The American Army Bombe

Dermot Turing
Visiting Fellow, Kellogg College
60-62 Banbury Road
Oxford, OX2 6PN
dermotturing@btinternet.com

Abstract

This paper presents the U.S. Army's version of the anti-Enigma cryptanalytical bombe machine, which has not previously received attention in the literature on Enigma. Its unique features and applications are discussed, and the paper describes the sensitive context of the machine's development and deployment.

1 Introduction

In 1941, many months before the attack on Pearl Harbor, a courageous act took place in which the United States and the United Kingdom agreed to share their achievements in the sphere of cryptanalysis. Two years later this tentative, awkward and unstable agreement was nearly rescinded. The cause of the near-rift was the desire of the British to inspect certain cryptanalytical and cryptographic devices being developed for the U.S. Army at Bell Labs. The cryptanalytical devices in question included the U.S. Army bombe.

While the literature covers each of the Polish bomba (Link, 2009; McCarthy, 2019), the British 'Turing-Welchman' bombe (Davies, 1999; Carter, 2010) and the U.S. Navy's 'Desch' bombe (Erskine et al., 2002; DeBrosse and Burke, 2004), the U.S. Army bombe has largely been ignored. The fact that this branch of the bombe family has been overlooked is perhaps remarkable, given its innovative features: its significance may go far beyond a mid-war spat between intelligence services about who could see what. The purpose of this paper is to begin to fill the gap with a description of the U.S. Army bombe and to open a discussion on the role of this interesting piece of equipment.

The reader is assumed to be familiar with the standard Wehrmacht version of the Enigma cipher machine. As to bombes, their object was to identify the secret 'key' or set-up of the Enigma machine. In very brief summary, the British bombe tested all 26×26×26 possible positions of three chosen coding rotors to determine if a single starting-position of the rotors could consistently transform a segment of guessed-at plaintext (called a 'crib') into an observed, intercepted message. Additionally, the machine identified one possible pairing of letters effected on the Enigma machine's plugboard. When a logically consistent rotor orientation arose, the bombe machine would stop, allowing the operator to identify that orientation and the single plugboard pairing.

By the time of the historic visit of four Americans to Bletchley Park in January 1941, the bombe was already making a contribution to the solution of Enigma messages and thereby to the wartime intelligence picture. One outcome of the American visit was that the British would – albeit with some reluctance and delays – share the particulars of their bombe-based attack with the Americans. (Sherman, 2016)

2 The American Army Solution

Much has been written about the development by the US Navy of a four-rotor bombe at the National Cash Register Corporation in Dayton, Ohio under Joe Desch. However, that was not the only American response to the challenge of Enigma. Within two weeks of the launch of the Desch project, William F. Friedman, then the U.S. Army's principal cryptanalyst, put forward

his own argument for autonomous American cryptanalytic machinery for deployment against Enigma. Relying on the British could be unwise: the three-rotor bombes would be of no use if the German forces rolled out four-rotor Enigma modifications to their land and air forces; and 'should a few well-placed bombs destroy the present three buildings in which the Enigma-solving machinery is housed, all Enigma solution will stop…. Consequently, it appears vital that we take immediate steps to establish an Enigma solution unit of our own.'[1]

To implement the new plan, the U.S. Army turned to Bell Telephone Laboratories.[2] Bell Labs was the research offshoot of the American Telephone and Telegraph corporation, which contributed many technological breakthroughs in the mid-twentieth century (Gertner, 2012). Among the galaxy of intellectual stars in the Bell Labs sky were George Stibitz and Claude Shannon. In 1937, Stibitz had created a digital adding machine, stimulating the development of digital computing at Bell Labs. In the same year, Shannon had discovered that Boolean algebra and electrical circuitry shared features which enabled mathematical and logical functions to be represented in physical form through switching. It seems, though, that the idea of using electrical switching for the U.S. Army bombe originated with Lt Leo Rosen of Friedman's team, which led to Bell Labs being chosen for the Army's project.

2.1 The technology

The U.S. Army concept for a bombe was to omit the rotating parts of the British and Desch bombes, which wore out, needed specialist engineering, and were limiting components in that physical movement takes time and therefore slows the operation of the machine. Instead, the army bombe would rely on relays and switching. Relays are simple electromechanical instruments, which rely on electric current to generate a magnetic field which pulls into place an electrical contact, thus switching the path of a current in a new direction.

The U.S. Army bombe used relay technology to replace rotating drums by switching. 'M' units, also called 'Multiple Paths', to direct electricity into fixed-wire circuitry imitating the internal wiring of Enigma rotors in a progressive fashion, so that each entry-connection on a 'rotor' would be connected in succession, with suitable switching to copy the stepping pattern of the 'middle' and 'slow' rotors of an Enigma machine.

To bring about this progression, the continuous supply of voltage of traditional bombes was replaced by pulses of electricity. Each pulse not only coursed through the circuitry to carry out the logic test designed by Alan Turing for the British bombes, but operated on the relays in the M units so as to change the electrical path to be followed by the succeeding pulse.

Replacing the rotating drums of the British bombe with circuitry required a new method for set-up of the cryptanalytic machinery. Running a 'menu' – the logic diagram resulting from comparing crib and intercept – requires a number of three-rotor devices each imitating the behaviour of the moving parts of an Enigma machine, each of which compares an actual transformation of a letter from plaintext to ciphertext as observed in the intercepted message. (A plaintext-ciphertext letter pair is referred to as a 'constatation'.) As different constatations came from different parts of the intercept, the Enigma analogues needed to be moved on an appropriate number of steps to reflect the progression of Enigma rotors as the message was enciphered. This would be done on a traditional bombe by moving the drums round; on the U.S. Army bombe, by advancing the progression of switching on the M units.

As explained by Alan Turing in his technical report, written after an inspection of a single M unit and Enigma emulator on 5 February 1943, the progression was essentially a 'Vigenère slide' achieved by electrical arithmetic in base 3. Three pairs of relays were connected in series, and the connection point to the Enigma emulator achieved by the additive effect of the relays, as illustrated in Box 1. 'If any particular total slide is required it is possible to choose certain of the six relays to energise so that this total will be obtained.'[3] This was done in a 'control turret'

1 Friedman to Bullock, 14 September 1942. NARA RG 457, HMS Entry A1-9032, Box 1283, Nr 3815.

2 Special Research History No 361 'History of the Signal Security Agency, Volume Two, The General Cryptanalytic Problems', page 257. NARA RG 457, HMS Entry A1-9002, Box 96.

3 Turing report, 11 February 1943. TNA HW 62/5.

from which other aspects of menu set-up were done, such as the patching-together of the Enigma analogues testing the different constatations. Choice of rotors was also made from a control panel, rather than physically selecting drums.

Relay	Neither closed	One closed	Both closed
A , A′	0	1	2
B , B′	0	3	6
C , C′	0	9	18

Box 1: Relays which are in the 'on' position contribute units, threes, or nines in base-3 arithmetic. Combining the results identifies the input contact to an Enigma emulator. With appropriate choice of closures, each value from 0 to 25 can be obtained.

Another innovation was to do with 'stops'. British and Desch bombes were designed to stop when the machine detected a rotor start-position and plugboard cross-wiring consistent with the plaintext having been transformed into the observed intercept. A typical bombe-run would yield several 'stops', each of which had to be checked. The U.S. Army machine dealt with stops by not stopping, but recording the result.[4]

All of this required a vast amount of switching equipment and plenty of space. A demonstration version consisting of a single M unit was 3m high, 2m wide and 50cm deep; the finished machine had 72 of these, together with all the associated rotor-emulator racks, patch panels and so forth. The capacity of the U.S. Army bombe was equivalent to four British bombes, but it occupied four times the space (see Figure 1).

There were compensating advantages. The machine was fast (7 minutes for a run, compared with around 12 for a British bombe); the components were nothing more than standard telephone equipment, which aided both maintenance and secrecy in manufacture; omitting heavy moving parts eliminated mechanical stress and saved on wear and tear; fewer operators were needed; rotor changeover took 30 seconds as compared to 10 minutes for a rotary bombe, and the U.S. Army machine, being digital, was more accurate.[5]

2.2 Flexibility and future-proofing

The relay-based approach was highly flexible and future-proof. Given that the German navy had already devised a way to squeeze a fourth rotor into its Enigma machines, it was likely that further modifications would arise if the German forces continued to rely on Enigma. Indeed, towards the end of the war, new components such as a settable reflector (*Umkehrwalze D*), a hand-turned attachment to the plugboard to rotate its cross-wirings (the *Uhr*) and rotors with adjustable stepping notches (*Lückenfüllerwalzen*) were all proposed or rolled out at some stage. Even abandonment of Enigma might be possible, in which case some new encryption device might come into being. The British or Desch bombes would be more-or-less useless against such developments.

By using readily available components and relying on circuit design rather than hardware for its problem-solving logic, the U.S. Army bombe was highly adaptable. Over the course of 1943-44 a range of peripherals were developed to tackle specific Enigma problems:[6]

- Machine-gun (October 1943). This attachment automated the checking process for stops. 'Checking' meant testing the cross-plugging implied for each constatation in the menu to identify inconsistencies: if letter P was supposed to be cross-plugged to T it could not also be cross-plugged to K, so if checking led to that result, it would be a 'false stop'.
- Double-input (October 1943). This adaptation allowed the machine to test two menus simultaneously.
- Dud-buster (October 1944). A 'dud' was a message where the message setting (orientation of rotors at the start of encipherment) was not known, but all other aspects of the Enigma set-up (rotor choice and order, plugboard and ring-settings) were. The dud-buster found the

4 Stevens report of Bell Labs visit, 3 February 1942. NARA RG 457, HMS Entry A1-9032, Box 1283, Nr 3815.

5 Stevens report; Friedman to Corderman, 29 March 1944. NARA RG 457, HMS Entry A1-9032, Box 950, Nr 2809.

6 SRH 361, pages 265-267.

missing setting. Many of the most valuable applications of dud-busting were naval, but it does not appear that the U.S. Navy had a machine solution to duds; the record is obscure as to whether naval problems were among those solved on the Army's equipment.

- Autoscritcher (by December 1944). This device was invented to counter the settable reflector, by identifying its wiring pattern in force for the time being. A functionally equivalent device built in Britain, called the Giant, linked four rotary bombes together. The U.S. Navy also built a machine called the Duenna for the same purpose.

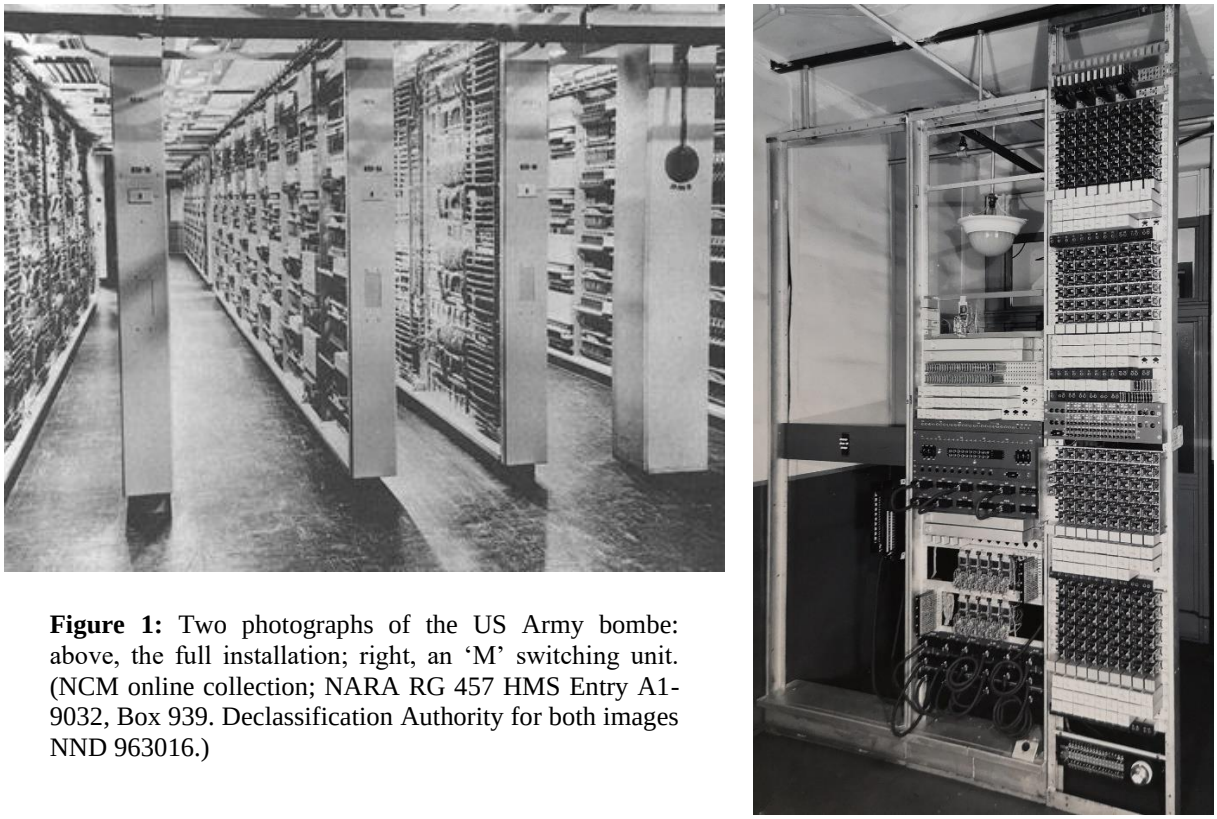

Figure 1: Two photographs of the US Army bombe: above, the full installation; right, an 'M' switching unit. (NCM online collection; NARA RG 457 HMS Entry A1-9032, Box 939. Declassification Authority for both images NND 963016.)

All these developments showed the versatility of a machine to which plug-on additions could be attached simply without the need for re-engineering. But, perhaps more importantly, the machine showed the way forward for future cryptanalytical problems as yet unforeseen. As William F. Friedman mentioned to Alan Turing on the occasion of the latter's visit to Bell Labs, 'the machine is intended to be "a general cryptographic machine".'[7] Indeed so: Friedman noted just after the end of the war that it would be useful if 56 of the 144 frames of the bombe machinery were redeployed to test the security of the US Army's own encryption systems, 'since it will facilitate certain investigations of a general nature in connection with rotor cryptographic machines.'[8]

3 The Secrecy issue in 1943

Despite the cooperation between Britain and the United States on cryptographic matters during World War II, in its early stages there was official resistance at the highest level in the U.S. Army to the British being allowed to see what they were building. Given that the British had invented the concept of the rotary bombe, it was going to be hard for the British to understand

7 Turing report.

8 Friedman to Hayes, 6 July 1945. NARA RG 457, HMS Entry A1-9032, Box 1283, Nr 3815.

why they (and the rotary bombe's chief logical designer, Alan Turing) should not take a look at the U.S. Army's bombe project.

It was not easy for the British authorities to work out what the Americans were concerned about in 1942. The British thought they had given full details of their Bombe technology, but because the details did not include 'blueprints', in July 1942 the Americans accused the British of holding back on them, notwithstanding 'assurances that it was not intended to build bombes'. (A separate agreement covered the American plan to build four-rotor naval Enigma bombes.) It was against this backdrop that Alan Turing was sent to America to work with Desch and to 'advise on the security of a U.S. speech scrambling device made by Bell Laboratories.' Friedman thought he had obtained approval on behalf of the U.S. Army's Signals Security Service for Turing to have access to Bell Labs.

However, U.S. Army Staff demurred. Various problems were mentioned to the UK's own chief cryptographer, John Tiltman, but these were unconvincing, and raised British suspicions. 'This thoroughly bad impression was reinforced a hundredfold by Colonel Tiltman's report that the War Department had without our knowledge or consent begun… building a bombe machine at the Bell Laboratories.' [9]

Matters did not end there. Turing's clearance to visit Bell Labs apparently did not extend to the speech encryption device, now known by the name SIGSALY and then under code reference X61753. The British were informed that the device was 'considered too secret to allow Dr. Turing to look in on it'. [10] Friedman was too junior – despite being the top military code-breaker – and Turing's visit should have been cleared at a much higher level. The British were told that the objection came from the very top, namely General George C. Marshall, the US Chief of Staff.

To deny Turing access to the speech encipherment machine did not appear logical. After all, the speech machine was in part a response to insecurity of the transatlantic radio-telephone link, which was used not just to keep the Chiefs of Staff connected to their commanders in the European Theatre of Operations but to allow political liaison between President Franklin D. Roosevelt and Prime Minister Winston Churchill. If Churchill was going to use it then the British were going to see it sooner or later. Perhaps the secrecy of X61753 was a specious reason for excluding Turing from Bell Labs. In any case, Bell Labs was a huge building, and to keep him away from one project while he looked at another would have been perfectly feasible. Perhaps something more was afoot, perhaps something reflecting embarrassment about the American change of policy on building their own non-naval bombes.

Now that the U.S. Army bombe documentation has been largely declassified, it is possible to put forward a more convincing reason for the desire to keep the British away in 1943. The possibilities suggested by digitising the logic of the bombe – and in particular the power and versatility of the new approach, and how they might be exploited and even turned against the United States itself in the wrong hands – may have been a secret far more important than X61753/SIGSALY or any short-term operational considerations relating to Enigma intelligence.

In the early months of 1943 the British were still, just, the dominant partner in the trans-Atlantic intelligence relationship. A single hint that the British would simply cut out the Americans if Turing's access was not granted was followed within two days by a removal of the obstacles. On 4 January, formal permission to inspect project X68003 – the Army bombe – was granted to Tiltman and Turing once again.[11] Turing was admitted to Bell Labs two weeks later to see the speech machinery, and at last, on 5 February 1943, to see the Army bombe. Once the ruffled feathers between the two allies had been smoothed over, a cooperative arrangement was worked out between Bletchley and Arlington Hall (where two finished Army bombes were installed) whereby specific problems, well-suited to the versatility of the X68003 equipment, were agreed for the U.S. Army's machine cryptanalysis team. Indeed, eventually the team's tasks seem to have been largely directed from Bletchley Park.[12]

9 Briefing for Travis (undated, April 1943). TNA HW 50/13
10 Dill to Marshall, 2.12.42. TNA HW CAB 122/14.

11 Memorandum by Bullock, 4 January 1943. NARA RG 457, HMS Entry A1-9032, Box 1283, Nr 3815.
12 SRH 361, page 269.

4 Digital cryptanalysis

The American army bombe represents a step forward in the mechanisation of cryptanalysis. Its development marks a change in thinking, from seeing large key-space cryptanalytical problems thrown up by the invention of cipher machines as case-by-case challenges, each demanding a bespoke mechanical response, towards a more universal, digital, computerised approach. Cryptanalysis was part of the business case for the United Kingdom's post-war computer project called ACE, which mentioned cryptically that 'the promised support of Commander Sir Edward Travis [by then the head of GCHQ], of the Foreign Office, will be invaluable.'[13]

In retrospect, it seems likely that the American fears about the innovative aspects of their army bombe becoming shared intellectual property were well-founded. The evolutionary pathway from wartime cryptanalytical devices to postwar programmable computing machines is well known (Corera, 2015). Electronics added speed, but the real breakthrough in this era was the ability to conceptualise machine-solvable problems in digital terms. While one can argue that the British bombe was digital – in the sense that its output was a binary presence or absence of voltage in a single wire of a 26-wire cable, the precondition for a 'stop' – it is probably more accurate to see the British bombe as a pre-computing-era hybrid between single-purpose analogue devices and digital data-processing machinery such as Hollerith punched-card sorters. The Desch bombe did not break from that tradition, whereas the U.S. Army bombe depended on binary processing of electrical pulses for its entire logical operation. Furthermore, the army bombe was to a degree programmable for new tasks, albeit not a 'stored-program computer' of the post-war era.

The use of electrical pulses and logical path moderation through relay switching shifted the focus of thought towards logic and programming and away from engineering: the design features of the U.S. Army bombe implied a new direction for computing. These lessons were not lost on Alan Turing, who appears to have spent the years after his Bell Labs visit in developing his own thoughts about computing machinery, culminating in his 1945 design proposal for the ACE.

13 Womersley to Darwin, undated memo entitled 'ACE Machine Project'. alanturing.net/turing_archive/archive/index/aceindex.html documents, accessed January 2021.

Acknowledgments

The author gratefully acknowledges assistance and materials from John Harper, Michael Barbakoff, Philip Marks and Rob Simpson in with the research for this article.

References

Frank Carter. 2008. *The Turing Bombe*. Report No.4, Bletchley Park Trust, Milton Keynes, UK.

Gordon Corera. 2015. *Intercept*. Weidenfeld and Nicolson, London, UK.

Donald Davies. 1999. *The Bombe – a Remarkable Logic Machine*. Cryptologia, 23(2):108-138.

Jim DeBrosse and Colin Burke. 2004. *The Secret in Building 26*. Random House, New York, NY, USA.

Ralph Erskine, Philip Marks and Frode Weierud. 2002. *Review of US Bombes*. IEEE Annals of the History of Computing, 24(3):85-87.

Jon Gertner. 2012. *The Idea Factory*. Penguin Books, New York, NY, USA.

David Link. 2009. *Resurrecting Bomba Krypto-logiczna*. Cryptologia, 33(2):166-182.

Jeremy McCarthy. 2019. *The Enigma of the Polish Bomba*. ITNOW, 61(3):26–27.

David J. Sherman. 2016. *The First Americans. The 1941 US Codebreaking Mission to Bletchley Park*. United States Cryptologic History, vol.12. National Security Agency/Center for Cryptologic History, Fort George G. Meade, MD, USA.