The Tanker arrives.

Air Force News
June 2011

33 Squadron's first of 5 KC-30A tanker aircraft arrived at Amberley on the 30th May. Based on the Airbus A330 passenger aircraft, the KC-30A's replace the RAAF's B707 fleet which was retired recently. The RAAF is the first 'customer' to receive the KC-30 aircraft which is the most advance tanker aircraft in the world today. It can transfer fuel at the rate of 1,200 gallons (5,400 litres) of fuel per minute from its rear mounted boom (which can extend 19 metres) and 420 gallons (1,900 litres) per minute from the wing mounted hose and drogue pods.

The KC-30A is the largest aircraft to be operated by the RAAF. It is 5.8m longer, 60cm taller, and has a wingspan 8.55m wider than the C-17A. The RAF, United Arab Emirates, and Saudi Arabia have all ordered similar aircraft.

Each aircraft carries a crew of 3, 2 pilots and an air-refuelling operator. Addition crew attendants will be carried depending on mission requirements. The air refuelling operator works from a console in the cockpit and can direct the Advanced Refuelling Boom System in the tail of the aircraft using fly-by-wire controls. The operator is also responsible for the two hose and drogue refuelling pods on the wings. This console includes 3 dimensional and panoramic displays, which feed video of outside the aircraft, allowing clear situational awareness of receiver aircraft.

It can carry 50 tonnes of fuel, fly 1,000nm and act as a refuelling station for fighters, staying on the job for more than four hours. The fuel is carried below the floor, in the space normally used to carry passenger's luggage in commercial aircraft. It will be able to act as tanker for the F-18's, the Wedgetail, C-17's and other KC-30As. Parked alongside the C-17As at Amberley. the KC-30A will make a massive contribution to Air Force's air mobility fleet.

When required, it can be fitted with 270 passenger seats and be used as a rapid troop carrier in which case it will also carry these two lovely girls who are airborne Crew Assistants. The role of the Crew Assistant is to provide safety, comfort and in-flight service to passengers – "ol i kolim" … Hosties…

L-R: Erin Wallace, Daniella Olofsson

With the seats removed, it can carry 45,000kg of cargo. The RAAF should have the Squadron up to speed and all 5 KC-30's at Amberley fully operational by end 2012.

Tunny.

Richard Harcourt from the UK sent us this story.
He found it on ZD Net.

Engineers at the National Museum of Computing at Bletchley Park have rebuilt the Tunny machine, a key device used in decoding German High Command messages during the Second World War.

TUNNY was the top-level cipher system, developed by used between Army HQ in Berlin and the Generals and Field Marshals in the field. Many were signed by Field Marshals; von Rundstedt, Rommel, Keitel, Jodl etc. – including messages signed by Hitler himself. Tunny had 12 wheels, was very advanced, more complex, faster and more secure than the 3-wheel Enigma machine. Tens of thousands of Tunny messages were intercepted by the British and broken at Bletchley Park by Capt. Jerry Roberts and his fellow code-breakers in the Testery. These messages contained much vital insight into top-level German thinking and planning.

Tunny was one of three types of teleprinter cipher machines used by the Germans during the war. At Bletchley Park these were given the general cover name 'Fish'. The other members of the Fish family were Sturgeon, the Siemens and Halske T52Schlüssel fernschreib maschine ('Cipher Teleprinter Machine') as well as the unbreakable Thrasher. Thrasher was probably the Siemens T43, a one time tape machine but it was upon Tunny that Bletchley park chiefly focussed.

The Tunny machine, which measured 19" by 15½" by 17" high, was actually a cipher attachment and when attached to a teleprinter, it automatically encrypted the outgoing stream of pulses produced by the teleprinter, or automatically decrypted incoming messages before they were printed. (Sturgeon, on the other hand, was not an attachment but a combined teleprinter and cipher machine.) At the sending end of a Tunny link, the operator typed plain language at the teleprinter keyboard, and at the receiving end the plaintext was printed out automatically by another teleprinter (usually onto paper strip, resembling a telegram). The transmitted 'ciphertext' (the encrypted form of the message) was not seen by the German operators.

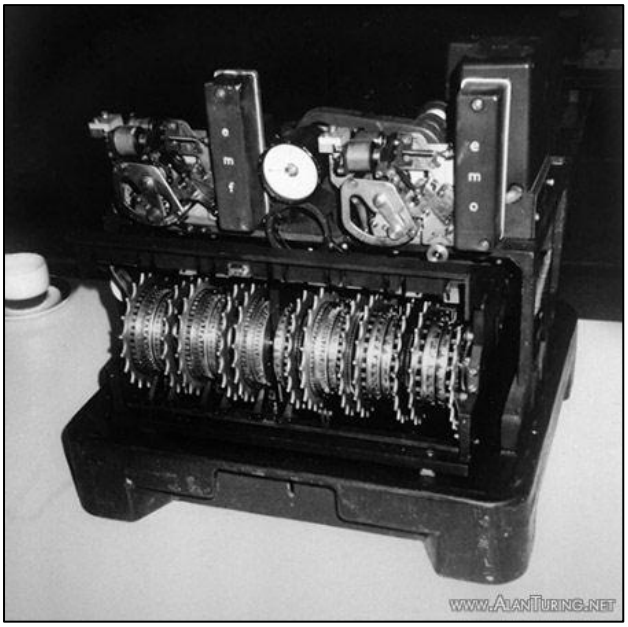
With the machine in 'auto' mode, many long messages could be sent one after another—the plaintext was fed into the teleprinter equipment on pre-punched paper tape and was encrypted and broadcast at high speed.

Enigma was clumsy by comparison. A cipher clerk typed the plaintext at the keyboard of an Enigma machine while an assistant painstakingly noted down the letters of the ciphertext as they appeared one by one at the machine's lamp-board. A radio operator then transmitted the ciphertext in the form of Morse code. Morse code was not used with Tunny: the output of the Tunny machine, encrypted teleprinter code, went directly to air.
International teleprinter code assigns a pattern of five pulses and pauses to each character. Using the Bletchley convention of representing a pulse by a cross and no pulse by a dot, the letter C, for example, is •xxx•: no-pulse, pulse, pulse, pulse, no-pulse. More examples: O is •••xx, L is •x••x, U is xxx••,and S is x•x••. (*You old Comm Officers can see the complete teleprinter alphabet HERE*).

When a message in teleprinter code is placed on paper tape, each letter (or other keyboard character) takes the form of a pattern of holes punched across the width of the tape. A hole corresponds to a pulse (cross).

The first Tunny radio link, between Berlin and Athens/Salonika, went into operation on an experimental basis in June 1941. In October 1942 this experimental link closed down, and for a short time it was thought that the Germans had abandoned the Tunny machine. Later that same month Tunny reappeared in an altered form, on a link between Berlin and Salonika and on a new link between Königsberg and South Russia. At the time of the allied invasion in 1944, when the Tunny system had reached its most stable and widespread state, there were 26 different links known to the British. Bletchley Park gave each link a piscine name: Berlin-Paris was Jellyfish, Berlin-Rome was Bream and Berlin-Copenhagen Turbot etc. The two central exchanges for Tunny traffic were Strausberg near Berlin for the Western links, and Königsberg for the Eastern links into Russia.

The distant ends of the links were mobile. Each mobile Tunny unit consisted of two trucks, one carrying the radio equipment and the other the teleprinter equipment and two Tunny machines, one for sending and one for receiving. The radio trucks had to be kept well away from the teleprinters for fear of interference. The radio truck also carried a device for punching tapes for auto transmission. If a land line was used in preference to radio, the truck carrying the Tunnies would be connected directly into the telephone system. (Only Tunny traffic sent by radio was intercepted by the British.)



As with the Enigma, the heart of the Tunny machine was a system of wheels. Some or all of these wheels moved each time the operator typed a character at the keyboard or if punched tape was being fed into the machine, each time a new letter was read. There were twelve wheels in all. They stood side by side in a single row, like plates in a dish rack. As in the case of Enigma, the rim of each wheel was marked with numbers, visible to the operator through a window, somewhat like the numbers on the rotating parts of a combination lock.

From 1941 Hitler and the German High Command relied increasingly on Tunny to protect their communications with Army Group commanders across Europe. Tunny messages sent by radio were first intercepted by the British in June 1941.

From October 1942 and before starting to send a message, the operator would use his thumb to turn the wheels to a combination that he looked up in a codebook containing one hundred or more combinations (known as the QEP book). At Bletchley Park this combination was called the setting for that particular message. The operator at the receiving end, who had the same QEP book, set the wheels of his Tunny machine to the same combination, enabling his machine to decrypt the message automatically as it was received. Once all the combinations in a QEP book had been used it was replaced by a new one. The wheels were supposed to be turned to a new setting at the start of each new message although because of operator error/laziness this did not always occur and it was thanks to the interception of these messages, in the summer of 1941, that the Research Section at Bletchley Park first found its way into Tunny.

When these two messages with the same indicator were intercepted, Bletchley Park suspected that they had found an important clue into the code system, but as it turned out, the first transmission had been corrupted by atmospheric noise and the message was resent at the request of the receiving operator. Had the sender repeated the message identically, the use of the same wheel settings would have left Bletchley Park none the wiser. However, in the course of the second transmission the sender introduced abbreviations and other minor deviations (the message was approximately 4000 characters long). So the depth consisted of two not-quite-identical plaintexts each encrypted by means of exactly the same sequence of key—a code-breaker's dream. It was William Thomas Tutte (right) who worked out the coding method from the two messages.

The Tunny machine encrypted each letter of the message by adding another letter to it. The internal mechanism of the Tunny machine produced its own stream of letters, known at Bletchley Park as the 'key-stream' key. Each letter of the cipher text was produced by adding a letter from the key-stream to the corresponding letter of the plaintext. The Tunny machine adds letters by adding the individual dots and crosses that compose them. The rules that the makers of the machine selected for dot-and-cross addition were simple. Dot plus dot is dot. Cross plus cross is dot. Dot plus cross is cross. Cross plus dot is cross. In short, adding two sames produces dot, and adding a mixed pair produces cross. (*The Nerds will recognise Tunny addition as boolean XOR*.)

For example, if the first letter of the plaintext happens to be M, and the first letter of the key-stream happens to be N, then the first letter of the ciphertext is T: adding M (••xxx) and N (••xx•) produces T (••••x).

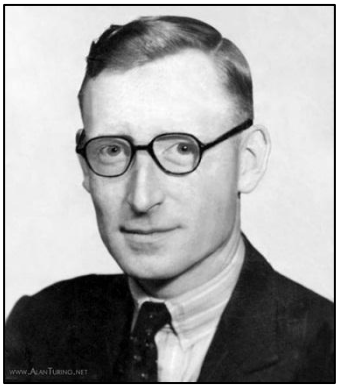
The German engineers selected these rules for dot-and-cross addition so that the following is always true (*no matter which letters, or other keyboard characters, are involved*): adding one letter (or other character) to another and then adding it again a second time leaves you where you started. For example, adding N to M produces a T and then adding N to T leads back to M.

Once Bletchley knew the nature of the coding machine, the next step was to devise methods for breaking the daily traffic. A message could be read if the wheel settings and the wheel patterns were known. The German operators themselves were revealing each message's setting via the 12-letter indicator. Thanks to Tutte's feat of reverse-engineering, the wheel patterns were known for August 1941. The codebreaker's problem was to keep on top of the German's regular changes of wheel-pattern.

In July 1942 Alan Turing invented a method for finding wheel-patterns which became known as 'Turingery'. Turing was at that time on loan to the Research Section from Hut 8 which was working on the code used by the German Navy called Enigma. Turingery was the third of the three strokes of genius that Turing contributed to the attack on the German codes, along with his design for the Bombe (an electromechanical device) and his unravelling of the form of Enigma used by the Atlantic U-boats. It was said that "what Turing did might not have made us win the war, but we might have lost it without him".

Turingery was a manual method, involving paper, pencil and eraser. Beginning with a stretch of key obtained from a message, Turingery enabled the breaker to prize out from the message the contribution that the chi-wheels had made. The cam-patterns of the individual chi-wheels could be inferred from this. Further deductions led to the cam-patterns of the wheels. Once gained via Turingery, this information remained current over the course of many messages. Eventually the patterns were changed too frequently for any hand method to be able to cope (there were daily changes of all patterns from August 1944), but by that time Colossus, not Turingery, was being used for breaking the wheel patterns. These decrypts contained intelligence that changed the course of the war in Europe, saving an incalculable number of lives.

Colossus



Colossus was the first large-scale electronic computer and was used at Bletchley Park against the German code system. It was designed by an engineer named Tommy Flowers (right) at the Post Office Research Station, Dollis Hill (below left).

They had the prototype, Colossus Mark 1, working in December 1943 and operational at Bletchley Park by February 1944. An improved Colossus Mark 2 was built in June 1944, just in time for the Normandy Landings. Ten of the massive (in physical size) computers were in use by the end of the war.

When Flowers proposed the machine to the "powers that be" there was considerable skepticism as it was thought that the one to two thousand thermionic valves that were needed to operate the machine could not work reliably as they had a reputation of failing quite often but he persisted with the idea and obtained support from the Director of the Research Station. He suggested that the main reason valves failed was because they were switched off and on regularly, he proposed that the Colossus be turned on and not turned off.

Colossus Mark 1 contained 1,500 valves while the Mark 2 had 2,400 and was both 5 times faster and simpler to operate than Mark 1. Later computers like the Manchester Mark 1 of 1949 used about 4,200 valves and the ENIAC (1946) used 17,468 valves. Colossus could process 5,000 characters per second whereas the average over the counter computer today processes 1.87 thousand million.

Colossus was the first of the electronic digital machines, however:

- it had no internally stored programs. To set it up for a new task, the operator had to set up plugs and switches to alter the wiring.
- Colossus was not a general-purpose machine, being designed for a specific cryptanalytic task involving counting and Boolean operations.

The notion of a computer as a general purpose machine, that is, as more than a calculator devoted to solving difficult but specific problems, did not become prominent for several years.

Construction of a fully functional replica of a Colossus Mark 2 was commenced in 1993 by a team led by Tony Sale of the British Computer Society. In spite of the blueprints and hardware being destroyed (for security reasons), a surprising amount of material survived, mainly in engineers' notebooks, but a considerable amount of it was in the U.S. The optical tape reader might have posed the biggest problem, but Dr. Arnold Lynch, its original designer, was able to redesign it to his own original specification.

In November 2007, to celebrate the project completion the National Museum of Computing put out a challenge to amateur radio blokes worldwide to see who could first decipher a message encrypted with the WWII German equipment (Lorenz SZ42).

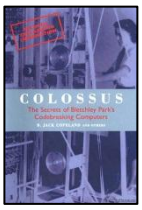
The Museum and the Amateurs had to receive and decode three messages transmitted from radio station DL0HNF in the German *Heinz Nixdorf MuseumsForum* computer museum.

The reconstructed Colossus computer in the UK.

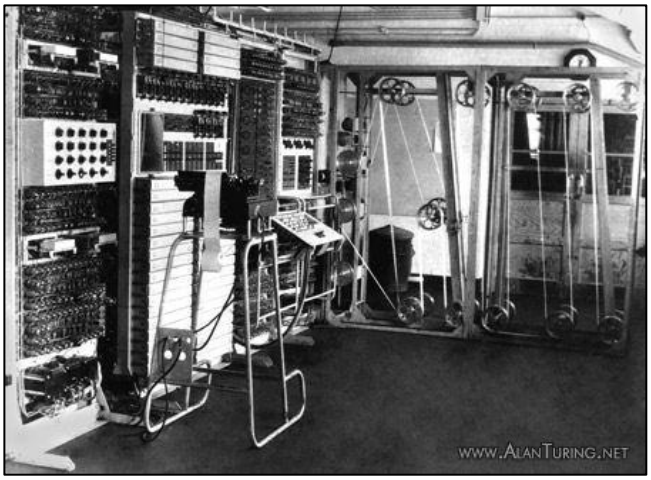
The challenge was easily won by a radio amateur using a 1.4GHz laptop who took less than a minute to break the code. By comparison, the Colossus had a clock speed of 5.8 MHz, remarkable for a computer built in 1944.

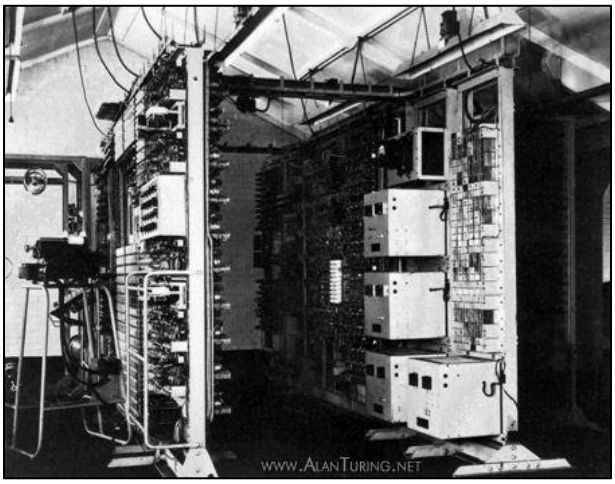
The Colossus team were hampered by their wish to use World War II radio equipment, delaying them a day because of poor reception conditions.

The reconstruction is now on display, in the historically correct place for Colossus No. 9, at The National Museum of Computing, in H Block Bletchley Park in Milton Keynes, Buckinghamshire.



(For those interested, there is an interesting book called Colossus: The Secrets of Bletchley Park's Codebreaking Computers which gives the full story of Colossus.)





The Eniac.

In 1946, two Americans, John Mauchly and John Presper Eckert developed the ENIAC computer, (**E**lectrical **N**umerical **I**ntegrator **A**nd **C**alculator). Their research was sponsored by the US military which needed a method of accurately and quickly calculating artillery firing tables.

The Ballistics Research Laboratory, or BRL, the branch of the military responsible for calculating the tables, heard about John Mauchly's research at the University of Pennsylvania's Moore School of Electrical Engineering. Mauchly had previously created several calculating machines, some with small electric motors inside. He had begun designing a better calculating machine that would use valves to speed up calculations.

It took Mauchly and Eckert about one year to design the ENIAC and 18 months and 500,000 tax dollars to build it. By that time, the war was over but the ENIAC was still put to work by the military doing calculations for the design of a hydrogen bomb, weather prediction, cosmic-ray studies, thermal ignition, random-number studies and wind-tunnel design.

What Was Inside The ENIAC?

The ENIAC contained 17,468 valves, 70,000 resistors, 10,000 capacitors, 1,500 relays, 6,000 manual switches and 5 million soldered joints (Ross Hilder – where are you??). It covered 1,800 square feet (167 square meters) of floor space, weighed 30 tons and drew 670 amps of electrical power. There was even a rumor that when turned on the ENIAC caused the city of Philadelphia to experience brownouts, however, this was first reported incorrectly by the Philadelphia Bulletin in 1946 and since then has become an urban myth.

In one second, the ENIAC (one thousand times faster than any other calculating machine in existence at that time) could perform 5,000 additions, 357 multiplications or 38 divisions. The use of vacuum tubes instead of switches and relays created the increase in speed, but it was not a quick machine to re-program. Programming changes would take the technicians weeks, and the machine always required long hours of maintenance, however, research on the ENIAC led to many improvements in the vacuum tube.

In 1946, Mauchly and Eckert started the Eckert-Mauchly Computer Corporation and in 1949 they launched the BINAC (BINary Automatic) computer that used magnetic tape to store data. They were bought out by the Remington Rand Corporation in 1950 which changed the name to the Univac Division of Remington Rand. Their research resulted in the UNIVAC (UNIVersal Automatic Computer), an important forerunner of today's computers.

In 1955, Remington Rand merged with the Sperry Corporation and formed Sperry-Rand. Eckert remained with the company as an executive and continued with the company as it later merged with the Burroughs Corporation to become Unisys.

At 11:45 p.m., October 2, 1955, with the power finally shut off, the ENIAC retired.

A hooker once told me she had a headache.