How the Allies broke the German Diplomatic cipher Floradora.

During World War 2, the Germans believed their two major diplomatic cryptographic systems were impregnable. Both were based on a dictionary-like code book that employed 57,000 5-figure groups to represent words, phrases, numbers, dates and letters. The primary purpose of the code was to abbreviate messages rather than to hide their meaning. Secrecy was gained by superencipherment – that is by adding other groups of figures to the code. There were two systems: one was called Floradora and the other was a One-Time Pad. In the event the Allies broke both systems after a colourful saga of daring, luck, hard work and fruitful cooperation.

In the Floradora system, the enciphering clerk first turned the message into a series of 5-digit groups using the code book. Then he added to each group two 5-digit numbers drawn from a secret additive book, which had 10,000 rows with six 5-digit groups in each row. The resultant sums made up the ciphertext. Here is an example.

message:	attack	Gibralter	at	sunset.
code:	23091	30994	16431	73298
additive 1:	43219	76420	21754	96371
additive 2:	17382	12388	35339	34562
sum:	83692	19802	73524	04231

ciphertext: 83692 19802 73524 04231.

Selection of the additives was a crucial part of the system. For each message, the clerk had to choose two rows from the 10,000 rows in the additive book. He denoted the row numbers to the recipient after enciphering them with a special system. Here is how it worked. First of all he chose at random two bigrams from a secret book of 100 different bigrams. Each bigram comprised a consonant and a vowel and each was associated with a 2-digit number. Thus he might choose AB and FA giving him, for example, 09 24. He then reversed the letters to get two new bigrams, AF and BA in this case, for which the associated digits may be 73 and 59. He formed two 4-digit numbers, 0924 and 7359, to which he then added the key for the day and a constant. In this way he got two new 4-digit numbers, like this:

Numbers from digraphs:	0924	7359
key for the day:	9135	2568
unchanging constant:	5000	5000
sum:	5039	4927

Now he uses row 5039 for additive 1 and row 4927 for additive 2 (together with following rows as necessary for a long message). He puts the indicator ABFA AFBA at the beginning of the ciphertext and then sends the enciphered message by radio.

The recipient reverses the process, first using the indicator to find the row numbers for the additives and then recovering the code by subtraction and finally finding the plaintext from the code book. The purpose of the palindromic indicator was to help in garbled transmission and this feature led the British to name the cipher ‘Floradora’.

The Germans updated their code book during the war and changed the bigram book every 3 months and the key for the day every two days. Changes were sometimes conveyed by diplomatic pouch, in an effort to

keep them secure, but at other times were encrypted and transmitted by Morse code.

To break a Floradora message, four items were needed: the code book, the secret books of additive keys and of bigrams, and the key of the day. Of course the operating system of the cipher also needed to be understood but this was described to the British early on by a French agent who had seen a decipherment being carried out.

The code book proved the easiest to obtain. Some of it had been worked out by the Government Code and Cypher School (GC&CS, the British codebreaking unit) before the war from messages that had been sent without superencipherment. Then in May 1940 a British raiding party on Reykjavik, Iceland, arrived at the German Consulate just as they were burning their secret papers. The raiders managed to save most of the German code book from the flames and so extended knowledge further. The raid also yielded 10 lines out of 5,000 from the additive book (the first 5,000 rows were repeated as reciprocals to make another 5,000 lines).

Later in 1940 GC&CS obtained a copy of the complete code book from a mysterious source described as 'the Dutch east'. The US authorities got their hands on the second edition of the code book at the end of 1940, as well as some other cipher materials. This happened when a clandestine German courier, transiting the Panama canal in a Japanese steamer, got nervous and threw his cipher materials overboard in an unsuccessful attempt to avoid discovery.

The bigram table was in the hands of the US Army's Secret Intelligence Service (SIS) by the end of 1940, together with some of the daily keys for 1941, (presumably having also been fished out of the Panama canal).

As early as 1940 GC&CS at Bletchley Park and the SIS at Arlington Hall, Va, began sharing information. In February 1941 Capt. Abraham Sinkov arrived in England from the US with several crates of cipher machines and materials, including the Floradora materials taken in the Panama incident.

With just a few rows of additive available, the likelihood of solving Floradora was very low. But there was enough for the British and Americans to begin a very slow and painstaking extension of the additive book, which would take two years to complete. By using lines of known additive, known daily keys and guessed cribs, parts of some of the German messages could be deciphered. This led to teasing out the rest of the messages and consequent discovery of further lines of additive. In the SIS Frank Lewis (R.MASTERTON) was one of the cryptanalysts who worked on Floradora (or 'Keyword' as it was called in the US).

Then in 1942, out of the blue, a German sailor delivered the daily keys for the next three months to the British Consulate in Mozambique, mistaking it for the German Consulate! The local MI6 agent sent the keys to GC&CS and this led to a blossoming of Floradora solutions and extensions to the additive book.

By the end of 1942 the Allies on both sides of the Atlantic were reading one-quarter of Floradora messages. A partition of work was agreed in which the SIS focussed on Tokyo traffic and GC&CS on Dublin and Berlin. By mid-1943 the complete additive book was recovered and all Floradora messages were being read currently.

When the Allies invaded Normandy in June 1944 the general cipher traffic was so heavy that only those Floradora messages of immediate use were fully deciphered and this was done within a day of receipt. Not only was this cipher freely read by the end of the war but also the other ‘impregnable’ German Diplomatic cipher, the one-time pad. But that is another story.