August 16th

Transatlantic Cable

Aug. 16, 1858

Queen Victoria sent the first official telegraph message from London across the Atlantic Ocean to US President James Buchanan in Washington D.C. The telegraph cable link had been completed on [Aug 5].

Buchanan sent back a flowery missive, including the verbiage, "May the Atlantic telegraph, under the blessing of heaven, prove to be a bond of perpetual peace and friendship between the kindred nations, and an instrument destined by Divine Providence to diffuse religion, civilization, liberty, and law throughout the world."

The reception across the cable was terrible, with it taking around two minutes to transmit each character. As a consequence, the President's message took 17 hours and 40 minutes to deliver.

Two weeks later, on Sept. 3, the cable failed during an attempt to increase transmission speed. The voltage on the line was boosted from 600V to 2,000V, and the insulation on the cable proved inadequate.

It would be six years before enough money was raised to lay another cable. The new connection was completed in 1865, and following some setbacks, was put into service on July 28, 1866. This cable proved more durable, although also sometimes expensive [Nov 23].

Hollerith and US Census 1890

Aug. 16, 1890

Prev: [April 17]

After Herman Hollerith [Feb 29] won the competition [April 17] to process the 1890 census data, his machines (key punches, tabulators, and sorters) went to work in July. Clerks began punching holes in cards to record age, state of residence, gender, and other information from the returns.

Replica of a 1890 Hollerith tabulating machine. Photo by Adam Schuster. CC BY 2.0.

The first task was a general tally of the population, and Hollerith devised a special counter for the job – a typewriter-like device equipped with twenty keys, numbered 1 to 20. It allowed a skilled operator to process up to 50,000 people in a single day.

On this day, only six weeks after the count had begun, the census tally was completed: 62,622,250 (or perhaps 62,947,714). With great fanfare, the figure was announced in October, but because it was far lower than the 75 million expected, it led to some unfounded criticism of the accuracy of Hollerith's machines.

However, the general view of Hollerith's work was best summarized in the Nov 11, 1891 issue of *The Electrical Engineer*: "This apparatus works as unerringly as the mills of the gods, but beats them hollow in speed."

Although it took 2.5 years to complete the census, it was estimated that Hollerith's automation saved the government over 5 years of work, and over $1 million.

Marian Adam Rejewski

Born: Aug. 16, 1905;

Bydgoszcz, Poland
Died: Feb. 13, 1980

Rejewski was a skilled cryptologist in the Polish Cipher Bureau who became the first person to break the Enigma code [Feb 23] on Nov. 10, 1932, with the help of two young mathematicians, Jerzy Rozycki and Henryk Zygalski.

In Oct. 1936, the Germans started using more plugboard pairs in their Enigma machines, making it much harder to break its code. In response, Rejewski built a machine to assist with the mathematical analyses, which he called the cyclometer.

In Sept. 1938, the Germans changed the Enigma machine's internals again, and the Poles responded by creating the bomba, short for "cryptologic bomb" (the Polish is "bomba kryptologiczna"). It emulated six Enigma machines simultaneously, and allowed a user to test over 17,000 possible settings every two hours.

The reason for calling it a "bomb" is unclear. One story is that it relates to a beloved Polish ice-cream dessert of the same name. A more likely reason is due to the noises it made during operation. A US Army report of the time noted that a loud noise was generated by a weight dropping from the machine when a possible solution was found.

Five weeks before the German invasion of Poland on Sept. 1, 1939, Rejewski and his colleagues presented their work to French and British intelligence at a secret meeting in a forest in Pyry near Warsaw. It was this gift that first enabled the British to read Enigma-encrypted messages. In particular, Alan Turing [June 23] visited the Polish codebreakers and applied their knowledge to develop his own "bombe" [March 18].

When Rejewski escaped to England in Aug. 1943, he was assigned the job of cracking ciphers based on the Doppelkassettenverfahren ("double Playfair") system. Cryptologist Alan Stripp later suggested that setting him to work on this was like "using racehorses to pull wagons."

Peter Richard Samson

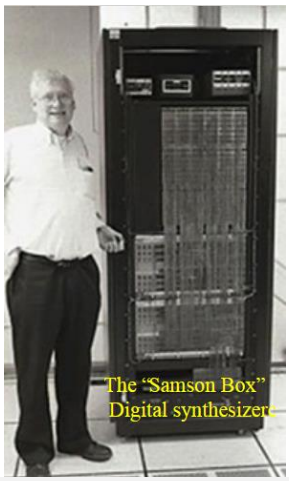
Born: Aug. 16, 1941;

Fitchburg, Massachusetts

As a member of the Tech Model Railroad Club (TMRC [Sept 6]), Samson made numerous contributions to the Signals and Power Subcommittee, the technical side of the club.

His interest in music synthesis, led him to create the "Harmony Compiler" so people could encode and play music on MIT's PDP-1 [Nov 00]. Perhaps the most famous piece it played was Mozart's "Eine Kleine Nachtmusik".

In the late 1970s, he designed the Systems Concepts Digital Synthesizer, then the world's largest, most capable music synthesizer. For more than a decade, it served as the principal compositional tool for the computer music group at Stanford. The "Samson box" resembled a 'green fridge', but was actually a dedicated PDP-6.



From "A Brief History of CCRMA" by John Chowning. Stanford Historical Society.

Samson also wrote the "Expensive Planetarium" star display used in Spacewar! [May 17] to heighten the game's realism. It included every star in a band between 22.5° N and 22.5° S in the night sky, and displayed them at their relative brightness. Spacewar! also inspired Samson and Alan Kotok [Nov 9] to write T-Square, a drafting program that employed a Spacewar! controller as its input device.

His TJ-2 (Type Justifying) system, released in May 1963, was probably the first page layout program. It aligned left and right margins, justifying the output using white space and word hyphenation. Its inspired TYPSET and RUNOFF [Nov 6] for the CTSS OS [May 3], which evolved into runoff for Multics [Nov 30], and roff and nroff for UNIX [Oct 15].

In 1966, Samson's interest in the NYC subway system led him to tabulate all the train schedules so that he could calculate the minimum-transfer path from any station to any other (the program was written in LISP [April 15]). The results were put to a test on March 31, 1966, with the complete subway traversal taking 25 hours, 57 minutes, and 24 seconds; the event attracted considerably media attention.

Jarkko Oikarinen

(aka WiZ)

Born: Aug. 16, 1967;

Kuusamo, Finland

In Aug. 1988, Oikarinen released a server and client that supported Internet Relay Chat (IRC), a protocol for text communication. It was mainly intended for group discussion forums, but also handled one-on-one private messages and file sharing.

Oikarinen had been inspired by Jyrki Kuoppala's "rmsg" program, and by BITNET [May 5] Relay Chat.

IRC became known to the general public in 1991, when an IRC link into Kuwait stayed operational for a week after radio and television broadcasts were cut off after Iraq's invasion.

Telenet Operational

Aug. 16, 1975

Telenet was the first packet-switched network service available to the general public. Its use of the X.25 protocol (as defined in *The Orange Book* [Aug 15]) gave that approach a big boost for use in wide-area networks but gradually IP became more popular [Jan 1].

Telenet was established by Bolt Beranek and Newman (BBN [Oct 15]) in Jan. 1975 and recruited Larry Roberts [Dec 21] as its CEO. The network initially had nodes in seven US cities: Washington, D.C., Boston, New York, Chicago, Dallas, San Francisco, and Los Angeles,

It was later acquired by Sprint and renamed "Sprintnet".

King's Quest IV

Aug. 16, 1988

Sierra Entertainment [Oct 30] released "King's Quest IV: The Perils of Rosella" for PCs, making it the first major graphical adventure game with a female protagonist. The player takes on the role of Princess Rosella, who must save her father and defeat an evil witch. It became the most successful game of the year.

It was also the first commercial game to support PC sound cards and synthesizers such as the AdLib and Roland MT-32 [Nov 16]. This allowed it to include realistic sound effects and an orchestrated score which had been impossible with a one-channel PC speaker.

Typing in curse words would generated the message: "Perhaps you need to purchase a copy of Leisure Suit Larry?" [July 5]. Typing "undress" or "remove clothes", would bring up the

comment, “Not in front of the game players!”

Solar Flares

Aug. 16, 1989

A geomagnetic storm caused by a very large solar flare led to the halt of Toronto’s stock market. The flare was even stronger than the one from five months before which had caused the shutdown of Hydro-Québec’s electricity transmission system. There were concerns that this event was part of a Cold War attack.

Both flares were actually part of the 22nd solar cycle recorded since 1755. This cycle lasted nearly ten years, beginning in Sept. 1986 and ending in Aug. 1996.

On July 23, 2012, the most powerful solar storm for 150 years just missed the Earth. NASA said that if we had been hit, technology might have been knocked back by hundreds of years. It was comparable to the Carrington Event [Sept 1] of 1859.

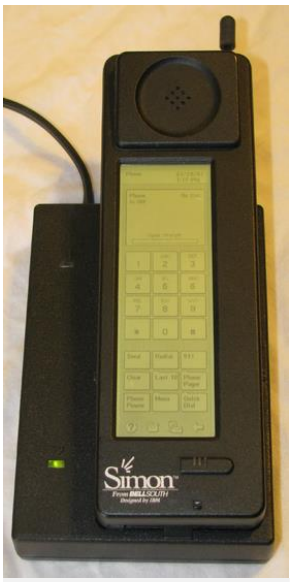
IBM Simon Debuted

Aug. 16, 1994

The IBM Simon Personal Communicator was the first cellular phone to include telephone and PDA features in one device. It's widely considered to be the first smartphone, and appeared a year before that term was coined by Pamela Savage (in an article entitled “Designing a GUI for business telephone users”).

Simon featured a monochrome 640 x 200 pixel LCD touchscreen measuring 4.5 by 1.4 inches, a stylus, 1 MB of RAM, and 1 MB of storage.

Software included a notes-taking application, an address book, calendar, world clock, and a way to schedule appointments. Problems with the software had led to Simon's release being delayed, but IBM had first demoed a prototype, codenamed “Angler,” at COMDEX in 1992.



IBM Simon in its charging station. Photo by Bcos47.

Approximately 50,000 units were sold during the six months it was on the market.

Hal’s SSL Challenge

Aug. 16, 1995

Damien Doligez won "Hal’s SSL Challenge" by cracking SSL [Dec 23] data inside a Netscape [March 25] browser protected by a 40-bit RC4 encryption key. The challenge had been set up on July 14 by Hal Finney to highlight how easy it was to crack 40-bit keys, since that size meant that there were only around a trillion (10^{12}) possible values for the key. Netscape was utilizing such a weak method in order to comply with the requirements of the US government for exportable cryptographic software [June 5].

Doligez broke into the data after eight days by running a brute force search through all the possible key values by employing 112 networked workstations. That sounds like quite a long time, but the machines were quite old (even in 1995), and Doligez estimated that he could have got roughly the same speed on a network of 40 to 50 PCs with Pentium processors [March 22].

The uselessness of small-bit encryption was clearly shown a few years later in 1998, when the Electronic Frontier Foundation’s (EFF [July 6] "Deep Crack", built for just $250,000, broke a 56-bit Data Encryption Standard (DES [Jan 15]) key in days. The machine was capable of testing over 90 billion keys per second.

Most current Web browsers use at least 2048-bit RSA encrypyted keys [Aug 00], which are considered reasonably strong, at least until quantum computers become somewhat more powerful [Dec 19].

Internet Explorer

Aug. 16, 1995

Next: [March 18]

Microsoft Internet Explorer (MSIE, later just IE) made its debut as part of Microsoft Plus! for Windows 95 [Aug 24]. At this stage, the IE team consisted of just six people, led by Benjamin Slivka [Aug 15]. Such a small team was only viable because Microsoft had licensed much of its browser technology from Spyglass [April 5].

IE 1.5 was released several months later for Windows NT and included free of charge with that OS. Incidentally, this meant that Microsoft didn’t have to pay any royalties to Spyglass (only a quarterly fee), which resulted in Spyglass filing a lawsuit [Jan 22].

After passing through numerous versions, IE became the most widely used Web browser, attaining a staggering 95% usage share in the early 2000's. That declined almost as rapidly after the launch of Firefox ([Nov 9] 2004) and Google Chrome ([Sept 2] 2008).