Harold Berman

Bletchley Park1944. US Army in Military Section. Harold Berman originally wrote this memoir for his youngest grandchildren. Joshua and Deborah.

From January 1943 to October 1944 I served in the US Army Signal Corps in England (chiefly London) as a cryptanalyst, deciphering German messages sent in code by radio and intercepted by English and American intelligence. Prior to the invasion of Normandy in June 1944 these were largely practice messages, since the only operations were the organization of defenses; nevertheless, through the decoding of such messages much could be learned about troop sizes and whereabouts and officer personnel.

Then came D-Day. I was at British intelligence headquarters in Bletchley, where I had been sent to work with British cryptanalysts on a new cipher system the Germans had introduced and were just beginning to use. From early morning of June 6, 1944, the sky was filled with fleets of aircraft going east - there were thousands of them, all day long. I was sent back immediately to London to work on what were now operational messages, which were coming in under the older system of encipherment — but now with a difference.

In the older system the plaintext - that is, the original German message - was written out in double lines, one under the other, like this

A L L E S H A T E I N E N D E N U

R D I E W I U R S T H A T Z W E I X

which translated means, 'Everything has an end but a sausage has two' (German practice messages were like that - lots of sayings, proverbs, verses, little jokes.)

When it came to enciphering the message, the German cryptographer would transform the text into what we called 'bigrams', that is he would take the first letter from the top line (A) and put it with the letter under it (R), making the bigram AR, and he would encipher that bigram, and then he would do the same

with the next letter of each line (LD), and the next (LI), and so on. If the encipherment of AR were, let's say, BR and the encipherment of LD were MC, and the encipherment of the next bigram LI were YF, and so on, then the message that our radio people intercepted would read BRMCYF and so on.

Of course all this was top top secret, but an English genius figured out what they were doing. They were getting the cipher letters from two boxes of alphabets, five horizontal letters and five vertical letters in each box, making 25 letters (the J was omitted), like this:

QMKRP WECSQ
ANOBS MBDIH
CFLDX OKATU
EGIZU ZRNGF
HTWYV YXPLV

To decipher the bigram BR one must take the B in the second box and draw a diagonal line from it to the R in the first box, go down to the B in the first box and up to the E in the second box, so you would get BE. BUT THEN THE GERMANS DID A VERY TRICKY THING. THEY ENCIPHERED THE BE IN THE SAME WAY, GETTING AR. IT WAS A DOUBLE ENCIPHERMENT. And so MC, by the same process, would get you A in the first box and O in the second box, and then the re-decipherment of AO would get you the LD that you wanted.

Now I had had a year and a half of doing this, and 1 had become quite good at reconstructing the boxes - which is what you had to do to solve new messages within the thirty-six hours that was the limit of time within which the messages had to he deciphered if the decipherment was to do any good (This was called 'medium-grade traffic' – 'top grade' was supposed to be undecipherable ever, but in fact it was machine traffic and it was broken by machine - the original computers. 'Low-grade traffic' was for field operations and had six- or eight-hour security.) By the way, the Germans were supposed to change the boxes every three hours.

So here we were in the crucial weeks after D-Day and eventually General Patton's tanks were able to break through the German lines and - lo and behold! - suddenly we were unable to break the German messages we were getting. When we did break some, because we could guess what they were saying (sometimes they were repeated in

plaintext, and sometimes we could tell by the patterns of bigrams what they were saying) - we still could not reconstruct the boxes in order to break the others. They were doing something different!

The second day of this, I sat up with messages all day and all night and most of the next day - something like 30 hours --- struggling with the decipherment From long experience I could guess what some of them were saying· 'An alle Einheiten', - 'to all units', or to a particular unit, and with signatures, and referring to supplies, etc. And so I could get some bigrams and begin to construct a text. But the phrases would not begin to give me the two boxes and the double encipherment.

So Colonel Neff came around and saw I was pretty exhausted and told me to go home - back to the barracks (a four-story house near Hyde Park!) So I went - and as I was walking down the street, (I remember it well, though its name has slipped my mind) suddenly, suddenly, suddenly it struck me! I rushed back and told the colonel - it's obvious, what they are doing! They're in a hurry and they're just doing a single encipherment, and that's why we can't reconstruct the boxes! And the message I had been struggling to decipher - I went back to it: it was 'To all units, dump your fuel at banana.'

And that's how General Patton got the gasoline he needed to get his tanks through Normandy and France! Our people knew where banana' was, and Patton went there and got the fuel! And that's why I was given a Bronze Star Medal,