May 6th

Ronald Linn Rivest

Born: May 6, 1947;

Schenectady, New York

In 1977, Rivest co-invented the RSA encryption algorithm [Sept 6] with Adi Shamir [July 6] and Leonard Adleman [Dec 31] (RSA comes from the first letters of their last names).

He was also the inventor of the symmetric key encryption algorithms RC2, RC4, RC5, and co-inventor of RC6. The "RC" stands for "Rivest Cipher", or alternatively "Ron's Code". RC3 is missing from the list because its encryption was broken during the algorithm's development and so was scrapped; similarly for RC1.

He also found time to author the MD2, MD4, MD5 and MD6 cryptographic hash functions. "MD" stands for "Message-Digest", which is a bit of a let down after "Ron's Code".

In 2006, he published the ThreeBallot voting system, a scheme that incorporates the ability for the voter to check that their vote was counted while still protecting their privacy. Surprisingly perhaps, this system doesn't rely on cryptography.

He's a co-author of "Introduction to Algorithms", the standard textbook on algorithms, with Thomas H. Cormen, Charles E. Leiserson [Nov 10] and Clifford Stein. It is one of the most cited publications in computer science.

EDSAC Squares

May 6, 1949

The Electronic Delayed Storage Automatic Computer (EDSAC) was probably the first practical stored-program computer. It was certainly the first to be utilized as part of a regular computing service, at the University of Cambridge, where the machine's development was led by Maurice Wilkes [June 26]. Work began officially in 1947, although Wilkes started sketching out the design while attending the Moore School Lectures [July 8] in Philadelphia, and during his return voyage across the Atlantic on the Queen Mary [Aug 19].

On this day, EDSAC successfully ran its first program, written by Wilkes, to calculate a table of squares. The moment was recorded in the machine log:

"Machine in operation for first time. Printed table of squares (0-99), time for programme 2 mins 35 secs."

Later the same day, it ran a program that calculated a sequence of prime numbers.

The EDSAC used 3,000 vacuum tubes, and 16 mercury delay lines to offer a total of 512 words (of 18- bits each) of memory (extended to a magnanimous 1024 words in 1952). Each delay line was 5-feet long, machined to an accuracy of a thousandth of an inch, and stored in a long box that looked not unlike a coffin.

M.V. Wilkes: O death, where is thy sting?

During a discussion on what liquid to use in the lines, Alan Turing [June 23] had advocated gin, which he said contained alcohol and water in the right proportions.

In modern times, rebuilding the EDSAC was hampered by regulations against the large-scale use of mercury in the delay lines. Sadly they went with a nickel-based solution rather than Turing's suggestion.

J. Presper Eckert [April 9] originated the idea of using mercury delay lines for memory [July 15], and employed them in the BINAC [April 4]. This approach was readily understood by Wilkes due to his radar work with delay lines during WWII. Wilkes was also fortunate to employ William Renwick as his chief engineer, who had spent much of the war working with the same technology.

There's a highly contested debate over which computer was the first to implement von Neumann's stored program concept. The other contenders are the Manchester Baby [June 21] (an experimental machine), and the BINAC [April 4] (which suffered from reliability problems).

In any case, the EDSAC achieved several software and programming firsts. For example, Wilkes established a library of short programs (which he termed "subroutines"), stored on punched paper tape for use in solving problems.

In 1950, Wilkes and David Wheeler [Feb 9] used EDSAC to solve a differential equation relating to gene frequencies, the first application of a computer to a problem in biology. EDSAC was also the first machine to find new prime numbers [June 7]. In 1952, Sandy Douglas [May 21] developed OXO, a version of noughts and crosses (tic-tac-toe) that may well have been the world's first computer game.

µA741 Op-Amp Announced

May 6, 1968

Operational amplifiers (op-amps) have been called the "sliced bread" of analog design: you can combine them with almost anything and get something satisfying.

The first op-amp to go on sale was the μA702 in 1963, developed by Robert Widlar and Dave Talbert at Fairchild Semiconductors [Oct 1]. Widlar followed it up with the improved μA709, slashing the price from $300 to $70, making it a huge success. However, when he failed to get a raise as a reward, he moved to National Semiconductor where he created the even better LM101 in 1967.

Back at Fairchild, David Fullagar (who started work at the company the week after Widlar had left) realized that the LM101 had a few drawbacks. He incorporated circuitry to make the amplification smoother – a fixed internal capacitor – which also meant his μA741 didn't require any additional external components. The μA741 became the op-amp standard, selling in the hundreds of millions. Its success was apparent almost from the start; on June 7, Fairchild issued an internal memo with the subject line "We've Got a Winner".

Xerox Dorado

May 6 – 8, 1980

The first conference paper about the Xerox Dorado, "A processor for a high-performance personal computer", was presented by Butler W. Lampson [Dec 23] and Kenneth A. Pier.

The Dorado was a follow-up to the Alto [March 1] intended as a research machine to test out new ideas. The main aim was to increase performance while retaining the sophisticated programming environment, which included Cedar and Smalltalk-80 [May 17]. It also added support for virtual memory which addressed a major weakness of the Alto.

The implementation of a prototype Dorado "Model 0" began in the Computer Science Lab (CSL) at PARC [July 1] in 1977, led by Lampson, Chuck Thacker [Feb 26], and Ron Rider. The next version, the Dorado "Model 1", was operational by the spring of 1979. By the fall of 1982, a production line had been set up that was delivering Dorados to PARC at the rate of three or four per month. Around 80 were in service by 1983.

The famous Dec. 1979 PARC demo [Dec 00] given to Steve Jobs [Feb 24] and others from Apple was done on a Dorado.

There were several other research machines aside from the Dorado, all with names beginning with "D", and so known as "the D-machines": the Dandelion (least powerful), Dolphin; Dorado (most powerful); and hybrids like the Dandel-Iris.

The innovations tested in the Dorado series would eventually be commercialized in the Xerox Star 8010 [April 27].

iMac G3 Unveiled

May 6, 1998

Steve Jobs [Feb 24] introduced the iMac G3 at the Flint Center Theater, the same venue where the Mac had debuted on [Jan 24] 1984.

Even before its release on Aug. 15, Apple received an unprecedented 150,000 orders for the machine, marking the beginning of the company's renaissance. It also ushered in the era of Apple adding the letter "i" to just about every product.

Ken Segall had come up with the "iMac" name, while Jobs preferred "MacMan", but was eventually brought around. Segall was also part of the team that created the "Think Different" campaign [Sept 28].

The iMac utilized a PowerPC G3 [Oct 2] processor, a 15in display, and a 4GB - 60GB hard drive. Rather shockingly, it abandoned the floppy drive and the Apple Desktop Bus connector in favor of the emerging USB standard [Jan 15].

The inclusion of only a CD-ROM drive [Sept 1] meant that there was no way to write files to a removable device without an add-on. This was a big gamble since it assumed that most people would transfer files via a network. Eventually the rise of USB keychains alleviated the problem, but they were far from common at the time.

The iMac came with the Apple USB Mouse, commonly known as the "Hockey Puck" (because of its shape), which echoed back to one of the first mice, the Rollkugel [Oct 2].

Most obviously, the iMac sported a radically different look – a gumdrop-shaped, colored, translucent plastic case, designed by Jonathan Ive [Feb 27]. In particular, its all-in-one design did away with most wires and cables, a particular bugbear for Jobs.

The first iMac was later known as the "Bondi Blue" because of its color, and later releases took the number of colors to thirteen [Feb 22].

Bondi Blue. Photo by Masashige Motoe. CC-BY-SA-2.0.

The iMac was also the first Mac without the rainbow colored Apple logo, which had first appeared on the Apple II in [April 15] 1977.

Eve Online Launched

May 6, 2003

Eve Online is a space-based massively multiplayer online role-playing game (MMORPG), noted for its storylines created mostly by the players themselves.

A typical adventure involves economic competition, galactic warfare across 7,800 star systems, planetary heists, and political scheming. The game has been called the “largest collective work of collaborative science fiction”, the work of hundreds of thousands of contributors. It’s also been described as “spreadsheets in space” and “the most thrilling boring game in the universe.”

The “Bloodbath of B-R5RB”, a battle involving thousands of players in a single star system, lasted for 21 hours, and is considered one of the largest fights in gaming history.

Eve Online was developed by the Icelandic video gaming company, CCP Games, founded in June 1997 by Reynir Harðarson, Þórólfur Beck Kristjónsson and Ívar Kristjánsson. To finance the development, they first released a board game, called Hættuspil (“Danger Game”), which sold more than 10,000 copies to Iceland’s 80,000 households.

The installer for "Eve Online: Trinity", released in Dec. 2007, was found to have a nasty bug because of an incorrectly coded file path name. Instead of deleting its own boot.ini file, it would remove MS Window's boot.ini, which could sometimes cause the machine not to start when it was next booted.

Non-Latin Web

May 6, 2010

The first completely non-latin web addresses (more formally known as Internationalized Domain Names (IDNs)) debuted when Egypt, Saudi Arabia, and the United Arab Emirates were assigned country codes in Arabic. They are: Egypt: مصر Saudi Arabia: السعودية and the United Arab Emirates: امارات

One of the first websites was the Egyptian Ministry of Communications and Information Technology (MCIT), located in Smart Village Egypt.

The Internet wasn’t designed to be multilingual. Specifically, the domain name system (DNS) only supports the characters a through z, A through Z, 0 through 9, and the hyphen: the the Letter-Digit-Hyphen (LDH) subset. The change wasn't achieved by upgrading DNS's alphabet. Instead a multilingual translation service was added to the browser which converts an IDN into an odd-looking combination of ASCII characters, known as punycodes.

IDN was first proposed in Dec. 1996 by Martin Dürst, and implemented in 1998 by Tan Juay Kwang and Leong Kok Yong under the guidance of Tan Tin Wee.

One increasingly severe security problem with IDNs is their use by scammers to trick users into visiting fake websites. For example, paypal.com and paypal.com are actually two different domains; the first one uses the Cyrillic “p”. The punycode version of the first is: https://www.xn--ayal-f6dc.com/