Course Handout - Short-Term Memory Subtypes in Computing and Artificial Intelligence
Part 3 - A Brief History of Computing Technology, 1943 to 1950

First published online 12:12 GMT 27th January 2003. **This version [refresh hyperlinks after 20 years and remount as a .pdf] dated 10:00 GMT 29th February 2024**

This is the third part of a seven-part review of how successfully the psychological study of biological short-term memory (STM) has incorporated the full range of concepts and metaphors available to it from the computing industry. The seven parts are as follows:

Part 1: An optional introductory and reference resource on the history of computing technology to 1924. This material follows below and starts to introduce the vocabulary necessary for Parts 6 and 7. To go back to Part 1, click here.

Part 2: An optional introductory and reference resource on the history of computing technology from 1925 to 1942. This will further introduce the vocabulary necessary for Parts 6 and 7. To go back to Part 2, click here.

Part 3: An optional introductory and reference resource on the history of computing technology from 1943 to 1950. This will further introduce the vocabulary necessary for Parts 6 and 7. In so doing, it will also refer out to three large subfiles reviewing the history of codes and ciphers, and another subfile giving the detailed layout of a typical computer of 1950 vintage. The main sections are:

14 - Hardware Summary Table, 1943-1950

Part 4: An optional introductory and reference resource on the history of computing technology from 1951 to 1958. This will further introduce the vocabulary necessary for Parts 6 and 7. To go directly to Part 4, click here.

Part 5: An optional introductory and reference resource on the history of computing technology from 1959 to date. This will further introduce the vocabulary necessary for Parts 6 and 7. To go directly to Part 5, click here.

Part 6: A review of the memory subtypes used in computing. To go directly to Part 6, click here.

Part 7: A comparative review of the penetration (or lack thereof) of those memory subtypes into psychological theory. To go directly to Part 7, click here.

1 - Computerised Cryptanalysis

Clever though the ABC and Z3 (see Part 2) may have been, the fates chose to ignore them. They were not *lucky* systems. They lacked political, financial, and/or academic clout, and as a result simply got sidelined by history. Atanasoff's Iowa State biographers assure us that he left filing the patent to his University, who then lost the paperwork, and when Zuse's prototype was demonstrated to the Wehrmacht they decided that the system's benefits were unlikely to justify the development costs. But there were lucky systems as well, and while Zuse had been funding the Z3 largely out of his own salary, the big boys were about to sink fortunes into computer development projects which could not be allowed to fail. Three main wartime driving forces may be identified, namely (a) computation for code breaking, (b) computation for ballistics, and (c) computation for the nuclear physicists developing the atomic bomb. The next six items specifically address the first of these histories.

1.1 Computerised Cryptanalysis (1930-1939 - The Polish *Bomby*)

The story of mechanically assisted cryptography began with simple contrivances like Alberti's cipher disk, and moved on during the 1920s to multiple disk keyboard scramblers such as the German Enigma system. The technology was then blooded in Poland during the run-up to the Second World War, when, as likely enemies of a resurgent Germany, the Poles resolved to decipher their neighbour's Enigma traffic. This exercise began as soon as the German army adopted the Enigma system in 1928 (Bury, 2002), and involved three mathematics graduates from Poznan University - Marian Rejewski, Jerzy Rozycki, and Henryk Zygalski. These three young men were recruited straight out of university into a special *Biuro Szyfrów* (= Cipher Bureau) project in early 1930, and by painstaking work, plus experience of the simpler commercially available machines, managed by 1932 to work out the Enigma's internal wiring logic, that is to say, the top secret randomising connections pressed into the inner ring of each Hebern wheel. They immediately built a number of replica Enigmas of their own, and by January 1933 were deciphering live German transmissions.

Now the reason the Enigma story is central to the history of computing, is that the Poles also made significant progress automating the cryptanalytical process. By November 1938, they had developed a "***bomba kryptologiczna***", in which six of their replica Enigmas were mechanically linked together, and motor-driven through permutation after permutation until the output of one of them matched a pre-set target value, whereupon the whole contraption stopped automatically, with the probable Enigma *Grundstellung* clearly displayed.

> **ASIDE:** The point of using six replica machines, is that each had its rotors set in a different left-to-right order, one for each of the *Walzenlage* permutations possible with a three-from-three Enigma. The process could have

been executed on a single replica machine, but this would have been able to deal with only one *Walzenlage* at a time, so on an unlucky day would take up to six times as long to finish. **This is a very early demonstration of the advantage of *parallel* over *serial* processing.** The *bomby* allowed the Polish cryptanalysts to do all the necessary trial and error work at machine speed, and the system was so successful that Bury estimates that the *Biuro Szyfrów* decoded around 100,000 transmissions in the six years before Poland was eventually occupied. Kahn (1996, p975) describes the *bomby* as "the roots of protocomputers".

Unfortunately, the Poles lost the naval traffic on 1st May 1937, as a consequence of the Kriegsmarine tightening its operating procedures [see next section but two], and to rub salt into their wounds they then lost the army traffic on 15th December 1938, when the three-from-five Enigma was introduced.

ASIDE: As soon as the Germans increased the available rotor stock, the number of possible *Walzenlage* permutations started to shoot up. For example, there are 10 different ways of selecting three out of five rotors, and then - as before - six different ways of sequencing the three you have selected into the available slots, making 60 permutations in all. So in going from three to five rotors, it takes you from six to 60 permutations: one small step for the cryptographers, but ten times as much work for your enemies.

But what the Poles were really short of, of course, was time, and by late June 1939 it was apparent that the German invasion was not far off. The Polish Chiefs-of-Staff therefore resolved to share their accumulated Enigma secrets with their French and British allies. An approach accordingly went out through diplomatic channels, and ended up on the desk of Commander Alexander G.A. ("Alastair") Denniston (1881-1961).

BACKGROUND: Denniston had been a code breaking expert during World War One, and had kept "Blinker" Hall's Room 40 skill base alive by forming the Government Code and Cypher [sic] School (GCCS) in 1920. He had then run GCCS (known cryptically as "Station X") as a small peacetime unit attached to the Foreign Office, where it could serve the diplomatic and peacetime military intelligence worlds. The organisation was then progressively expanded during the 1930s, as it became more and more apparent that another war was on its way, and was moved out of London in 1938 to the newly acquired house and estate of Bletchley Park. It was from this base that it formed a key element in a high level British military intelligence project codenamed "Ultra".

Realising the potential importance of the Polish work, Denniston personally led a top-secret mission in late July 1939 to the *Biuro Szyfrów* station hidden in the *Lasy Kabackie*, the woods outside Pyry, a small town south of Warsaw. He was accompanied by Alfred Dillwyn ("Dilly") Knox (1884-1943), one of his long-term Room 40 colleagues, and Commander Humphrey Sandwith, of the naval intelligence service. Together, they toured the Polish decoding school, observed their methods, studied their thus-far-unsuccessful attempts to defeat the three-from-five Enigmas, and brought back specimens of the sort of paperwork which needed to be done before a *bomba* could be set to work. The Poles also offered them one of the replica Enigmas, and this seems to have been brought out of the country in a diplomatic bag a few days later, and collected personally by Colonel (later Sir) Stewart Graham Menzies, head of MI6, in a furtive suitcase-swap at London's Victoria Station during that August (Kahn, 1991).

ASIDE: As head of Britain's Secret Intelligence Service (MI6), Menzies would have been referred to within the profession as "C". The role (and possibly the person himself) was subsequently fictionalised as "M", by a certain Ian Fleming.

The German blitzkrieg against Poland finally began on 1st September 1939, and was followed two weeks later by a carefully synchronised Russian invasion from the east. Caught between two giants, the immediate military outcome was a foregone conclusion, and as their defences collapsed around them the *Biuro Szyfrów* destroyed its heavy equipment and evacuated its key personnel to France, where during October they became part of a joint French-Polish decryption unit known as "Bruno". This unit was housed in the Chateau de Vignolles (a sort of French Bletchley Park), at Gretz-Armainvilliers, just outside Paris, and there they

remained until the fall of France in June 1940, whereupon they had to be evacuated again, this time to Algiers [but that's another story - Ed.].

1.2 Computerised Cryptanalysis (1939 - The Jeffries Sheets)

Upon Denniston's return from Warsaw, he immediately reorganised his Bletchley Park resources. Not unreasonably, given the Polish successes, his strategy was (a) to recruit as many university geniuses as he could get his hands on, (b) to break back into the improved three-from-five and naval systems, (c) to pass the resulting intercepts to Churchill and his Chiefs-of-Staff, who would use the intelligence gained to help operational planning, and (d) to build some suitably wired *bomby* of his own. He then allocated his available staff to a number of "huts". Huts 6 and 3 would address the Army and Luftwaffe Enigma systems (Hut 6 doing the primary cryptanalysis, and Hut 3 handling the resulting translation and onward routing), Huts 8 and 4 would carry out cognate duties on the Kriegsmarine codes, and Hut 3N would ensure that nothing fell down the cracks between land, air, and sea. Two special Intelligence Sections (ISOS and ISK) would conduct primary cryptanalysis of the Abwehr traffic, although follow-up processing for this stream was carried out elsewhere by reason of its sensitivity (Twinn, 1993). W. Gordon Welchman (1906-1985) was made responsible for expansion of the establishment during that autumn as new staff poured in (Welchman, 1982), and additional units were set up as numbers grew. Here, by department, are some of the names mentioned in the literature:

Department	Officer Commanding	Team	Duties
Hut 3	Malcolm Saunders Eric (later Sir Eric) Jones (from mid-1942)	Frederick Norman; Ralph Bennett (from February 1941); William Millward (from April 1942); Telford Taylor (US liaison; from 1943).	Army and Luftwaffe Enigma translation and initial follow-up (supporting Hut 6).
Hut 3N (= Hut 3/4 Liaison)	N/K	Edward Thomas (from February 1942)	Covered the grey area where army, air force, and navy matters interact.
Hut 4 (aka "Naval Section")	Walter Eytan (Z Watch, from February 1941)	Harry Hinsley (from October 1939); Alec Dakin (from May 1940), Patrick Wilkinson; Charles Leech, Gordon Priest, Eric (later Sir Eric) Turner, Ann Toulmin; Leonard Forster; Ernest Ettinghausen; Thelma Ziman; Vivienne Alford; Peter Twinn	Naval Enigma translation and initial follow-up (supporting Hut 6).
Hut 6	Gordon Welchman (September 1939); Stuart Milner-Barry (1940)	Derek Taunt; Dennis Babbage	Army and Luftwaffe Enigma primary cryptanalysis.
Hut 8	Commander Edward (later Sir Edward) Travis Alan ("Prof") Turing	Joan Murray (June 1940); Hugh Alexander; Alex Kendrick; Jack Good (May 1941 to April 1943); Hugh Foss; Leslie Yoxall; Shaun Wylie; Michael Ashcroft; Richard Pendered	Naval Enigma primary cryptanalysis.
The Newmanry	Max Newman (from September 1942)	Jack Good (from May 1943); David Rees; Bill Tutte	

The Testery (Part of Block F)	Major Ralph Tester	Roy Jenkins; Alan Turing; Peter Benenson; Peter Hilton; Donald Michie	
Hut 7	John Tiltman		
The Cottage - Intelligence Sections OS and K	Oliver Strachey (= OS) and Dillwyn Knox (= K)	John Jeffries; Keith Batey; Mavis Lever; Margaret Rock	Abwehr non-Enigma and Enigma traffic respectively - cryptanalysis and onward despatch.

Denniston's strategy immediately led him to a young mathematician named Alan Turing .....

> **ASIDE:** In wartime, the military draw heavily on the services of civilian academics and engineers, especially in the areas of physics, mathematics, and telecommunications. These were routinely referred to as "boffins", and in this section we meet one of the boffinest, **Alan Mathison Turing** (1912-1954). Turing had achieved early academic fame with a 1937 paper entitled "On computable numbers, with an application to the *Entscheidungsproblem*" (Turing, 1937). In this paper, he proposed a hypothetical decision-making machine, fed with a series of simple yes-no questions from a paper tape input. The philosophical issue was whether there was any mathematical problem which could not be programmed in this way (Turing used the phrase "calculable by finite means"). Turing concluded that in fact there were such problems, albeit not many, and his hypothetical machine is now commonly seen as the idealised binary digital computer, or **"Universal Turing Machine"**. The Turing Archive for the History of Computing contains digital facsimiles of many of Turing's wartime papers, now declassified.

Turing reported for duty on 4th September 1939 (Hodges, 1992), and was joined shortly afterwards by another Cambridge mathematician, John Jeffries, already an expert on ciphers. The most logical way to fulfil Denniston's masterplan was therefore to give Jeffries the job of attacking the logic of the cipher, while Turing drew up plans for the computing machine to deal with it on a day-to-day basis once it had been broken. Jeffries' work exposed him immediately to the *Lasy Kabackie* papers, amongst which were some pen-and-paper cryptanalytic techniques devised by Zygalski, and known therefore as **"Zygalski Sheets"**. These were rotor analysis matrices which when appropriately punched and stacked (for details, see Savard, 2002) would reveal likely *Walzenläge*. One large matrix was needed for every letter of the alphabet for every *Walzenlage* permutation. For the old three-from-three Enigmas, this meant 26 sheets for each of the six possible *Walzenläge*, and for the new three-from-five Enigmas, it meant ten times as many [see previous inset]. Welchman (1982) gives fuller details of the "perforated sheet" approach to cryptanalysis, if interested.

By December 1939, the new "Jeffries Sheets" were ready (60 sets, one for each possible *Walzenlage* again, and each set containing 26 matrices), and by one account Turing delivered them in person to Rozecki, Zygalski and Rejewski, now codenamed "Equipe Z" (= "Team Z"), at Vignolles, where - after just over a year in the dark - they enabled the first successful decryption of a three-from-five Enigma on 17th January 1940.

The Allies were now free to resurrect the principles of the Polish *bomby*, namely to work through the *Walzenläge* from the first to the 60th, searching for a fragment of pre-set **"cribtext"** .....

> **Key Concept - The "Crib":** Cryptologically speaking, a "crib" is a short fragment of known or strongly suspected ciphertext content. Many cribs derived from the repetitive nature of military communication. For example, many units reported NICHTSZUMELDEN (= "nothing to report") on a daily basis, or their radio operators would send a pro forma tuning message before anything else (Taunt, 1993). The other main sources of cribs were (a) weather reports, (b) proper names, (c) plain old-fashioned operator bad practice, and (d)

deliberately creating an operational event and then checking to see how it was reported the next day (a process known as **"seeding"**).

The Enigma cribs were given added importance by one of the system's basic design features, namely that no letter was allowed to encrypt as itself. This meant that if you aligned a slip of cribtext above a line of ciphertext, **no vertical pair of characters could be the same**. If they were, then the crib could not exist at that position. Milner-Barry (Hut 6) summarises the argument this way:

> "If, for example, you were looking for the most likely position [for the word] *Besonderen* [= "special"], and you noticed that under the [cribtext] B in *Besonderen* was another B, you would know for a certainty that that could not be the right position." (Milner-Barry, 1993, p94.)

It followed that if a crib could be logically excluded in all text positions, then either (a) the crib was wrong, or (b) the crib was right, **and that particular machine setting could be excluded**; and on most days, on routine intercepts, you had very high levels of confidence in the crib. Taking this argument a step further, if you could carry out this process of elimination at speed and exclude all machine settings except one, then that would be the one to use to decipher that day's intercepts.

1.3 Computerised Cryptanalysis (1940-1941 - The Bombes)

> **Key Locations - BTM:** In this section, we meet "BTM", the British Tabulating Machine Company premises at Letchworth, Hertfordshire. BTM was formed in 1908, as a London-based licensee of Hollerith punched card technology (see Part 1). The company was renamed International Computers and Tabulators in 1959, acquired Ferranti's computing division in 1963, and merged with English Electric to form **International Computers Ltd (ICL)** in 1968. ICL was the British computing industry in the 1970s and 1980s, but was taken over by Fujitsu Corporation in 1990. The marque was finally withdrawn (for marketing image purposes) in 2001.

The bombes were put together by BTM at their Letchworth factory, and Welchman (1982) dates the experimental systems to September 1940 (the first was nicknamed "Agnes"). However, Welchman also estimates that it took another year or so before they started to take the pressure off the pen-and-paper techniques. Indeed, Welchman repeatedly stressed that the bombes themselves did not break codes, but that people did. The processing logic meant that the more machines you had, the shorter could be the *Walzenlage* tape for each, and the quicker you could get your results. About six bombes were operational by mid-1941, and perhaps twelve by late summer (Welchman, 1982). Production then proceeded at about one machine per week, the machines being transported from the BTM factory without escort to avoid attracting anybody's attention. Different machines serviced different huts, and different regional or administrative networks within huts. Worthwhile intelligence started to appear in the July 1940 defence of Norway (Thomas, 1993), and there were also successes in the evacuation of the Aegean in early 1941, and in the war against the Afrika Korps' supply convoys later that same year.

1.4 Computerised Cryptanalysis (1941-1942 - The Naval Enigmas)

With the German army and air force codes under some semblance of control, attention turned to the Kriegsmarine system. This had been a much tighter system since the introduction of more vigorous procedural protection for the message header on 1st May 1937, but it was nevertheless strategically vital for it to be defeated, because it was the key to countering the German U-boat offensive. This is how Irving John ("Jack") Good, who joined the team in May 1941, summarised the complex Kriegsmarine operating procedure [we recommend sketching out his worked example as you go]:

> "The German operator would haphazardly choose the settings for the three wheels as shown by the rings, say ASC, but he would not send ASC in clear. Instead, he would first set the wheels at [the key of the day] *Grundstellung* [and] tap out ASCASC. [This] would give him a hexagraph, say LQRCPY. He would write this in the pattern [L over space, Q over C, R over P, and space over Y] and fill in the [resulting four-by-two] rectangle with two letters that he chose haphazardly. For example [O bottom left and T top right]. Next he

> would encrypt the vertical digraphs LO, QC, RP, and TY by using a secret 'digraph table'. There were ten possible digraph tables (fixed for an appreciable time, perhaps of the order of a year), and which of the ten he was to use would be shown by part of the keys of the day. For example, LO might become TU, QC might become AH, RP might become LS, and TY might become IU. Then his rectangle would become [TALI over UHSU]. Then at last he would transmit TALI UHSU. The legitimate receiver would use the same procedure in reverse order to recover the true initial wheel-settings for the message, and he would get a check because of the repetition [.....] I noticed on one night shift that about twenty messages were enough to identify which digraph table was in use." (Good, 1993, pp155-156.)

Fortunately, May 1941 turned out to be a doubly lucky month for British codebreaking. Firstly, a copy of the June 1941 codebook was recovered from a captured German trawler, and secondly one of the machines itself was recovered from a captured U-Boat (U-110). This gave sufficient specific background information for the naval Enigma to be effectively broken for the remainder of that year. Then came more ominous news. Thomas (Hut 3N) tells how in August 1941 he inspected the inside of captured U-570 (Thomas, 1993). No code books or machines were recovered on this occasion, for the crew had ditched these over the side, but what they had not ditched was the transportation box for a machine still under test, which, Thomas noted, was recessed to accommodate a four-slot machine, rather than three. It subsequently transpired that the Kriegsmarine was about to upgrade to a four-from-eight Enigma system, and when this eventually went live in February 1942 it brought blackout for the rest of that year, (a) because there were new rotors whose internal wiring needed to be broken, and (b) because the cryptanalysts now had many more permutations to wade through at run time.

> **ASIDE:** The 1942 naval Enigma machines were not just fitted with four rotors rather than three, but some of the rotors had more than one turnover notch, so they would "carry" to the adjacent rotor more often. As previously explained, there are 60 *Walzenlage* permutations on a three-from-five Enigma. If we do the same calculation with a four-from-eight naval Enigma we find there are 70 ways of selecting four rotors, and then another ten ways of sequencing the rotors-of-the-day across the available slots, making 700 permutations in all. (In fact, it was not quite as bad as this, because German operating procedures insisted that at least one of rotors VI to VIII was included.)

The four-from-eight naval system therefore demanded either more bombes or a more sophisticated computational solution, and, according to the Bletchley Park Museum, eventually around 200 machines were in operation 24-hours a day at sites across Britain. Bombe 2 was developed in early 1943 to substitute valve technology for some of the electromechanical. The first two American bombes entered acceptance trials in May 1943, and orders were placed for a US production run of 96 machines in June 1943 (Wenger, Engstrom and Meader, 1944; top secret report, now declassified). The role of NCR's Electrical Research Laboratory at Dayton, OH, in producing the US machines is currently being researched by Anderson (2000). The bombes worked well as far as they went, but were generally underpowered and slow. To set up and play with your own bombe, click here [**HIGHLY RECOMMENDED LEARNING EXPERIENCE**].

1.5 Computerised Cryptanalysis (1942-1943 - Breaking the Lorenz SZ42)

> **Key Location - TRE:** The next part of the story of British World War Two code breaking introduces another important location - **"TRE"**, the Telecommunications Research Establishment, Malvern, Worcestershire. This began life as an Air Ministry project to develop top secret radar equipment. Funding was authorised in 1934, and a small team was brought together in 1935 under Robert (Later Sir Robert) Watson Watt (1892-1973) at Orfordness, Suffolk. More permanent premises were acquired in 1936 at nearby Bawdsey Manor, and the official name Bawdsey Research Station was allocated. This name then had to change when the entire establishment relocated to Dundee in 1939, and the title Air Ministry Research Establishment (AMRE) was selected. There was then a further relocation to Worth Matravers, Dorset, in May 1940. The official TRE name was given in November 1940, and the move to Malvern took place in May 1942.
>
> **Key Personnel:** In this section, we also meet **Maxwell Herman Alexander ("Max") Newman** (1897-1984), a senior Cambridge mathematics professor before the war, who had lectured Turing as a student (in fact, it was he who had inspired the latter's *Entscheidungsproblem* paper and established the academic links with Princeton

> which had brought Turing into contact with von Neumann). We also meet again the Welsh physicist **Charles E. Wynn-Williams** (1903-1979), whose pre-war track record building electronic counting circuits was about to prove invaluable (remember that he beat Stibitz to the binary accumulator by six years - see Part 2). Wynn-Williams joined AMRE/TRE from Cambridge University at the beginning of the war.

Important though they were, the Enigmas were only tactical systems. Their job was to link Hitler's generals to their armies, his air marshals to their airbases, and his admirals to their U-boats and surface units. The various networks carried routine low-level orders in bulk, that is to say, the sort of traffic required to move and coordinate Hitler's war machine in much the same way that our motor nerves move and coordinate the individual muscles of our bodies. Yet another encryption system serviced strategic communication between the High Command and the far corners of the German military and diplomatic world; and, needless to say, one high level message could easily tell you as much as a few thousand day-to-day ones. The Germans therefore protected their strategic communications traffic with higher specification cipher machines - the Lorenz ***Schlüsselzusatz* SZ40/42** and the Siemens and Halske **T52 *Geheimschreiber***.

The SZ42 was a Vernam-style bit-flipping teletypewriter, as previously described. Using the commercially widespread system of five-hole tape [see under *Morkrum* and *Morkrum-Kleinschmidt* in Part 1], it carried out a key-controlled modulo 2 encryption of every bit in every character in the plaintext. It then produced a pre-perforated ciphertext tape for transmission, and the transmission itself was done at machine speed in ITA2, rather than at human speed in Morse Code. After each character, the encryption key was varied according to an advancing rotor system, not unlike the Enigma, only there were now twelve rotors, and they had many more pins. The Germans named this system Lorenz, after the Lorenz Teletypewriter Company which manufactured it, whilst the British named the equipment "Tunny" and its transmissions "Fish". The first Fish intercepts started to come through in the summer 1940. The British codenamed the *Geheimschreiber* "Sturgeon", after it was discovered being used for high level Luftwaffe communications from late 1941 (Hinsley, 1993). A full GCCS report, the "General Report on the Tunny" is available in digital facsimile, if interested. Unlike the various Enigma systems, the Lorenz systems could encipher letters as themselves.

The basic principles of the Lorenz code were initially unravelled by Colonel John Tiltman, head of the Military Section, and subsequently fleshed out by William T. ("Bill") Tutte (1917-2002), who had joined GCCS fresh from university in January 1941.

> **ASIDE:** It subsequently emerged that the Siemens and Halske system had already been cracked by the Swedish cryptographer Arne Beurling in June 1940 (Beckman, 1996). The German diplomatic telegraph cable passed through Swedish waters, and had been duly tapped by Swedish Telecom. All *Geheimschreiber* traffic from the day the system was first tested on 18th April 1940 was intercepted, and closely studied by Beurling. He broke the code later than summer, using pen and paper cryptanalysis and sheer force of logic. It took him a fortnight, although he too was helped by some sloppy operator discipline. Professional to the last, Beurling died leaving no published explanation of how he broke the *Geheimschreiber*: "A magician," he insisted, "does not reveal his secrets".

Tutte was given a good start by an unsafe transmission on 30th August 1941 from a German operator in Athens. This was a long dispatch in fish, which failed to decipher cleanly at its destination in Vienna. The receiving operator duly requested retransmission, and the Athens operator unwisely used the same machine settings for a close, but not exact, copy of the ciphertext.

> **ASIDE:** It is difficult to get a straight story from the literature here. Retransmission of a pre-perforated teleprinter tape would not, of itself, normally require a re-encryption, and would simply produce an identical copy. Nevertheless, the online Tunny Report (above) clearly states (p298) that the retransmission had been rekeyed to tape, complete with minor mispellings.

By painstakingly analysing those ciphertexts over a period of several months, Tutte and his colleagues eventually correctly deduced that the Lorenz machine had to consist of 12 different sized rotors, of size 23, 26, 29, 31, 37, 41, 43, 47, 51, 53, 59, and 61 (Good, 1993).

> **ASIDE:** The *Geheimschreiber*, by contrast, had ten such wheels, sized 73, 71, 69, 67, 65, 64, 61, 59, 53, and 47. Full details in Beckman (2003).

Aside from the rotor sizes, it was also necessary to learn the logic of their gearing. To start with there were five K (or chi) rotors (the 23, 26, 29, 31, and 41 pin ones), then there were five S (or psi) rotors (the 43, 47, 51, 53, and 59 pin ones), and finally there were two M (or mu, or motor) rotors (the 37 and 61 pin ones). This is how they worked together .....

> "The first set of coding wheels, K1-K5, and the first motor wheel, stepped every time. The second motor wheel stepped whenever the first motor wheel pattern enabled it to do so. The second set of coding wheels, S1-S5, stepped whenever the second motor wheel enabled it to do so." (Halton, 1993, p172.)

Halton continues .....

> "Whether or not a coding wheel reversed the sense of the digit passing through it depended on the setting of a tooth on its circumference, the tooth being either erect or folded down. The wheels all had different numbers of teeth, which were set up to the pattern specified for the day [Ed. in much the same way that we nowadays set the timer pins of central heating or pre-programmed lighting systems], and all could be rotated individually to any required position for the start of a message. The first set of wheels advanced one tooth for every character. Two more wheels of a similar type controlled the stepping of the second set of coding wheels and were called (at BP) the motor wheels. The first motor wheel advanced by one tooth for every character, but the second did so only when permitted to do so by the teeth of the first. The second set of coding wheels stepped only when permitted to do so by the teeth of the second motor wheel. Like the character-coding wheels, the motor wheels could be set to any specified tooth pattern and could be made to start from any position." (Halton, 1993, p169-170.)

Gil Hayward (1993), one of the Tunny engineers, adds:

> "Each rotor [in the first group of five] was advanced by one tooth for each character transmitted []. The enciphering was achieved by [exclusive-OR addition.] We knew this process as 'non-carry binary addition' [] The second set of rotors was driven indirectly via the [two M-rotors] and now processed the [five code] elements once more, performing an exclusive-OR of the output of the first set with their own tooth states. The SZ sent the final element outputs to line in serial form in real time." (Hayward, 1993, p178.)

Tutte's decryption has been described as arguably "the greatest intellectual feat of the whole war" (Sale, 1997), because once the technical "go" of the new machine had been established, it again became possible to resort to largely automated trial-and-error. The main task was to find the settings of the five K-rotors (Good, 1993), and the algorithm which did this was called the "double-delta" method. However, the number of permutations to get through was far higher than in the Enigma machines, so the first thing Max Newman did when he joined GCCS as head of the Tunny team in September 1942, was to determine that a quantum leap in computing power was required. He therefore drew up the detailed specification for a machine capable of automating Tutte's double-delta method, and his team relocated to a larger building, nicknamed "the Newmanry", to do the design work. They were joined by **Donald Michie** [Wikipedia biography], straight out of school, but later professor of artificial intelligence at the University of Edinburgh.

This time it was Wynn-Williams and his high-tech TRE team who put the hardware together, and the resulting computer, codenamed the **Heath Robinson**, was operational around April 1943. Here is Michie's own summary of its working principles:

> "The [Heath Robinson] machine incorporated two synchronised photo-electric paper tape readers, capable of reading 2000 char/sec. Two loops of 5-hole tape, typically more than 1000 characters in length would be mounted on these readers. Counts were made of any desired Boolean function of the two inputs. Fast counting was performed electronically, and slow operations [] by relays. The machine, and all its successors, were entirely automatic in operation, once started, and incorporated an on-line output teleprinter." (Michie, cited in Randell, 1976, p9.)

Good (1993, p162) adds:

> "The input to Heath Robinson was a pair of teleprinter tapes, one containing cipher and the other one some function of the chi wheels. The tapes would be stuck into closed loops and driven partly by pulleys and partly by their sprocket holes. Both tapes would be read photoelectrically and the innards of the machine would count the number of times that some Boolean function was equal to a dot. The cipher tape would have a length prime to that of the key tape, so that in the course of a 'run' all possibilities were examined. The machine had perhaps about two dozen vacuum or gas-filled valves or tubes. [] The main weakness of the design was the driving of the tapes partly by their sprocket holes at about a hundred times the speed of the tapes in normal teletypewriter usage. This would cause these holes to stretch and the tape to have a tendency to tear [.....] Also, from time to time, the machine would begin to smoke."

1.6 Computerised Cryptanalysis (1943-1945 - The Colossus)

> **Key Locations - "Dollis Hill":** The third part of the story of British World War Two code breaking involves workers at another important location - "Dollis Hill", the Post Office Research Station, at Dollis Hill, North London. These telecommunications workshops were opened in 1921, at a time when the Post Office was responsible for Britain's telegraphy and telephony as well as for its postal services, and so it attracted some of the country's best electrical engineers. It was Britain's Bell Labs, if you like (but on our usual amateurish scale). The location sounds humble enough, but it concealed a very special secret, for in 1938 the buildings had been extended downwards to provide an emergency seat of government should the Cabinet Room at Whitehall be put out of commission for any reason.
>
> **Key Personnel:** In this section, we meet (the seriously under-acclaimed) **Thomas Harold ("Tommy") Flowers** (1905-1998) [Wikipedia biography], a telecommunications engineer at Dollis Hill. Flowers was an experienced electronics designer, and had been experimenting with valve technology in telephone switching gear since 1931.

The Robinsons were transitional machines; faster than the bombes, but still largely relay-based, experimental, and with the reliability problems mentioned above. The decision was accordingly taken to build a machine which would be faster still and have greater processing power, and in order to achieve these higher speeds, valves were going to have to replace relays wherever possible. Britain's expert on valves at that time were Dollis Hill's Tommy Flowers and TREs's Charles Wynn-Williams. Flowers had already been involved with miscellaneous GCCS projects since February 1941, during which time he had met with Wynn-Williams and Turing. He had been given the specifications for various pieces of equipment, and had carried out the necessary engineering back at Dollis Hill, assisted by a colleague, Sidney W. Broadhurst. His team had also worked in 1942 with H.M. Keen at BTM on upgrading the bombes, and with TRE on upgrading the Robinsons. He would now do the same again, but working this time on what would become GCCS's - and Britain's - flagship wartime computing project, the Colossus.

The detailed design for Colossus was teased out in the winter of 1942/3 by Newman and Flowers, with major contributions from Good and half a dozen others. The Dollis Hill group, now with additional assistance from W.W. Chandler, then spent the first eleven months of 1943 putting the machine together and testing it, and it began productive work in December 1943. The Colossus consisted of 1500 valves, weighed about a ton, and could make do with only a single input paper tape, from which data could be read at the rate of 5000 characters per second. To reduce tape handling failures, the cipher tape was read once, and its contents written to memory (this was the essence of the advance over the Heath Robinson, and accounts for the much higher number of valves used). Thyratron valves were included as memory units.

The British now had significant access to German communications at the highest level, and the team's early successes included forestalling the German counter-attack against the Anzio bridgehead in February 1944, and breaking into the network centred on von Rundstedt's headquarters in France in March 1944. As a result, Dollis Hill received an order for a number of more powerful follow-up machines, the Colossus 2s, and Michie contributed major improvements to the upgraded design (Andresen, 2001). The Colossus 2s had 2400 valves and could process several input streams in parallel, giving them an effective input speed of 25,000 characters per second. More importantly, at least one of the new machines was needed to be up and running by 1st June 1944 to handle the increased volume of traffic expected after the Normandy invasion (Randell, 1977). Fortunately, Flowers' team had been strengthened by the arrival of A.W.M. Coombs and Wilfred Saville, and they met the deadline with literally just a couple of hours to spare. By the end of the war, 63 million keystrokes of German code had been deciphered (Andresen, 2001), and in the best traditions of "real programming", not one of the people Randell (1977) interviewed had any recollection of anybody ever producing any system maintenance manuals.

Here is an analysis of the COLOSSUS's strengths and weaknesses, measured against the criteria of modernity discussed so far .....

Electronic rather than Electromechanical	**Digital rather than Analog**	**Binary rather than Decimal**	**General Purpose Stored Program**
Yes	Yes	Yes	General purpose in principle, but in practice all the input-output peripherals were tuned for code-breaking applications, so considerable reconfiguration would have been necessary. Externally programmable due to shortage of memory.

ASIDE: A moment's pause before moving away from the codebreaking applications. It is nowadays altogether too easy to be carried away with the technicalities of cryptology, and we should not forget that lives were at stake every minute of every day. When you broke a code, these tended to be your enemy's lives, and when you did not, they were your own. Either way, the casualties were real people, not numbers. Dakin (1993) recalls being emotionally moved later in the war by the number of German sailors receiving messages telling them that their homes had been AUSGEBOMBT, and Eyton (1993) reports being unable - then - to make sense of a curious phrase from an Aegean maritime intercept later in the war, when a cargo of Jews was reported as being en route for the ENDLÖSUNG (= "final solution"); the code, on this occasion, was stronger than the cipher! On the lighter side, Jack Good, it is reported, went out of his way to acquire an "007" car registration plate once the James Bond stories hit the headlines in the early 1960s, and drove it, no doubt, with a cryptic smile.

2 - The Harvards Mark 1 to 4

The Harvard Mark 1 was a joint venture between IBM and Harvard University, under the general direction of Professor Howard Hathaway Aiken (1900-1973). Eager to develop a giant digital calculator to rival MIT's big analog machines (see Part 2), Aiken had approached the Monroe Calculating Machine Company for development funding in 1936. They had turned him down, but had passed him on to IBM's Thomas J. Watson, who agreed more or less on entrepreneurial instinct to underwrite the project. Construction began in 1937, and went on for six years. The end result was that by January 1943 Aiken's team had put together a machine known as the Automatic Sequence-Controlled Calculator (ASCC), or "Harvard Mark 1".

The Harvard Mark 1 was the largest (55 feet long, 8 feet high, and containing over three quarters of a million parts) electromechanical calculator ever built. It was sited at the IBM installation at Endicott, NY, and (like Colossus) was something of a "transitional" species, retaining moving parts characteristic of the old da Vinci machines, but incorporating Babbage-style modularity and programming (not surprising, since Aiken had

explicitly based his first-cut design on Babbage's four main modules - see Part 1). It received its processing instructions on previously perforated paper tape, and data input/output on punched cards. It was fitted with 72 23-decimal-place registers (one of the 24 decimal wheels making up each register was reserved for use as a sign digit), each cannibalised from IBM's pre-war range of electromechanical calculators, and was thus capable of doing very big sums to very high levels of accuracy. These registers were "accumulators" - they would store whatever number was put into them until next required, and then allow it to be added to. A further 60 registers were "read only", and were manually set to program constants prior to the run commencing. Each tape-punched instruction served to identify the next operation to be carried out, together with the location of the registers containing the operands for that operation and the destination of the answer. The main drive shaft rotated at 200 rpm, meaning that the machine could work at the rate of just over three "elementary operations" (such as simple additions) per second.

The system remained under trial and improvement until mid-1944, whereupon it was shipped lock, stock, and barrel to the Harvard Computation Laboratory. It was then immediately leased by the US Navy's Bureau of Ships - no less than three admirals being present at the official inauguration on 7th August 1944 (Williams, 1999) - and put to work in aid of the war effort, with armed guards patrolling the campus. It continued in service until 1959. An improved version of basically the same design was laid down in 1942, for installation at the US Naval Proving Ground, Dahlgren, VA. This was the Harvard Mark 2, or the "Dahlgren Calculator" (Freeland, 1947). The basic technology was unchanged, but enough improvements were incorporated to push performance up to around 30 simple additions per second (that is to say, it was about ten times as fast as the Mark 1, but a lot noisier). It contained 13,000 high specification multiple-contact relays (at $15 apiece), and could do floating point arithmetic. It was also built for greater ease of maintenance - many key components were modular and could be exchanged with minimal fuss in the event of failure (Freeland, 1947). A third machine in the series was completed in 1949, and incorporated magnetic drum storage and a stored program, and thus marked a major modernisation. The technical platform was mixed valve and relay (5000 and 2000 respectively). A fourth machine, the Harvard Mark 4, went live in 1952, and was even more modern, but by then Harvard had lost its IBM backing, and the running was being made elsewhere. The Mark 4 was nevertheless one of the first deployments of a newer form of computer memory device, "the ferrite toroid single-bit flip-flop" (more on which shortly, in the section on *The Whirlwind Project*).

Here is an analysis of the first two Harvard machines' strengths and weaknesses, measured against the criteria of modernity discussed so far .....

Electronic rather than Electromechanical	**Digital rather than Analog**	**Binary rather than Decimal**	**General Purpose Stored Program**
No - electromechanical	Yes	No - decimal (a hangover from the days of the desk calculator, **and a major design weakness**)	General purpose, within the limitations of its rudimentary instruction set, but not stored program.

3 - The Bell Telephone Laboratories Machines

Bell Labs began their involvement with computers following Stibitz's experiments with binary adding circuitry in 1937 (see Part 2), and although they started after Aiken their machines were much smaller and thus a lot quicker into service. Samuel B. Williams led their Model 1 Relay Calculator project (aka the "Complex Number Computer"), and had the product ready for action in January 1940. It was publicly demonstrated in September 1940, being operated over a teletypewriter link. It was not programmable,

however, and this defect was remedied as an adjunct to Bell's work on flak systems in the Model 2 Relay Calculator (or "Relay Interpolator"), a tape-controlled device with self-checking arithmetic. This became operational in September 1943 at the US National Defence Research Council, where it was initially used to produce lifelike test data for Bell's AA Predictor No. 9. The machine contained 500 relays, and remained in use until 1961. Cesareo (1946) details its biquinary adding circuits, if interested. The Model 3 Relay Calculator (or "Ballistic Computer") was started in 1942, completed in June 1944, contained 1300 relays, and remained in use until 1958. It was purpose-designed to speed the analysis of test firing data. Juley (1947) describes it as another teletypewriter tape machine, and identifies four separate input tapes, one containing coded data from cine film of the target position, the second containing the gun control parameters under test, the third containing reference data, and the fourth (which was read as a continuous loop), containing the master control instructions, or program. Biquinary notation was used as before. The Model 4 Relay Calculator was basically similar to the Model 3. The Model 5 Relay Calculator (or "General Purpose Relay Calculator") was, as its name suggests, a truly general purpose computer, complete with conditional logic branching. The Model 5 was a two-off project, one machine being produced for the National Advisory Committee on Aeronautics, Langley Field, VA, and the other for the US Ballistic Research Lab, Aberdeen, MD (henceforth "BRL"). The machine was started in 1944, completed in 1946 (Langley Field) and 1947 (BRL), contained 9000 relays, and weighed about ten tons. It was relatively slow, but generally reliable and required minimal changeover time in that the use of tapes allowed runs to be prepared offline.

The limiting factor in all these machines was still the technology. Circuits were hand-built and hand-soldered out of individual capacitors, valves, and resistors, mounted on a metal chassis. The machines worked, but only after a fashion - they were big, heavy, got very hot, and kept breaking down as fuses blew, switches failed, and valves burned out. The next breakthrough came in 1947, when John Bardeen, Walter H. Brattain, and William Shockley - more Bell Labs researchers - brought together a number of earlier discoveries and invented the **"transistor"**, a development for which they were awarded the 1956 Nobel Prize for Physics .....

> **Critical Invention - The Transistor (1947):** A transistor is a "cold-running" electronic switch. In its original form it consisted of a "semiconducting" - that is to say, unidirectional - crystal of germanium, onto which was placed a metal contact. This "point contact" device made use of fundamental properties of this type of interface, namely that electrons are drawn away from the contact more easily in the conducting medium than in the non-conducting crystal. Such units could therefore be installed in electronic circuits in place of valve diodes, where they would rectify AC the same way, but with no need either (a) for a heating current, or (b) for a glass capsule. **They therefore allowed the work of the thermionic valve to be done at fractional cost, size, and power.** A different layout followed shortly, in which two point contacts were applied to one face of the crystal, and a flat contact on the opposite face. This served in place of valve triodes, allowing one part of a circuit to switch the current flowing in another part.

4 - The Moore School's ENIAC and EDVAC

> "There are 10 types of people in the world - those who understand binary, and those who do not" (Anonymous Internet wag, October 2002.)

As with the British codebreaking machines, the major historical step away from electromechanical architectures in the US came in 1943. This was when the Moore School of Electrical Engineering at the University of Pennsylvania built the Electronic Numerical Integrator and Calculator (or ENIAC). Somewhat ironically, the project only came about because the Moore School had acquired one of Bush's analog differential analysers, and this brought them to the attention of the technical staff at BRL, who had more sums to do than their own differential analyser would cope with. Lieutenant Paul N. Gillon, the officer in charge of computation at BRL, therefore requisitioned time on the Moore School machine, and Lieutenant Herman H. Goldstine was assigned to the Moore School as liaison officer and project coordinator. This gave

Goldstine access to two differential analysers, one at BRL, and a bigger one at Moore (Moye, 1996), but still the backlog of ballistics computation work was piling up.

Enter John William Mauchly (1907-1980), a Cincinnati physicist, and John Presper Eckert (1919-1995), a Philadelphia electrical engineer. Mauchly and Eckert were Moore School lecturers, and it so happened that the quirky performance of the analog systems had been irritating the both of them as well. Indeed, Goldstine's arrival coincided with a paper Mauchly had written in August 1942, proposing a digital electronic computer. Goldstine knew a bit about mathematics himself, and was so impressed with Mauchly's ideas that he immediately sought the necessary funding from the ordnance department budget. Moore School professor John Grist Brainerd (1904-1988) presented the business case to BRL's commanding officer, Colonel Leslie E. Simon, and his senior scientific advisors, and was not beyond using a little non-military camouflage to help his case, deliberately describing the proposed hardware as an "electronic diff. analyser", and so confusing digital *differencing* with analog *differentiation* (Winegrad, 1996).

Brainerd was successful, and the contract for ENIAC was duly signed in June 1943. The project proceeded under the codename "Project PX". Brainerd was appointed project manager, Eckert chief engineer, and Mauchly principal consultant (Moye, 1996). Others involved were Arthur W. Burks, Thomas K. Sharpless, and Robert F. Shaw. Eckert's initial role was to increase the average life expectancy of the electronic valves which were going to be required, because the fact that large numbers of them were going to be used meant that the final system was otherwise at risk of being permanently out of service.

> **ASIDE:** The problem of valve burn-out, it will be recalled, had been Zuse's worry back in 1938, when he elected to keep the Z3 project electromechanical - see Part 2. However Tommy Flowers' advice on the Colossus development had been that the majority of valve failures took place when they were warming up, and that systems which could be switched on and left on were much less vulnerable. That and high specification manufacturing brought performance up to acceptable standards.

Eckert was also responsible, he later recalled, for testing whether the Pennsylvania mice liked the taste of the electrical insulation on his cable stock. The types they refused to chew when half-starved were the ones which got used, on the grounds that the mice would be less inclined to build their nests inside the completed machine later on. Construction began in June 1944, final assembly took place in autumn 1945, the machine went live in February 1946, and was delivered to BRL in January 1947 (Moye, 1996). It weighed in at 30 tons, contained 18,000 thermionic valves, and its computing power was used, yet again, to prepare military ballistics tables. It also assisted the nuclear weapons programme (although it took time off in 1949 to compute π to a record 2035 places of decimals). Input was on IBM 80-column cards, and, since this was commonly available technology, it allowed the necessary data to be shipped in and out as trays of Hollerith cards (on one occasion, around half a million of them, direct from the nuclear physicists at Los Alamos). Each memory unit had its own external neon light, so that the electronic state of the processor could be visually assessed by the operator, and the machine could be run in single-instruction mode so that progression through a program could be step-by-step monitored if needed. Modular construction allowed critical circuit components to be replaced in minutes, thus helping to achieve a mean time between failures of 5.6 hours (Muuss, 1992/2002).

Thanks to its electronics, the ENIAC was nearly 2000 times as fast as the ASCC, leading Eckert, rather disparagingly, to dismiss the rival Harvard machines as just "fancy tabulators". Around 5000 simple additions were possible per second (compared to the Mark 1's three). Moye (1996) explains that ENIAC could do in 30 seconds what took the Bush differential analyser 15 minutes (far less accurately) and a skilled mathematician 20 hours; one commentator even pointed out that it was faster than the projectiles it was tracking. The system was decommissioned in 1955.

Here is an analysis of the ENIAC's strengths and weaknesses, measured against the criteria of modernity discussed so far .....

Electronic rather than Electromechanical	Digital rather than Analog	Binary rather than Decimal	General Purpose Stored Program
Yes	Yes	No - decimal, 10 places of.	General purpose, but not stored program.

The ENIAC profile table still contains two significant NO entries - it computed in decimal rather than in binary, and it had no memory to spare for program storage. In the world of computer design, these are both signs of considerable immaturity, but the decimal issue represented by far the greater practical barrier, for it is an example of how "functional fixedness" can impede technological innovation. As with the Harvard Mark 1, the ENIAC's designers thought in decimal, and so presumed that their creation should do likewise. "Proper" computers, on the other hand, were already computing in binary rather than decimal. Wynn-Williams had seen this, Zuse and Stibitz had seen this, and so too had Atanasoff, but the Harvard and Moore School teams had simply built decimal logic circuits out of binary basics, and, for technical reasons beyond the scope of this paper, that was actually a circuit designer's nightmare.

> **ASIDE:** Upon learning after the war that the Americans had used 18,000 valves in their ENIAC, Zuse is reputed to have shaken his head and asked what on earth they had all been for. He and Schreyer had studied valve-based logic circuits in 1936 (see Part 2), and knew that a binary system of ENIAC's overall capability should need less than 3000 valves, that is to say, ENIAC was an order of magnitude larger than it strictly needed to be. This is a measure of the inherent inefficiency of trying to do decimal computation with essentially binary hardware.

In March 1946, a dispute broke out between Eckert and Mauchly on the one hand, and the University of Pennsylvania on the other, as to who should own the rights to the ENIAC patents. As a result, Eckert and Mauchly resigned from the Moore School and formed the **Electronic Control Company**, to be renamed the **Eckert-Mauchly Computer Corporation** in December 1947. Neither the Moore School, nor Eckert and Mauchly, fully recovered from this split.

The decimal-binary issue was not fully resolved until 1946, when the Hungarian-American John von Neumann (1903-1957) joined the Moore School team, just as they began work on the Electronic Discrete Variable Automatic Computer, or EDVAC, the ENIAC's replacement. Von Neumann had visited the ENIAC development in August 1944, as part of his fact-finding duties as academic advisor to a number of US government agencies, and had followed this up with a paper extolling the virtues of all things binary in 1945 (von Neumann, 1945/1982).

Now the beauty of binary is that it simultaneously eases data transmission and manipulation. In binary computing machines, information is stored in "binary digits" (or **"bits"** for short) [the term "bit" was introduced in the early 1950s by the Institute of Advanced Studies' John Tukey (see next section but one)]. Conceptually, a bit is either a nought or a one, but physically it can be any convenient local state within the underlying hardware, typically a voltage being high or low, a switch being open or shut, an area of magnetic medium being magnetised (that is to say, "written to") or not magnetised ("not written to"), a hole punched or not punched into a Hollerith card or length of teletypewriter tape, or whatever. Such changes of state got referred to as "flip-flopping", and any mechanism which could be used to do it got called a **"flip-flop"**. As a computer designer, therefore, you could store as many bits of information as you could build flip-flops.

The time was now right to share a few of the secrets, and the Moore School therefore took the very farsighted step of ensuring that everyone in the rapidly burgeoning industry would all be singing from the same hymn book. Between 8th July and 31st August 1946, they ran a 48-lecture course entitled "Theory and Techniques for Design of Electronic Digital Computers". There were 28 officially named attendees, including Maurice Vincent Wilkes (Cambridge), and Bletchley Park's Irving J. ("Jack") Good and D. Rees (both by then at the University of Manchester), and they were taught by experts drawn from the Harvard and Moore School teams.

EDVAC's sponsor was the BRL at Aberdeen, but without Mauchly and Eckert it was a slow and troubled development. The machine was eventually assembled in August 1949, but continued to suffer significant teething troubles until October 1951. It sported 5000 valves, and was fitted with 128 mercury delay lines [see next section], each capable of holding eight 44-bit words. Eckert explained the project problems this way: "Other people tried to build the machine that I didn't build, and they managed to foul it up and it never got really built decently" (Smithsonian Institute, online). Nevertheless, it achieved an impressive mean time between failures of around 8 hours (Muuss, 1992/2002). Here is an analysis of the EDVAC's strengths and weaknesses, measured against the criteria of modernity discussed so far .....

Electronic rather than Electromechanical	**Digital rather than Analog**	**Binary rather than Decimal**	**General Purpose Stored Program**
Yes	Yes	Yes	Yes

Note that we now have a run of four straight yesses across the EDVAC's key points profile, as a result of which many commentators rate it as the class-defining modern computer - the first working "Eckert-von Neumann machine" (see next section but two). The EDVAC should also get the credit for including the first workable **"Operating System"** (see Part 4), and for solving the problem of program "branching", known officially as "conditional control" .....

> **Key Development - Conditional Control:** This is a facility whereby one machine instruction moves not to the immediate next but to the beginning of a logically related series of instructions further down or further up the program. This gives the programmer the ability to apply a degree of modularity to the totality of his logic. It is a vital part of effective programming, and will be further discussed in Part 5 and Part 6.

5 - The National Physical Laboratory Projects

> **Background:** Britain's National Physical Laboratory (NPL) was founded in 1902, and from its workshops at Teddington, Middlesex, was involved in the calibration and testing of scientific and civil engineering projects for a century. During the war, it took part in many top secret research and development projects, including Barnes Wallis's bouncing bomb, aerodynamics, and ship design. In the late 1940s, the Director of the NPL was Sir Charles Galton Darwin (1887-1962; grandson of the famous naturalist), and the Superintendent of the Mathematics Division was John R. Womersley (1907-1958).

Many Colossus personnel were transferred to the NPL after the war, including Alan Turing in October 1945 to lead their computerisation efforts. By 1946 Turing had compiled plans for a machine which was grandly intended to resolve, given the right programming and sufficient run time, any computable problem. It was thus a physical realisation of his hypothetical "Turing Machine", and was originally intended to be bigger in terms of processing power than all the US machines put together. The NPL, equally grandly, believed that if Britain was going to have a large computer of its own to rival the American ones, then Teddington was "the obvious place for it" (Womersley, 1946). Turing presented his proposals in a 1945 design draft

entitled "A Proposal for Development in the Mathematics Division [of the NPL] of an Automatic Computing Engine (ACE)".

> **ASIDE - System Acronyms:** Computing has a long tradition of the contrived computer acronym. Unlike ENIAC and EDVAC, the ACE was deliberately greater than the sum of its initials. There are similar "in jokes" with LEO, the Lyons machine, the fact that ACE was followed by DEUCE, and the fact that many nuclear weapons calculations during the 1950s were carried out, literally, by a MANIAC.

The project did not make much progress, however, primarily because it was technically over-ambitious. The design called for a number of huge technical steps forward (not least a number of parallel processors and a convoluted instruction set), and was accordingly going to require more staff than were available (Flowers, for example, declined an offered post because he was busy repairing the nation's war-damaged telephone system). By December 1946, things had got so bad that the NPL directors called upon one of the delegates to the Moore summer school, Cambridge's Maurice Wilkes, for an opinion on the project's viability, and he wisely suggested that a scaled down version of the system be put together to test the basics (Wilkes, 1946). This was called the Pilot ACE.

In 1948, Turing transferred to Max Newman's laboratory at Manchester, and the Pilot ACE continued in development for two more years under James H. Wilkinson and E.A. Newman, and executed its first program on 10th May 1950 (making it, they claim, the fourth group in the world to deliver a stored program electronic digital computer), and was publicly demonstrated in December that same year. It contained a mere 800 valves, could perform 16,000 simple additions per second in optimal conditions (making it very fast for its day), and input and output were on punched cards. The machine also had available 18 delay lines (eleven slow ones, each capable of storing 32 32-bit words, and seven smaller but faster) .....

> **Key Development - Delay Lines:** This was an apparatus capable of maintaining an electrical pulse train indefinitely, by constantly using it to repropagate itself. The British National Physical Laboratory (see next section) commissioned Dollis Hill's Flowers and Coombs to do some basic research here in June 1946, and they had a prototype 1000-bit delay line working in January 1947. The most common form was the "mercury acoustic delay line", an elongated bath of mercury, some one to two metres long, with a crystal oscillator at both ends. The pulse train was input to the oscillator at one end, and thereby generated a matching pressure wave (push or no-push) within the mercury. This was then detected by the oscillator at the far end, and converted back into electrical pulses. Typically about sixteen 35-bit words would be in transit between the oscillators at any one time, arriving at around one bit per microsecond. The processor had to wait for the desired word to arrive at the far end before it could retrieve it, which was a major source of microdelay. Delay lines were used on the EDVAC, Pilot ACE, EDSAC, BINAC, and UNIVAC systems, and can be described as reliable but slow.

Another GCCS veteran, Treorchy-born Donald W. Davies (1924-2000), joined the project as a mathematician in September 1947, and made important contributions to the final design. He also coded an early noughts-and-crosses computer game before going on to become a major force in packet-switching data transmissions (an ancestor of today's Internet). Pilot ACE was decommissioned in June 1956, and its main components are in the Science Museum. Work on the larger follow-up machines, DEUCE, Full ACE, and the American ACE-clone, the Bendix G15, is described in Part 4. The NPL was also involved in one of the early defence computers, MOSAIC.

6 - The IAS Machine and the "Eckert-von Neumann" Architecture

Having influenced the design of the Moore School's EDVAC, von Neumann returned to Princeton and set up a project there in March 1946, sponsored by the US's newly formed Office of Naval Research. The intention was to build the best that could be built in terms of performance and reliability. It was named the IAS machine, after the hosting Institute of Advanced Studies. The project was led by von Neumann, and

implemented the basic design he had been preaching since 1944 (see under ENIAC above). The resulting hardware sported 3000 valves, and adopted a binary processing with a parallel bus. It could store 2048 40-bit words on magnetic drum and 1024 words in electronic form. It was fast, being capable of 30,000 simple instructions per second (or 1000 complex instructions such as division). One of their team, a programmer named John Wilder Tukey (1915-2000), is famous for having coined the terms **"bit"** (a contraction of "binary digit") and **"software"**.

Alert readers will have noted how John von Neumann's name has occurred several times so far. Basically, this is because he had established a considerable reputation as a mathematical genius before the war. He had joined the staff at Princeton University in 1930, and in 1933 had became one of the six mathematics professors at their newly founded Institute for Advanced Studies. He was thus automatically involved in any computer development carried out at Princeton, and, by virtue of his eminence, as advisor to a host of projects elsewhere (not least, the Manhattan Project). He also taught the young English postgraduate Alan Turing between 1936 and 1938, before the latter returned to Britain to work on the British codebreaking effort.

Above all, von Neumann had used the war years to crystalise a particular technical vision of how digital computers ought to work, and in the closing months of the war he drew up the plans for what came to be called the "von Neumann architecture" for a "general purpose computer" (GPC). His proposals were published in Goldstine and von Neumann (1945), von Neumann (1945), and Burks, Goldstine, and von Neumann (1946), and did much to foster the necessary common understanding and standardisation of approach.

> **ASIDE:** The technical vision was not uniquely von Neumann's, but only he combined the understanding with a position of sufficient influence to do something about it (Zuse, by contrast, was probably technically ahead in 1946, but was working on a shoestring in a country ravaged by war). In the remainder of this paper, we are going to follow Maurice Wilkes' argument (Hipwell, 1999) that ENIAC's Presper Eckert contributed at least as much real substance to this architecture as the more theoretical von Neumann. He therefore prefers the term **"Eckert-von Neumann architecture"**.

In the event, there was little disagreement over von Neumann's proposed macro-architecture, because in terms of its main modules it was essentially little different to Babbage's Analytical Engine, a century beforehand [see Part 1]. To qualify as an "Eckert-von Neumann machine", a computer has to have a number of particular qualities:

- it needs to be electronic not electromechanical
- it needs to be digital not analog
- it needs a binary micro-architecture, not decimal
- it needs to be functionally organised so as to have separate modules for (1) memory, (2) control unit, (3) calculation, and (4) communication with the outside world (ie. input/output, or "I/O" for short), all interconnected by a wiring loom known as the "bus" (a term derived from the "bus-bars" used to carry signals around the old electromechanical switching gear).
- it needs to run binary stored programs from memory, accessing binary data temporarily in that same memory (from which it follows that the control unit must be able to tell the one type of content from the other - or else).
-

These were the design concepts put across at the 1946 Moore School summer school, and they influenced the design of every machine then in the pipeline except the decimal computer ENIAC, which was already too near completion to do anything about. Specifically, it evolved into Williams and Kilburn's Manchester Mark 1, the NPL's Pilot ACE, Eckert and Mauchley's BINAC, the Institute of Advanced Studies' machine, and Wilkes' EDSAC. **In short, the Eckert-von Neumann architecture shaped the computer as we know it today.** It is therefore necessary to look in greater detail at the functional components, because a large

proportion of modern computer jargon dates from these machines - click to be transferred to the associated subfile.

7 - The Engineering Research Associates Machines

Engineering Research Associates (ERA) was formed in January 1946 by a team of experts from the American wartime cryptanalysis effort. They were led by Howard T. Engstrom (1902-1962), previously a Yale mathematics professor, and William C. Norris. The company was based in St. Paul, MN, and did well thanks to the US military's continuing need for code-breaking number crunching. In fact, at a time when some of the Moore School and Harvard developments were struggling, ERA were soon "one of the most advanced computer companies in the world". Their largest project during this period was the 1947 "Task 13" project, another early attempt at a general purpose stored program computer. Gray (1999) is the most accessible source on the resulting ERA 1101. The early work was subsequently scaled up as the Atlas mainframe, and ownership transferred in 1952 when ERA merged into the Remington-Rand Corporation. As explained in Part 4 (Section 1.3), the Atlas then formed the basis of the UNIVAC 1103 production machine. ERA's senior staff were never entirely happy as part of Remington, and in 1957 Norris led a minor exodus to set up the Control Data Corporation [see Part 5 (Section 1.5)].

8 - The Standards Bureau Machines

The American National Bureau of Standards (NBS) also became involved in early computer development. This came about thanks to their prior interest in the production of mathematical tables - experience which meant they had to work very closely with military research units during the war. This cooperation continued after the war, and in 1947 the Office of Naval Research sponsored the "National Applied Mathematics Laboratories" (NAML) as the division of NBS responsible for advising government agencies on computing issues. This brought with it a research funding role, and resulted in two computer development projects. The first contract went in October 1948 to the Institute for Numerical Analysis at the University of California, Los Angeles (UCLA), under the direction of wartime code-breaker Harry D. Huskey, and the other went to its headquarters laboratories in Washington, DC, under the direction of Samuel N. Alexander .....

> **BIOGRAPHICAL ASIDE - HARRY D. HUSKEY:** [Compiled from a number of Internet sources.] Harry D. Huskey became involved in ENIAC in 1944, when it was about half built, and worked on input and output devices for the machine. When the ENIAC team started to split up, he accepted an invitation from the UK to join the ACE project at the NPL [see Section 5], where he was instrumental in initiating the construction of a test model. On returning to the USA in 1948, he joined the NBS, which then pursued two different lines of development: the serial SEAC and the parallel SWAC. Huskey designed SWAC in 1950-53. He moved to UC Berkeley in 1957 and in 1966 founded the Computer Science Department at UC Santa Cruz. After SWAC, Huskey designed a "minicomputer" built by Bendix as their G15.
>
> **BIOGRAPHICAL ASIDE - SAMUEL N. ALEXANDER:** From the Charles Babbage Institute website: "Alexander received his A.B. and B.S. from the University of Oklahoma in 1931, and earned his M.S. from the Massachusetts Institute of Technology in 1933. He was a laboratory engineer for Simplex Wire & Cable Company, a physicist in electronic instrumentation for the Navy, and senior project engineer for Bendix Aviation Corporation, before coming to the National Bureau of Standards in 1946. There he was chief of the Electronic Computer Laboratory, 1946-1954; head of Data Processing Systems Division, 1954-1964; and head of the Information Technology Division, 1964 until his death in 1967. He worked on development of input-output devices for use with electronic computers and wrote specifications for and supervised the procurement of the UNIVAC computer. When delivery of this computer was delayed by design problems, he was assigned to direct the design and assembly of the NBS Interim Computer, later named SEAC".

Due to the widely separated geographical locations of the two development sites, the systems became known as **Standards Western Automatic Computer (SWAC)** and **Standards Eastern Automatic Computer (SEAC)** respectively. SWAC was a serial processing machine fitted with 40 Williams-Kilburn electrostatic

storage tubes, giving a total memory capacity of 256 40-bit words. Backing storage was on an 8192 word magnetic drum. The system remained in use until 1962. SEAC was basically an EDVAC clone (Huskey, 1980), and thus a serial processing machine. Its memory initially consisted of 3072 bytes of mercury delay line storage (Kirsch, 2003). Being a simpler design, and prioritised as a stop gap machine to compensate for delays on the UNIVAC project, it was ready earlier than SWAC, going operational in May 1950 (*Ibid*.). Urban (2001) offers some informative and entertaining reminiscences.

9 - The Whirlwind Project

At MIT, meanwhile, their summer school delegates had gone straight to work on a machine called **"Whirlwind"**. This work was carried out under the aegis of Professor Gordon S. Brown (1907-1996), then the world authority on the theory of servomechanisms (see, for example, Brown and Campbell, 1948), whose Servomechanisms Laboratory had already spent the war years on the sort of analog computation, power-assisted, fire control mechanisms which had transformed the fire control industry from ready reckoner to lethal science. The sponsor, once again, was the Office of Naval Research.

Now it so happened that one of Brown's 1944 projects had been the US Navy's ASCA flight simulation system. This was being developed to an analog computer specification, with the recently graduated Jay Wright Forrester in charge of the computing aspects, and, by a fortunate coincidence, Forrester had on his team a young engineer named Perry Crawford. Crawford had written his master's thesis on the topic of digital fire control systems, and according to Forrester himself was the person who first called his attention to the possibility of digital computation. Forrester accordingly proposed that Whirlwind should do the ASCA processing digitally, rather than electromechanically, and work began against the revised digital specification in early 1946. It then continued as a series of incremental developments until a system was ready for acceptance trials in early 1950. The initial specification was for a ten-ton machine offering 32 different op codes. The Williams-Kilburn Tube (see next section but one) was for rapid access memory until that technology was replaced in 1953. Gordon Welchman, late of Bletchley Park, assisted the application development team between 1948 and 1951.

The Whirlwind project is rightly famous for having introduced ferrite core RAM, and for promoting the use of subroutines. The ferrite story began in 1949, when a Harvard researcher named An Wang (1920-1990) developed the **ferrite toroid** single bit flip-flop, and continued in 1951 when an MIT researcher used these units to build a workable **"core memory"** .....

> **Critical Invention - The Ferrite Toroid (1949) and Ferrite Core Memory (1951):** Wang's invention was a tiny ferrite toroid. Ferrite is a clay-iron oxide mix, baked as a ceramic. It therefore has good magnetic properties. Before firing, the mixture can readily be pressed into shape. A toroid is the technical name for the shape of a doughnut, so it has a central hole through which a thin wire can be passed. The passage of a current through the wire will then affect the magnetic state of the ferrite, and the magnetic state of the ferrite will affect the passing current. This therefore offered a conceptually neat way of linking two electrical states (On/Off) with two magnetic states (On/Off), or, to put it another way, of storing electrical pulses in ferrite on demand, and retrieving them as electrical pulses when needed. Wang filed for a patent on 21st October 1949 (granted 17th May 1955), but his invention fell short of RAM as we know it today, largely because Wang himself did not fully realise the implications of what he had done. This required a second advance, namely of wiring the ferrite toroids from two directions at once, that is to say, of passing two wires through each toroid so that they ended up strung together like the knots ("nodes") on a fishing net. The technique was developed by MIT's Whirlwind team in 1951, and a matrix of 16,384 toroids was fitted to the Whirlwind in August 1953. The technology remained in use until the mid-1970s, when integrated circuits allowed much greater miniaturisation.

Waldrop (2001) points out that Whirlwind was not designed for calculating per se. It was built as an electronic flight simulator, "a machine for which there was never an 'answer', just a constantly changing sequence of pilot actions and simulated aircraft responses" (p73). In consequence, the machine rates as the

first major real-time digital computer. Forrester subsequently spent a number of years networking a large number of Whirlwind clones into a giant command and control system known as SAGE, which effectively was US strategic air defence between 1963 and 1983.

10 - The IBM SSEC

The Selective Sequence Electronic Calculator (SSEC) was IBM's first in-house digital computing project, and it owes much of its success to the fact that it was conceived in a moment of anger. Pugh (1984) suggests that IBM's Thomas J. Watson Sr was so deeply angered by the lack of credit given to IBM during the development of the Harvard Mark 1 that he authorised the follow-up project in-house. The project began in March 1945, and was led by Wallace J. Eckert, originally a Columbia University astronomer. Faced with some difficult astronomical calculations during the 1930s, Eckert had pushed IBM's tabulating equipment to, and beyond, its limits, so that by 1934 it could carry out multiplications and subtractions as well as additions, and could do so, moreover, in simple controlled sequences. When Watson wanted someone good, and someone non-Harvard, Eckert got the job. The specifications were ready in January 1946, and at Watson's direct insistence outperformed everything Harvard was working on. The machine was ready in July 1947, was publicly announced on 27th January 1948, and consisted of 21,500 relays and 12,500 valves. It had eight 20-decimal digit registers, and could perform about 250 simple additions per second. It was replaced in 1952 by the IBM701 series (see Part 4). Apart from anything else, the SSEC earned some of its fame from the fact that Watson sited its computer hall at 590 Madison Avenue, New York, where it was deliberately visible from the street. As a result, the SSEC rapidly became the popular image of what computers ought to look like.

11 - The Manchester University Machines

Some of the Bletchley Park team, initially Newman, Good, and Rees, but eventually Turing himself, together with some of the TRE people, notably Frederic (later Sir Frederic) Calland Williams (1911-1977), Thomas ("Tom") Kilburn (1921-2001), and Geoff Tootill, ended up after the war at Manchester University. Newman, Good, and Rees were the first to arrive in around October 1945, and strengthened the Department of Mathematics. Good and Rees were amongst the delegates to the 1946 Moore School summer school, and, upon their return, the team sketched out the design for a second British Turing machine (to complement Turing's own proposed Turing machine at the NPL). Williams arrived in January 1947 as Professor of "Electrotechnics", and Kilburn and Tootill (initially on secondment from TRE) joined later. Using TRE surplus equipment, the team started to put together a Small-Scale Experimental Machine - the SSEM, or "Baby".

> **ASIDE:** Burton (2003 personal communication) attributes the design of the SSEM to Kilburn, assisted by Tootill, and points out that the motivation was as much the investigation of storage technology as computation.

The main SSEM build took place during 1947, and the machine ran its first program 21st June 1948. It contained some 500 valves, could process seven different instructions, and could access up to 1024 bits of randomly accessible information on what has come to be known as a Williams-Kilburn [Cathode Ray] Tube .....

> **Key Development - Williams-Kilburn [Cathode Ray] Tube:** This was a cathode ray tube (CRT) (just like those used in televisions), which made use of the one-second-or-so residual electrostatic charge left on the screen following each passing of the electron beam. Appropriately equipped with sensors, CRTs could thus operate as fast "random access" devices. The technology was subsequently used on the IAS machine, the Manchester Mark 1, and the Whirlwind project (until it developed ferrite core RAM in 1953), and can be described as fast but not particularly reliable. Impressed by the speed factor as a marketing advantage in their

confrontation with Remington-Rand, IBM did much to improve the reliability of CRT technology, and installed the technology in the highly successful IBM701 series (see Part 4).

The Baby was the world's first stored program machine (beating BINAC - see below - by nine months), and Kilburn wrote the first program. The system was demonstrated to Sir Ben Lockspeiser, Chief Scientist at the Ministry of Supply, in October 1948, and he was so impressed that government funding was made available via Ferranti Limited for a scaled up version (Lavington, 1980). This was known as the **"Ferranti Mark 1"**. Turing joined the Mathematics Department as reader in 1948, whilst among the younger members of the electrotechnics team were the Cwmamman-born Gordon Eric ("Tommy") Thomas, the Pontypridd-born David B.G. ("Dai") Edwards, Alec Robinson, Richard Grimsdale, and J.C. ("Cliff") West. Tommy Thomas's website is full of informative fact and anecdote, and shows that the Internet is no barrier to the properly trained old-timer.

The Mark 1 also had access to more permanent storage on a magnetic drum.

Key Development - Magnetic Drum: This was a non-ferrous cylinder, coated with magnetic medium, and rotated against a row of magnetic read-write heads connected to the input-output controller. It could thus be used a temporary storage for one or more rotations of the drum during program execution, or as backing storage between programs. Drums were used on the Manchester Mark 1, and the Whirlwind project (although again only until it developed ferrite core RAM in 1953).

12 - The Cambridge University EDSAC and the Lyons LEO

Cambridge University's attempt at an Eckert-von Neumann machine was led by Maurice Wilkes. The machine in question was the **Electronic Delay Storage Automatic Calculator**, or **EDSAC**. Work began as soon as Wilkes returned from the Moore School summer school, and the team included J. Bennett, W. Renwick, R. Piggott, S.A. Barton, David J. Wheeler, and (later) Stan Gill. The development lifecycle was carefully managed, and the machine went live just under three years later, on 6th May 1949. It was based around 32 random access mercury delay lines, each holding 16 35-bit words, could execute around 750 simple additions per second, and was used to support departmental research across the university. Here is the complete set of EDSAC "order codes", as laid down in Wilkes and Renwick (1950/1982). Note (a) how input and output feed in and out of memory (the "storage locations" mentioned), and (b) how memory is manipulated by accumulators and registers. **This is still how computers do their work.** The hard part is doing it all in the right order, and that is where computer programmers (and lots and lots of very expensive time for testing) come in.

A n = Add the number in storage location n into the accumulator.
S n = Subtract the number in storage location n from the accumulator.
H n = Transfer the number in storage location n into the multiplier register.
V n = Multiply the number in storage location n by the number in the multiplier register and add into the accumulator.
N n = Multiply the number in storage location n by the number in the multiplier register and subtract from the accumulator.
T n = Transfer the contents of the accumulator to storage location n and clear the accumulator.
U n = Transfer the contents of the accumulator to storage location n and do not clear the accumulator.
C n = Collate the number in storage location n with the number in the multiplier register, ie. add a '1' into the accumulator in digital positions where both numbers have a '1', and a '0' in other digital positions.

R 2 n-2 = Shift the number in the accumulator n places to the right; ie multiply it by 2^{-n}.

L 2 n-2 = Shift the number in the accumulator n places to the left; ie multiply it by 2^{n}.

E n = If the number in the accumulator is greater than or equal to zero execute next the order which stands in storage location n, otherwise proceed serially.
G n = If the number in the accumulator is less than zero execute next the order which stands in storage location n, otherwise proceed serially.
I n = Read the next row of holes on the tape and place the resulting 5 digits in the least significant places of storage location n.
O n = Print the character now set up on the teletypewriter and replace it with the character represented by the five most significant digits in storage location n.
F n = Place the five digits which represent the character next to be printed by the teletypewriter in the five most significant digits in storage location n.
X = Round off the number in the accumulator to 16 binary digits.
Y = Round off the number in the accumulator to 34 binary digits.
Z = stop the machine and ring the warning bell.

Wilkes and Renwick continue:

> "Ordinary 5-hole punched tape of the kind used in telegraphy is used for input. Each row of holes represents a 5-digit binary number and the basic input operation is to transfer this number to the store." (Wilkes and Renwick, 1950/1982, p418.)

Wilkes is often credited with the invention of **"Assembly Code"**, the generic name for software which translates human-readable instructions into machine instructions [more on this in Part 4 (Section 3.2)]. EDSAC was replaced in 1957 by EDSAC II.

Here is an analysis of the EDSAC's strengths and weaknesses, measured against the criteria of modernity discussed so far .....

Electronic rather than Electromechanical	**Digital rather than Analog**	**Binary rather than Decimal**	**General Purpose Stored Program**
Yes	Yes	Yes	Yes

The EDSAC was also the prototype for the Lyons Electronic Office ("LEO") series of production machines. Aris (2000) begins this story in 1923, when J. Lyons and Company, tea merchants and caterers, took on a Cambridge University mathematics graduate named John Simmons in order to bring some scientific rigour into the design and operation of its corporate processes. Slowly Lyons became one of Britain's best managed companies, and experts in what was then known as "O and M" (= organisation and methods) or "OR" (= operational research). This exposed them to the tabulating and calculating equipment of the time, and they began to incorporate this in very creative ways into their corporate systems. Indeed Simmons's motto was that an organisation's records ought to show its managers what needed to be done next, not what had already been done.

Simmons was joined in 1936 by David Caminer, who by the late 1940s had risen to manager of the Systems Research Office, "a forward-looking team, some twenty strong, considering new systems approaches and new technologies" (Aris, 2000, p5), and it was against this background of disciplined risk-taking that two of the company's directors, Thomas R. Thompson (d.1972) and Oliver Standingford, went off on a fact-finding tour of computing installations in the US. What they wanted to know was whether the new breed of computers was going to replace punched card tabulators, and what influence they were going to have on office automation. They consulted with established experts such as Goldstine, and upon their return prepared a computerisation proposal which would cost Lyons £100,000 up front, but deliver some £50,000 annual savings in administrative and clerical effort. This was the first attempt at electronic office automation in the civilian world, and Lyons helped defray what was at that time a major investment risk by allocating a further £3000 to the EDSAC team in Cambridge for technical advice. Lyons advertised for a project leader, and in January 1949 recruited an ex-TRE electronics engineer named John M.M. Pinkerton (1919-1997). No insuperable problems were encountered, and the machine - to all intents and purposes an EDSAC clone - ran its first program on 5th September 1951 (Bird, 1994). In 1949, Pinkerton devised the typical brought-forward/carried-forward batch processing routine for payroll applications, and with the aid of Caminer computerised a number of vital management systems. Caminer boldly raised his team of programmers in-house. In other words, he made the since-often-challenged value judgement that it was better to know the company and learn how to program, than the other way round. The company's payroll system first ran live in early 1954, and its stock replenishment system was sophisticated enough to allow "weather-sensitive logistics", increasing the number of salads supplied on hot days and the number of steak and kidney puddings on cold!

The LEO 1 contained 5000 valves, and used mercury delay line storage. It also used three buffered input channels, and two buffered output channels, enabling large blocks of data to be read or written at a time. In this way, the record for employee (n+1) would be on its way into the machine while that for employee (n) was being processed and that for employee (n-1) was on its way out of the machine. (The last British Telecom LEO 3-26 was withdrawn from service in 1980, a few weeks after the present author joined them as a trainee systems analyst.)

13 - BINAC and UNIVAC

Having resigned from the Moore School, Eckert and Mauchly's next projects were the UNIVAC for the commercial sector and the BINAC for the military. The BINAC development started first in response to an order from the Northrop Aviation Company for a small high reliability machine. The build lasted from October 1947 to August 1949, and the system was delivered in September 1949, making it the first operational US stored program computer. It developed 3500 additions per second from a 700-valve system with 512 30-bit registers, and boasted 16 order codes in its instruction set. Every critical module was twinned, so that each could check the output of the other, shutting down automatically should a discrepancy be detected. The machine was only five feet high and four feet long.

In purely commercial terms, however, BINAC was a disaster, coming in seriously over budget on what had been a fixed-price contract. The eventually more successful **Universal Automatic Computer**, or **UNIVAC**, development followed in 1948. This began life as a one-off for the US Census Bureau, under a contract signed in September 1946, but again development costs soon began to exceed the agreed price of $350,270, and in 1948 Eckert and Mauchly had no choice but to sell 40% of their company to American Totalisator Company in return for an injection of capital. A subsequent deal in November 1949 saw the company incorporated into the Remington-Rand Corporation, who funded the rest of the development.

The basic binary code used 6 substantive bits, giving it a repertoire of 64 different characters. There was also a seventh parity bit .....

> **Key Development - Parity Bit:** Parity bits are additional bits tagged on to the end of an otherwise already meaningful bit sequence. They are set according to a mathematical algorithm, and then regularly rechecked during processing. They are thus extremely effective ways of detecting incipient equipment failure or file corruption.

UNIVAC delivered 2000 simple additions per second from a 5400 valve system with 1000 84-bit words in mercury delay line memory. A total of 46 machines were produced before the range was replaced by the UNIVAC 2 (see Part 4). They were generally reliable and comparatively easy to program.

14 - Hardware Summary Table, 1943-1950

The EDSAC, LEO 1, and UNIVAC are convenient demarcation points between computing's formative years and the early production years (covered in Part 4). Here is a progress summary table for those formative years. The material contained is from many sources, including Berkeley (1949/1961), Wilkes (1956), Hollingdale and Tootill (1965), Evans (1983), and a host of US and British Internet primary sources, including, sadly, many obituaries. The concluding entry - for UNIVAC - is repeated at the beginning of the first table in Part 4, because it is a transitional machine.

Name/	Project Leader(s)/	Date/	Remarks

Claim to Fame	Purpose	Sponsor	
Relay Interpolator First use of biquinary notation for additional reliability	Samuel Williams, George Stibitz Ballistics computation for the AA Predictor No. 9 (see Part 2).	Started 1941 Operational September 1943 Decommissioned 1961 Bell Telephone Laboratories, for the US National Defence Research Laboratories	Also known as Bell Labs "Model 2 Relay Calculator". (The Model 1 was described at the end of Part 2.)
The Bombe First series of UK electromechanical digital computers	Max Newman, Tommy Flowers, Alan Turing, C.E. Wynn-Williams, Gordon Welchman, Jack Good (from 1941) Military code-breaking	Started late 1939 Operational late 1941 Bletchley Park Military Intelligence Centre	Once the prototype had proven itself, several hundred further machines were built by 1945.
The Robinsons First UK electronic digital computers	Max Newman, Tommy Flowers, Alan Turing, C.E. Wynn-Williams, Gordon Welchman, Jack Good (from 1941), Shaun Wylie (from 1943) Military code-breaking	Started 1942 Operational mid-1943 Bletchley Park Military Intelligence Centre	Valve-based experimental machines, soon replaced by the Colossus series (see below).
Ballistic Computer	Samuel Williams, George Stibitz Ballistics computation for the AA Predictor No. 9 (see Part 2).	Started 1942 Operational June 1944 Bell Telephone Laboratories, for the US National Defence Research Laboratories	Also known as Bell Labs "Model 3 Relay Calculator".
Colossus 1 First UK electronic digital computers	Max Newman, Tommy Flowers, Alan Turing, C.E. Wynn-Williams, Gordon Welchman, Jack Good (from 1941), Donald Michie (from 1942) Military code-breaking	Started January 1943 Operational December 1943 Bletchley Park Military Intelligence Centre	
Colossus 2 First UK electronic digital computers	Max Newman, Tommy Flowers, Alan Turing, C.E. Wynn-Williams, Gordon Welchman, Jack Good (from 1941), Donald Michie (from 1942), A.W.M. Coombs Military code-breaking	Started March 1944 Operational June 1944 Bletchley Park Military Intelligence Centre	A further nine machines were built by 1945.
ASCC (or "Harvard Mark I") Largest ever electro-mechanical calculator; digital rather than analog	Howard H. Aiken, Robert Campbell, Grace Hopper (from 1942) Ballistics computation and other *important* war work.	Started 1937; operational January 1943 on-site at IBM, August 1944 at Harvard; further development to 1947 (when replaced by Mark 2 - see below); dismantled for museum use 1959. Harvard University, largely funded by IBM	ASCC = Automatic Sequence-Controlled Calculator A work-horse, but not earth-shatteringly innovative.
AA Predictor No. 9 Third generation analog flak predictor	Samuel Williams	Started Operational 1943 Bell Labs	Very successful analog system. It would still be another decade before digital systems started to compete for battlefield computation. It did, however, make considerable use of digital equipment for testing purposes - see the entries for the Relay Interpolator and the Ballistic Computer above.
Z4 First complete programming language PLANKALKÜL	Konrad Zuse General purpose computing	Started 1941 Completed 1946 Konrad Zuse personally	
Harvard Mark II First computer "bug" located 15th September 1945 by Grace Hopper (a moth jammed into one of the 13,000 or so component relays)	Howard Aiken, Grace Hopper (until 1949), Edmund C. Berkeley, Frederick Miller	Started 1942 Acceptance testing July 1947 Delivered January 1948 to the Naval Proving Ground, Dahlgren, VA	

		Harvard Computation Labs	
ENIAC First purely electronic computer	John Brainerd, John Mauchly (until 1946), Presper Eckert (ditto), Herman Goldstine, Arthur Burks, Thomas Sharpless, Robert Shaw Ballistics computation and other *important* war work.	Started May 1943; operational February 1946; delivered to the Aberdeen Proving Ground, MD, January 1947; recommissioned August 1947; further development until October 1955. Moore School of Electrical Engineering, University of Pennsylvania, for the Ballistics Research Labs, Aberdeen, MD	Eckert and Mauchly fell out with the University of Pennsylvania in March 1946, and left to form their own company.
General Purpose Relay Calculator Early self-checking system, and therefore comparatively reliable	Bell Labs team, incl. George Stibitz and Samuel Williams	Started 1944 Two-off, one operational July 1946 at the National Advisory Committee for Aeronautics, Langley Field, VA, and the other February 1947 at the US Army's Ballistic Research Labs, Aberdeen, MD.	Also known as Bell Labs "Model 5 Relay Computer". These machines cost roughly $500,000 each.
Whirlwind 1 First use of ferrite core memory; first real time command and control applications	Gordon Brown, Jay Forrester, Robert Everett, Perry Crawford, William Papian, Harlan Anderson (from 1952), Ken Olsen, Jack Gilmore (from 1950), Charles Adams, John Carr, Gordon Welchman (from 1948 to 1951) Gunnery fire control; real-time simulation	Started 1944 as an analog flight simulator project; respecified for digital computation late 1945-early 1946; operational June 1950; fitted with 16kb ferrite core store August 1953 (enough for 1024 16-bit words). MIT, for the US Navy	Anderson and Olsen left in 1957 to found the Digital Equipment Corporation (DEC). Welchman had been one of the Bletchley Park originals.
EDVAC First US large-scale von Neumann (ie. binary stored program) computer; came complete with a operating system	Moore School team, now incl. John von Neumann, but no longer Eckert and Mauchly, who had transferred to the UNIVAC project (above)	Scoping meeting August 1944; design draft 1945; build started 1946, but subject to repeated design upgrades as problems were solved and new techniques developed; assembled and delivered while still non-operational August 1949; ran first program November 1951; operational April 1952; decommissioned December 1962. Moore School of Electrical Engineering, University of Pennsylvania, for the Ballistics Research Laboratory, Aberdeen Proving Ground, MD.	EDVAC = Electronic Discrete Variable Automatic Computer. This was not a particularly well managed project. ORDVAC (see Part 4) started many months later and nearly beat it into service.
IAS Early US stored program machine	John Von Neumann, Herman Goldstine, Julian Bigelow (from January 1946); Willis Ware (until 1952); John Tukey; Ralph Slutz	Started March 1946 Operational Spring 1952 Institute for Advanced Study, Princeton University	The IAS was to all intents and purposes a research machine. It had no fixed delivery date, and was constantly being tinkered with as new ideas - some good, some bad - came and went. Thus although development began before EDSAC the machine did not become operational until after it. Eventually, however, it would spin off a number of major clones.
Pilot ACE Fastest ever processor at the time, with a separate module for parallel computation of multiplications and divisions.	John Womersley, Alan Turing (until 1948), Jim Wilkinson (from May 1946), Edward A. Newman; G.G. Allway; Harry Huskey (from January 1947), Michael Woodger, Robin Gandy, Donald Davies (from September 1947)	Specification work 1946; development 1949; pilot operations April 1950, then constantly improved until discarded 1958 in favour of the full ACE. National Physical Laboratory	Huskey, an American on placement, returned to the US to manage the SWAC project, see below.
IBM SSEC First IBM in-house electronic digital computer.	Wallace Eckert, R. Seeber, Frank Hamilton, Wayne Brooke	Started March 1945; acceptance testing late 1947; operational January 1948; decommissioned August 1952 IBM	SSEC = Selective Sequence Electronic Calculator

Baby First stored program; Williams tube storage.	Frederick Williams, Tom Kilburn, Alec Robinson, Geoff Tootill research prototype	Started 1947 Operational 21st June 1948 Manchester University	Williams and Kilburn had worked together since 1942 on a number of military electronics projects. They moved to Manchester University in 1946. Tootill joined as Kilburn's assistant in 1947.
Harvard Mark III First major use of magnetic drum memory.	Howard Aiken, Grace Hopper (until 1949), Edmund C. Berkeley, An Wang (between 1948 and 1951), Frederick Miller	Started 1947 Operational March 1951 Harvard Computation Labs for the US Navy at Dahlgren, VA	An Wang patented the ferrite toroid (see main text) in 1949, left to found his own company, Wang Labs, in 1951, and from 1965 was a major force in the pocket calculator market.
Manchester Mark I First large-scale von Neumann computer; first Williams-Kilburn tube random access memory; first magnetic drum store; development prototype for Ferranti Mark 1 production series	Frederick Williams, Tom Kilburn, Alan Turing (from September 1948), Geoff Tootill (until January 1949), Alick Glennie, Jack Good (until 1948), David Rees (until 1949), P.M.S.Blackett, David Edwards (from October 1948), Tommy Thomas (same), Alec Robinson, Cliff West; Andrew Booth	Started 1948; Pilot Operations April 1949; Fully operational October 1949; Replaced February 1951 by a Ferranti Mark 1 Manchester University, with research funding from Ferranti and the Royal Society	Geoff Tootill left for Ferranti after the Baby had been born, and established close liaison between that company and Manchester University
EDSAC First full-sized stored program computer; first bootstrap (fast start) routine; first subroutines and reusable code; development prototype for J. Lyons and Company's LEO production series.	Maurice Wilkes, David Wheeler, W. Renwick, S. Barton, G. Stevens, Stan Gill (from 1949)	Started 1947; operational May 1949; further development until 1953; decommissioned July 1958, when replaced by EDSAC II Cambridge University, with some sponsorship from J. Lyons and Company.	EDSAC = Electronic Delay Storage Automatic Calculator The team subsequently published many of their ideas in the first textbook of programming, "The Preparation of Programs for an Electronic Digital Computer" (Wilkes, Wheeler, and Gill, 1951).
MOSAIC Early British use of valve-transistor mix.	Dollis Hill engineers under A.W.M. Coombs	Started 1947 Operational 1954 Dollis Hill, for the Ministry of Supply	
BINAC First twinned processor for greater reliability; early use of magnetic tape rather than punched cards; first US stored program computer.	Eckert and Mauchly	Started October 1947 Program Testing March 1949 Pilot operations August 1949 Delivered September 1949 Eckert-Mauchly Computer Corporation, Philadelphia, PA (on behalf of Northrop Aviation)	BINAC = Binary Automatic Computer. In purely commercial terms, this was little short of a disaster, forcing Eckert and Mauchly to sell control of their company to the Remington-Rand Corporation.
Harvard Mark IV	Howard Aiken, Grace Hopper (until 1949), Edmund C. Berkeley, An Wang (between 1948 and 1951), Frederick Miller; Ken Iverson (programming)	Delivered 1952 Harvard Computation Labs	Iverson subsequently developed the APL programming language.
LEO 1 Early use of buffered I/O channels; early UK use of transistors	John Pinkerton, Ernest Lanaerts, David Caminer General purpose commercial computing	Started 1949 Completed 1953 J. Lyons and Co Ltd	LEO = Lyons Electronic Office.
SEAC Probably the first US stored program computer to go fully operational	Sam Alexander	Operational May 1950 US Bureau of Standards, Washington, DC	SEAC = Standards' Eastern Automatic Computer
SWAC	Harry Huskey	US Bureau of Standards, Los Angeles, CA	SWAC = Standards' Western Automatic Computer
UNIVAC 1 First use of magnetic tape as long-term storage; first stores system project (on the USAF machine from	John Mauchly and Presper Eckert, Grace Hopper (from 1949) General Purpose Computing	Started 1948 Operational March 1951	UNIVAC = Universal Automatic Computer. Eckert and Mauchly's company was bought out by Remington-Rand in

1952); first payroll project (on the General Electric machine from 1953).		Initially Eckert-Mauchly Computer Corporation, Philadelphia, for the US Census Bureau.	1950. A total of 46 machines were eventually built, selling at around $1M each.

15 - References

[Back][Next][Home]