The battle to ‘break’ Enigma was not the only one being fought in 1942. Much of the high level traffic believed to be from Hitler and the High Command was being sent by teleprinter. The teleprinter signals being transmitted by the Germans, and enciphered using Lorenz, were first heard in 1940 by a group of police wireless operators on the South Coast who were listening out for possible German spy transmissions from inside the UK. Originally traffic interception was concentrated at the Foreign Office Y Station operated by the Metropolitan Police at Denmark Hill in Camberwell but, due to lack of resources at this time, 1941, it was given a low priority. A new Y Station, Ivy Farm Communications Centre Knockholt in Kent, was later constructed specifically to intercept Tunny traffic so that the messages could be efficiently recorded and sent to Bletchley Park. ‘FISH’ became the GC & CS’ generic code-name for the distinctive German radio signal that they had been intercepting on a regular basis since the outbreak of war, known by Y Station operators, used to listening to morse code transmissions, as "new music". Enigma decrypts had also revealed that the Germans called one of their wireless teleprinter transmission systems "Sägefisch" (sawfish), which led British cryptographers to refer to encrypted German teleprinter traffic as “Fish. It had been concluded that it was a non-morse radio teletype and there was a great concern that this could take over from Enigma, particularly as the volume of messages was steadily increasing. This would have been a disaster as the battle against Enigma was just beginning to be won.

Tunny" was the name given at Bletchley Park to the first non-Morse link, and it was subsequently used for the Lorenz SZ machines and the traffic enciphered by them. The Lorenz cipher machines were on-line attachments to the standard Lorenz teleprinters using Wireless telegraphy (WT) rather than land-line circuits for this traffic.

The German Army High Command had asked the C. Lorenz Company of Berlin to produce for them a high security teleprinter cipher machine to enable them to communicate by radio in complete secrecy. The Lorenz company designed a cipher machine based on the additive method for enciphering teleprinter messages invented in 1918 by Gilbert Vernam in America. SZ240 had 12 wheels as against the Enigma 4 wheels. Teleprinters are not based on the 26-letter alphabet and Morse code on which the Enigma depended. Instead teleprinters use the 32-symbol Baudot code where the code output consists of five channels each of which is a stream of bits which can be represented as no-hole or hole, 0 or 1, dot or cross.

The Baudot Code

The Vernam system enciphered the message text by adding to it, character by character, a set of obscuring characters thus producing the enciphered characters which were transmitted to the intended recipient. The simplicity of Vernam's system lay in the fact that the obscuring characters were added in a rather special way (known as modulo-2 addition).
Then exactly the same obscuring characters, added also by modulo-2 addition to the received enciphered characters, would cancel out the obscuring characters and leave the original message characters which could then be printed out. Vernam proposed that the obscuring characters should be completely random and pre-punched on to paper tape to be consumed character by character in synchrony with the input message characters. Such a cipher system (equivalent to a 'one-time pad system') using purely random obscuring characters is theoretically unbreakable.

The difficulty was how to ensure, in a hot war situation, that the same random character tapes were available at each end of a communications link and that they were both set to the same start position. The Lorenz Company decided that it would be operationally easier to construct a machine to generate the obscuring character sequence. Because it was a machine it could not generate a completely random sequence of characters. It generated what is known as a *pseudo-random* sequence. Unfortunately for the German Army it was more "pseudo" than random and that was the key that would lead to it being broken.

The amazing thing about the breaking of Lorenz is that the code breakers in Bletchley Park never saw an actual Lorenz machine until right at the end of the war but they had, by then, been breaking the Lorenz cipher for two and a half years.

Brigadier John Tiltman, one of the top codebreakers in Bletchley Park, took a particular interest in these enciphered teleprinter messages. Tiltman knew of the Vernam system and soon identified these messages as possibly being enciphered in the Vernam manner. Because the Vernam system depended on the addition of characters, Tiltman reasoned that if the operators made a mistake and used the same Lorenz machine starts for two messages (a *depth*), then by adding the two cipher texts together character by character, the obscuring character sequence would disappear. He would then be left with a sequence of characters each of which represented the addition of the two characters in the original German message texts. For two completely different messages it is virtually impossible to assign the correct characters to each message. Just small sections at the start could be derived but not complete messages.

As the number of intercepts, now being made at Knockholt in Kent increased, a number of Depths were intercepted but not much headway had been made into breaking the cipher until the Germans made one horrendous mistake. It was on 30 August 1941. A German operator had a long message of nearly 4,000 characters to be sent from one part of the German Army High command to another — probably Athens to Vienna. He correctly set up his Lorenz machine and then sent a twelve letter indicator, using the German names, to the operator at the receiving end. This operator then set his Lorenz machine and asked the operator at the sending end to start sending his message. After nearly 4,000 characters had
been keyed in at the sending end by hand, the operator at the receiving end sent back by radio the equivalent, in German, of "didn't get that - send it again". They then put their Lorenz machines back to the same start position. Although absolutely forbidden nevertheless they did it. The operator at the sending end then began to key in the message again, by hand. It was at this point that the codebreakers were given a gift of inestimable value. If he had used exactly the same key strokes as the first time which one would have expected from a German operator then all the interceptors would have got would have been two identical copies of the cipher text; the machines generating the same obscuring characters and the same cipher text. But, being only human and perhaps fed up with having to key it all again, the sending operator began to make slight differences to the second message compared to the first. It seems that the message began with that well known German phrase SPRUCHNUMMER (message number in English). The first time the operator keyed in S P R U C H N U M M E R. The second time he keyed in S P R U C H N R and then the rest of the message text. Now NR means the same as NUMMER, so what difference did that make? It meant that immediately following the N the two texts were different. But the machines were generating the same obscuring sequence, therefore the cipher texts were different from that point on.

Fortunately, the discriminators at Knockholt realised the potential importance of these two messages with the same twelve letter indicators. They were sent post-haste to John Tiltman at Bletchley Park. Tiltman applied the same additive technique to this pair as he had to previous ‘depths’. But this time he was able to get much further with working out the actual message texts because when he tried SPRUCHNUMMER at the start he immediately spotted that the second message was nearly identical to the first. Thus the combined errors of having the machines back to the same start position and the text being re-keyed with just slight differences enabled Tiltman to recover completely both texts. The second one was about 500 characters shorter than the first where the German operator had been saving his fingers. This fact also allowed Tiltman to assign the correct message to its original cipher text.

Tiltman started to add together, character by character, the corresponding cipher and message texts, revealing for the first time a long stretch of the obscuring character sequence being generated by this German cipher machine. He did not know how the machine did it, but he knew that this was what it was generating! This was to lead to one of the greatest feats of cryptography in WWII.

After three months of the Research Section failing to diagnose the machine from the almost 4,000 characters of key, John Tiltman then gave this long stretch of obscuring characters to a young chemistry and mathematics graduate, Bill Tutte, who had recently come to Bletchley Park from Cambridge. Originally rejected in interview by Alan Turing for a the message-codebreaking team. He was recruited in May 1941 by Tiltman for the Research Section, which actually turned out to be the best choice. He applied a technique that he had been taught in his cryptographic training, of writing out the key by hand and looking for repeats. Remember, this was before computers so he had to write out vast sequences by hand Tutte did this with the original teleprinter 5-bit Baudot codes, which led him to his initial breakthrough of recognizing a 41 character repeat. Over the following two months up to January 1942, Tutte and colleagues worked out the complete logical structure of the cipher machine. This remarkable piece of reverse engineering was later described as "one of the greatest intellectual feats of World War II", when it was finally given the recognition and publicity it deserved. After this cracking of Tunny, a special team of code breakers was set
up under Major Ralph Tester, most of them initially transferred from Alan Turing’s Hut 8.
The team became known as the ‘Testery’.
The Testery was a section of GC & CS was concentrating on this problem, initially only using hand decrypting methods in their efforts to break it. One of two sections named after their Chiefs, the other being the Newmanry, it was set up in July 1942 under Major Ralph Tester who was a linguist and departmental head, not a codebreaker. The three original founding members, who were cryptographers, and linguists – were, Captains Jerry Roberts and Peter Ericsson and Major Denis Oswald. All four were fluent in German. They and several others were members of the Intelligence Corps:-
Peter Benenson codebreaker - WO I
John Christie codebreaker - Lieutenant.
Peter Ericsson shift-leader, - linguist and senior codebreaker - Captain.
Roy Jenkins codebreaker (3 months later moved on to wheel setter) - Captain.
Denis Oswald linguist and senior codebreaker - Major.
Raymond Clarke (Jerry) Roberts shift-leader, linguist and senior codebreaker - Captain.
The Germans were convinced that the Tunny cipher system was unbreakable and so Tunny was the cipher system which carried only the highest grade of intelligence messages from the German Army Headquarters in Berlin to the top generals and field marshals on all fronts. Some were signed by Hitler himself. Tens of thousands of Tunny messages were intercepted by the British and broken at Bletchley Park by Captain Roberts and his fellow codebreakers in the Testery. These messages contained much vital insight into top-level German thinking and planning. This all came about due to this simple but devastating operator error.
The Testery had been breaking Tunny by hand for a year before the 'Newmanry' under Max Newman became active from July 1943. Mathematicians in the Newmanry used machine methods to speed up breaking Tunny. Early on, a machine called “(Heath) Robinson” was produced, to help speed up one stage, the breaking of the chi wheels, but the Robinson was slow and not reliable. Fortunately, in February 1944 a new machine called ‘Colossus’ became operational and it is now accepted as being the world’s first electronic computer. Colossus was designed and built in only ten months by Tommy Flowers of the G.P.O. working at the Post Office Research Station at Dollis Hill. It had far greater capacity and speed than the Robinson and so the whole breaking process became much faster. The Colossus was essential for making the very fast counts needed to work out the “de-chis”, but the psi-wheels and motor-wheels were still broken by hand in the Testery. With the help of the Newmanry, the Testery broke up to 90% of the traffic given to them to work on in the Colossus period.
The information provided by Tunny enabled the Allies to ascertain German movements, saving thousands of lives at critical junctures such as D-Day and the battle of Kursk in the Soviet Union. General Dwight D Eisenhower gave the best summary when he said that "Bletchley decrypts shortened the War by at least two years" and Tunny played a very important role in all of this - a war which was costing at least 10 million lives a year. A great deal of this was down to Bill Tutte but ably supported and developed by the work of Tester and his band of Intelligence Corps officers and NCO’s. By the end of the war in Europe in May 1945, the Testery had grown to nine cryptographers, a team of 24 ATS, and a total staff of 118, organised in three shifts, working round the clock.
The story of Enigma (declassified in the 1970s leading to the publication of Winterbotham’s book) is well known, but the story of Tunny, Germany's top-secret cipher machine, was only declassified a few years ago. There is no evidence - in fact it is almost certain - that
Winterbothan had any idea of what had been going on! Around 15 Tunny machines were built; though not as technically significant as Colossus nevertheless it was a remarkable achievement.

Many of the cryptographers in the Testery died before they could tell their stories. Roy (Lord) Jenkins went on to enter Parliament in 1948. He was Home secretary 1965-7 and 1974-75 and Chancellor of the exchequer 1967-70 in various Labour administrations. He was President of the European Commission 1976-81 and a founder member of the Social Democratic Party in 1981 and became Chancellor of the University of Oxford in 1987. Peter Benenson went on to practice law as a Barrister and was one of a group of lawyers who founded ‘Justice’. At a meeting in London in 1961 he and six others founded ‘Amnesty International’. After leaving Bletchley, Peter Edgerley was a member of the War Crimes investigation unit. Thereafter he pursued a career in marketing.

And what about Tester? Before the war he had been an accountant with Unilever. After the war he quietly went back to Unilever and his old job. No one there knew the immensity of his contribution to the defeat of Germany.

Despite the fact that nearly 900 members of the Corps are listed on the Roll of Honour as having worked at B.P nowhere there or in our Museum there is there any mention of this and the many other contributions made by the Intelligence Corps. Is it not time to do something to correct this?

Paul Croxson Sept 2012