Speaker: Brigadier General John Tiltman

The TUNNY machine and its solution

The cipher machine I am going to talk about is the SZ40. That is, Schluesselzusatzgeraet 1940, developed by the Germans for transmitting over the air messages converted to teleprinter form. We gave the name TUNNY to the machine early in 1942. Early transmissions which passed between Vienna and Athens shortly after the invasion of Russia in the summer of 1941. The transmissions were frequently of very great length. I remember one of about 16,000 consecutive symbols of cipher. Each transmission began with a set of 12 personal names – Anton, Bertha, etc., clearly a 12-letter indicator. The plaintext proved to be a report for the personal information of the German military attaché in Athens on the situation on the Russian front for the 29th of August 1941 starting at Odessa and finishing somewhere in Finland. In both plaintext versions, there were many places where the sending operator had struck a wrong key or made some other mistake necessitating long stretches of corrections and repetitions. This was the cause of the offsetting of the plaintext in the two versions culminating in the enormous offset of about 500 letters at the end. As far as I can discover, the machine could never have been solved if we had not been presented with the isolog depth of the 30th of August 1941.