numerous identical edits simultaneously. Pruitt was named one of the 25 most important influencers on the Internet by *Time* magazine in 2017.

On [Dec 15] 2005, the journal, *Nature* published a paper comparing 42 science articles from Encyclopædia Britannica [Dec 6] and Wikipedia. It found that their levels of accuracy were similar.

The earliest known proposal for an online collaborative encyclopedia was made by Rick

Gates on Oct. 22, 1993 in the USENET newsgroup alt.internet.services. The Interpedia project was actively discussed for several months, but never left the planning stage.

Today is informally known as “Wikipedia Day”; informal in the sense that it hasn't been decreed as a holiday by Wales. His approved holidays are:

- Jan. 25: Magnus Manske Day
- April 20: Justin Knapp Day
- June 1: Brion Vibber Day
- Oct. 31: Tim Starling Day

For more details, see `https://en.wikipedia.org/wiki/Wikipedia:Wikipedia_holidays`