THE BLETCHLEY PARK CODEBREAKERS
IN THEIR OWN WORDS

JOEL GREENBERG

Introduction by TONY COMER
‘A fascinating anthology . . . Joel Greenberg’s selection of letters from those who served at Bletchley Park provides a new perspective on what they achieved.’

Tony Comer OBE
Former Departmental Historian at GCHQ
THE BLETCHLEY PARK CODEBREAKERS IN THEIR OWN WORDS

JOEL GREENBERG
The Bletchley Park Codebreakers

First published in 2022 by
Greenhill Books,
c/o Pen & Sword Books Ltd,
47 Church Street, Barnsley,
S. Yorkshire, S70 2AS

www.greenhillbooks.com
contact@greenhillbooks.com


All rights reserved.

© Joel Greenberg, 2022

The right of Joel Greenberg to be identified
as author of this work has been asserted
in accordance with Section 77 of the Copyrights,

CIP data records for this title are available from the British Library

Printed and bound by CPI Group (UK) Ltd, Croydon, CR0 4YY

Typeset in 10.5/14.5 pt ITC Cheltenham Book &
10.7/14.8 pt ITC Cheltenham Light
Contents

What the Families Say vi
List of Main Contributors viii
List of Plates ix
Foreword by Tony Comer xi
Preface xv
Acknowledgements xvii
Prologue 1
Chapter 1 Between the Wars 6
Chapter 2 Bletchley Park: The Early Years 23
Chapter 3 Bletchley Park: The Intelligence Factory 94
Chapter 4 The Technical Challenge 134
Chapter 5 American/Canadian Liaison 175
Chapter 6 Post-War: Telling the Real Story 224
Epilogue 302
Appendix Letters to the Editor 307
Notes 316
Bibliography 326
Index 329
What the Families Say

Partly because he was so steeped in the secrecy surrounding their work, and partly from his inherent modesty, my father, Dennis Babbage, rarely spoke about his time at Bletchley – but it was important to him that the work and the history were properly understood. I'm delighted by the work that Joel Greenberg has done, in this and earlier books, to elucidate and enrich the Bletchley Park story. I know that my father, who was the Chief Cryptanalyst in Hut 6, would have felt the same.

Steve Babbage

* 

Joel Greenberg's research related to my father Gordon Welchman's biography was thorough and careful. I believe that this collection of correspondence from those who were at Bletchley Park is similarly well researched, and provides a valuable resource with new perspectives into the period.

Rosamond Welchman

* 

Joel Greenberg's anthology of letters written by the famous and the (undeservedly) less famous gives a wider perspective of the strength, depth and diversity of the GC&CS codebreaking team that my grandfather Alastair Denniston and his inner circle put together in the 1930s and early 40s – fascinating.

Nick Denniston

*
What the Families Say

Correspondence in this book reports on Alan Turing having buried silver bars in the fields around Bletchley. After the war he offered my father Donald Michie a third, or a daily rate, to retrieve them; fortuitously my father chose the daily rate, as Turing couldn’t remember where the bars were buried! Other letters describe my father’s contributions, along with Jack Good, to finding ways of improving the Colossus computers, used against the German High Command’s Lorenz cipher system.

Jonathan Michie

As a child I often heard my parents, Peter and Rosamond Twinn, refer to “Bletchley” and the people they knew there during WW2. Friends, including two honorary aunts, from Bletchley visited us now and then. But the talk was always of the social life, and in particular the music-making that first brought them together. There was never the slightest hint of what Bletchley was or what they did. Joel Greenberg’s wonderful new book fills in the gaps by painting a vivid picture of their working lives there.

Stephen Twinn

Those of us who grew up with an inkling of how the work at Bletchley contributed to the Allies’ success in the Second World War never expected the world to hear of it. Whilst BP codebreaking has since become common knowledge, full details remain elusive. Joel Greenberg’s researches have added further layers to the picture. For descendants of the BTM staff seconded to BP, such as my father Ronald Whelan, it is particularly good to see the idea debunked that Hut 7 and C Block were merely a ‘registry’ rather than a vital protosearch engine for German naval Enigma intercepts and other other code and cipher systems.

Penny Kay (née Whelan)


Main Contributors

Alastair Denniston for biographical information, see page 12
Dillwyn (Dilly) Knox 18
Gordon Welchman 32
Margaret Rock 38
Peter Twinn 56
Keith Batey 72
John Herivel 83
David Rees 87
R. V. Jones 91
Harold Fletcher 94
Dennis Babbage 114
Philip Lewis 116
Ronald Whelan 135
John Monroe 144
Max Newman 161
Bill Bundy 194
Pat Bayly 195
Ken Maidment 221
Frederick Winterbotham 225
Bill Filby 231
George McVittie 243
Stuart Milner-Barry 251
Peter Calvocoressi 260
Harry Hinsley 282
Joan Clarke (née Murray) 285
Donald Michie 295
Plates

Denniston, Vincent and Tiltman (*Bletchley Park Trust*);
Denniston’s Polish visa, January 1939 (*Bletchley Park Trust*);
Denniston’s diary for 24 July 1939 (*Author’s collection*);
Gordon Welchman in his Morgan car (*Welchman family*); Alan Turing (*Turing family*).
Hugh Alexander (*Crown Copyright*); Peter Calvocoressi (*Crown Copyright*); Reg Parker (*Parker family*); Dilly Knox and Margaret Rock (*Charles and Jane Foster*).
John Jeffreys and Pam Hemsted (*Author’s collection*); Peter and Rosamund Twinn (*Stephen Twinn*).
Women working on Hollerith equipment in Block C (*Crown Copyright*); Welchman’s diary for 15 July 1941 with the entry for his visit to the Foreign Office (*Author’s collection*).
Dennis Babbage (*Babbage family*); John Herivel (*Bletchley Park Trust*).
Keith and Mavis Batey (*Bletchley Park Trust*); David Rees (*Rees family*).
Electrical assembly area at BTM Letchworth (*Crown Copyright*); Harold Keen receiving an award (*Author’s collection*).
Stuart Milner-Barry (*Author’s collection*); Max Newman (*Bletchley Park Trust*).
High-speed four-rotor bombe (*Crown Copyright*).
Edward Travis (*Author’s collection*); Alastair Denniston and Bill Filby (*Julia Mills*).
Map board developed by SIXTA (*Crown Copyright*); Donald Michie (*Michie family*).
Attendees at the secret conference at Arlington Hall in March 1944 (*Author’s collection*); Prototype of the RM-26 ‘Mixmaster’ (*Crown Copyright*).
The Bletchley Park Codebreakers

Harold Fletcher (Crown Copyright); Gordon Welchman and William Bundy (Picture used with the permission of William Adams).

Joan Clarke with colleagues outside Bletchley Park after the war (Bletchley Park Trust); William Friedman and John Tiltman (Library of Congress).

Members of Hut 6 at the end of the war (Bletchley Park Trust & Kellogg College); Bletchley Park in the 1960s (Living Archive, Milton Keynes).

Items shown as Crown Copyright are reproduced by kind permission of the Director, GCHQ.
Allowing the participants in British signals intelligence (Sigint) to explore its history through the letters they exchanged with each other is an imaginative new approach to telling their story. This anthology includes both letters written contemporaneously with the incidents being described and the correspondence between veterans of Sigint, as they tried to reconcile their memories of what happened with those of their former colleagues.

Not only is more known about British signals intelligence – the Government Code and Cypher School (GC&CS) – at Bletchley Park during the Second World War than probably any other major intelligence organisation in history, but its history was first told by the individuals who worked there, before an official history of British Intelligence in the Second World War had been published, and long before the official wartime records had been released. This has created a unique narrative about what happened at Bletchley, because few of those telling the stories were members of the senior staff responsible for its strategic direction. The story has been told from the bottom upwards and is about the people who worked there and what they did, rather than about the impact of the intelligence they produced.

This book is a valuable addition to the literature on British Sigint, partly because it begins the story during the First World War, when British signals intelligence was created (Bletchley Park was the creature of twenty-five years’ experience); partly because some of the contemporary letters give an insight into what wartime life was like for those working at GC&CS – Margaret Rock’s letter to her mother describing being stuck at Euston during an air raid is a good example – illustrating the fact that just getting to work, physically and mentally ready for the day’s tasks, was harder than we might realise; but also because it charts the
way in which the former intelligence officers reconstructed what they had done there, more than thirty years after they had gone their separate ways convinced that they would never be allowed to tell their stories.

Peter Twinn, in one of the letters reproduced in this book, shows why we need to be cautious about over-reliance on what people claim to remember decades after the event:

They (GCHQ) thereupon sent Joan Clarke to see me with a copy of what I and others had written after the war as the official record. I was appalled to discover how my memory had played me false. Since then, I have been very sceptical of other people’s detailed reminiscences of those far off days.

The point, however, is that we read how the men and women of Bletchley tested each other’s reminiscences against their own, and this makes their conclusions a lot more likely to reflect the reality of what happened than some of the more imaginative reconstructions that have appeared.

There is one thread which runs through many of the letters: a sincerely held belief which I think is quite mistaken. It is perhaps best exemplified by an extract from a letter Sir Stuart Milner-Barry wrote to The Guardian:

But . . . the complaint is . . . a prime example of the lengths to which GCHQ’s paranoia about the preservation of ancient secrets will carry them. To talk of ‘direct damage to security’ in the context of Welchman’s article in Intelligence and National Security is surely absurd . . . to suppose that the battles which we had to wage before the birth of the first electronic computer (which must seem to present-day cryptanalysts rather like fighting with bows and arrows) could be relevant to security now is just not credible.

How could he know, forty years after leaving Bletchley Park, what could and couldn’t be relevant to security? I must declare an interest, as between 2009 and 2019 I was responsible for what
Foreword

GCHQ (Government Communications Headquarters) released – and what GCHQ didn’t release. I was regularly challenged, for example, to release material about the cryptanalysis of Japanese systems but consistently refused: the sensitivity is not in what systems were solved, but in how cryptanalysts approached the task of breaking them. Any approach which has not been publicised and which might still be useful against an adversary today is rightly kept secret. Records which can be released should be released, but GCHQ would be foolish if it allowed adversaries an insight which could allow them to make themselves more secure. It is unfortunate that GCHQ was unwilling to articulate this policy until relatively recently, but the policy is sound, however frustrating it was to people who wanted to tell all of their story and who found they could only tell part.

For those of us familiar with the Bletchley Park story, reading many of the letters in this book is like overhearing a conversation between old friends: we pick up new details and perhaps think a little more about the way in which the writers collaborated at the time. But there are details which can still shock, for example ‘Dilly’ Knox’s comments about A. G. Denniston as Head of Bletchley Park in a letter to C:

Neither Commander Denniston’s friends, if any, expected, nor his many enemies feared, that on the outbreak of war such responsibilities should be left in hands so incapable.

Much more positively, we see how the agreement signed off by President Roosevelt and Prime Minister Churchill translated into warm friendships between British and American cryptologists: Friedman’s with Denniston, Bundy’s with Milner-Barry. I am also particularly pleased that the Canadian cryptologist Pat Bayly, who designed the Rockex cipher machine, makes an appearance and records anecdotes about some of the most significant of his British colleagues. Today’s partnership between the Sigint organisations of Australia, Canada, New Zealand, the UK and the US – sometimes known as ‘The “Five Eyes” Agreement’ – is based on an agreement signed first in 1946, which has been sustained since then, not just by the political will of the governments of
The Bletchley Park Codebreakers

each country, but by the personal relationships which grow up between members of each country’s signals intelligence agency who share a common endeavour.

What Joel Greenberg’s judicious selection of material for this anthology shows is that we still have much to learn about the organisation that eventually became GCHQ. These letters shine a light on some of the gaps. Communications and communications security are not subjects normally dealt with by Sigint historians, yet Pat Bayly’s correspondence shows that secure forwarding was a crucially important part of the cryptologic picture. How far was the work of Bletchley Park hindered by rigid application of ‘need-to-know’ principle? These are just two of the questions which I hope new research, inspired by this anthology, will explore.

Tony Comer
Preface

The story of how people working at Bletchley Park (BP) during the Second World War (WW2) read millions of secret German communications has been told in numerous books and papers. Not surprisingly, it is a complex one, given that BP served as the main British war station for intelligence activities. It trickled out over the years and overcame the natural inclination of the authorities to suppress it. Historians did their best to piece the story together and some authors were able to take advantage of the relaxation of the rules governing what BP veterans could talk about. Their books were thus based, to some extent, on details extracted from veterans and supplemented with the gradual release of official documents, initially into the Public Record Office (PRO). In 2003, the PRO merged with the Historical Manuscripts Commission to form The National Archives (TNA) based at Kew in London.

However, despite these publications, some of the participants had felt honour-bound by the Official Secrets Act and said little about their wartime activities. Others, who had remained in GCHQ after the war, felt that any disclosures from them might threaten their pensions. Early accounts were short of detail and in some cases inaccurate. As official documents were gradually released by GCHQ and its American counterpart, the National Security Agency (NSA), historians and authors were able to piece together the story in a more accurate way. But still the participants remained reluctant to tell their story and restricted themselves to contributing chapters to books compiled by others. A few of the men involved wrote short books but revealed little more than what was already in the public domain. Some of the young women who had been involved wrote their memoirs, although many of them were restricted to accounts of their social lives.
The Bletchley Park Codebreakers
during the war. The one exception to this was Gordon Welchman who published his memoir, The Hut Six Story in 1982. This book revealed, for the first time, much of the operational and technical detail behind BP’s success. Only four of the key participants, Alastair Denniston, Dilly Knox, Alan Turing and Welchman have been the subject of serious biographies.¹

By the time I began seriously to research and write about BP and its wartime activities, most of the key personnel were dead, or elderly with failing memories. However, some of their families had faithfully kept their papers, which they were more than willing to share with me. While most veterans had remained reluctant to publish their real views or even to share them with authors and historians, many had no qualms about sharing them with former colleagues. Over the years, my research uncovered hundreds of letters and emails between veterans which I was able to recover from their families’ lofts and dusty cupboards. This book is based almost entirely on the words of the participants themselves in telling some of the story of BP. It also draws on letters and other documents which have been declassified by GCHQ. In their private letters, unhindered by official oversight, they talk freely about aspects of the BP operation in which they were involved. The letters demonstrate that the work of BP was not restricted to cryptography but also included data and traffic analysis. Several talk in detail about communications security, a subject almost completely untouched by those writing about Signals Intelligence (Sigint) in WW2. The letters are prefaced with short biographies of the correspondents and a description of their context. Obvious minor spelling and grammatical slips in the originals have been silently corrected but otherwise the documents are presented in unedited form. The spelling cipher (and its compounds) is used in all editorial text, but cypher is retained where it occurs in quoted matter.

The letters and private communications reveal the true feelings of the participants and they document both the successes and failures of their organisation during the war. In many cases, personal or departmental rivalry is shown to have contributed to such failures.
Acknowledgements

I have been researching, writing and speaking publicly about British signals intelligence in the twentieth century for a number of years. During that time, I have always been struck by how little is known about some of the key people involved, particularly at Bletchley Park during WW2. The families of Alastair Denniston and Gordon Welchman were kind enough to provide me with a considerable amount of their post-war correspondence. This helped me immeasurably when I came to write their biographies. Following the publication of this book, it is my intention to donate this correspondence to an appropriate research archive.

I am now grateful to the families of many other Bletchley veterans for sharing letters and photographs with me during the course of writing this book. In particular, I would like to thank the families of Dennis Babbage, William Bundy, Donald Michie, Max Newman, Reg Parker, David Rees, Margaret Rock, Peter Twinn and Ronald Whelan. Frank Carter and the late Ralph Erskine were kind enough to share with me their correspondence with Mavis and Keith Batey. I am most grateful to St John’s College, Cambridge, for allowing me to reproduce letters from their archives and to Tony Comer for his supportive comments about this book and for writing a foreword for it. I would also like to thank Kelsey Griffin for her advice and professional support over a number of years.

Finally and most importantly, I would like to thank my wife for her love and personal support while I managed to put this book together during the Covid pandemic. I could not have done so, while being restricted to home working for eighteen months, living with anyone other than my soulmate.
For the families of the
Bletchley Park codebreakers
Early histories of WW2 were written without any knowledge of the role that Sigint had played in its outcome. The Allies had managed to acquire an extraordinary amount of intelligence from the signals (i.e. communications) of their enemies. Many of these signals had been disguised by the use of codes and ciphers using both hand methods and machines. This intelligence helped Allied commanders make key decisions throughout the war and much of it came from a rather odd collection of wooden huts and brick buildings in the middle of the English countryside. The head of Britain’s Secret Intelligence Service (SIS), Admiral Hugh Sinclair, had acquired a 55-acre country estate called Bletchley Park in 1938 to serve as his war station for intelligence activities. It was from here for almost six years from early September 1939 until VJ-Day on 15 August 1945 that a stream of intelligence reports flowed to all sections of the British armed forces and to Britain’s allies. The work was carried out by personnel working for the Government Code & Cypher School (GC&CS), Britain’s signals intelligence department. Its ultimate role in the outcome of the war was probably most accurately articulated by the Supreme Commander of the Allied Expeditionary Forces, General Dwight D. Eisenhower in a letter to the Head of SIS and Director of GC&CS Major-General Sir Stewart Menzies. The letter, dated 12 July 1945, went on to say that:

The intelligence which has emanated from you before and during this campaign has been of priceless value to me. It has simplified my task as a commander enormously. It has saved thousands of British and American lives and, in no small way, contributed to the speed with which the enemy was routed and eventually forced to surrender.
The general public first became aware of BP and the codebreaking activities which took place there during WW2 when Frederick Winterbotham published his book *The Ultra Secret* in late 1974. The book was announced with some fanfare when it was previewed in two parts in the *Sunday Telegraph* several months earlier, on 21 and 28 July. Many BP veterans were astonished and some disgusted by this apparent breaking of the pledge they had made many years before never to talk about such matters. According to Winterbotham, in correspondence with his former wartime colleague Gordon Welchman years later, his British & Commonwealth publishers, Weidenfeld & Nicolson of London had been very helpful in getting him permission to publish. He claimed that, despite objections from members of the Defence Committee, ‘Sir George Weidenfeld is a close friend of Harold Wilson who had the final word’ with regards to publication. Winterbotham had not included any technical detail in his book because he knew very little about that part of the BP operation. He was not given access to official records and had no direct knowledge of the actual processes which produced the so-called ‘Ultra’ intelligence. Instead, he restricted himself to describing how intelligence produced at BP was processed and distributed to Allied commanders in complete secrecy. Meanwhile, British authorities continued to oppose the release of any information about the methods which were used to obtain the intelligence.

The British government finally agreed to relax some of the rules governing BP activities and the official position was articulated by the Foreign Secretary, Dr David Owen, in Parliament on 12 January 1978. He announced that some BP records were being released to the PRO, including those based on intercepted radio messages of the enemy armed forces. It was felt that they no longer required security protection and that their availability would enable a better historical judgement to be made of the part that intelligence played in the conduct of the war. He went on to say:

Those who gave the undertakings of reticence to which I have referred are now absolved from them to the limited extent that they may now disclose the fact that
they worked on or used material based on intercepted radio messages of the enemy armed forces. They may for example acknowledge having worked as interceptors, cypher breakers, distributors or users of this material, and may reveal what they know of the use made of it in the conduct of the war.\(^4\)

Remarkably, BP activities had been described in several publications, well before Winterbotham’s book appeared in print. In the second volume of his memoirs, published in 1973, the journalist and author Malcolm Muggeridge, a member of MI6 during the war, mentioned BP on numerous occasions. He described ‘cracked cipher material’ as being the staple product of MI6 which provided the basis of most of its activities. He went on to say that:

The establishment which produced this precious material was located at Bletchley, in a manor house in which I spent some days familiarising myself with the place, its staff, its output and manner of working. As might be supposed, in view of the business at hand, the staff were a curious mix of mathematicians, dons of various kinds, chess and crossword maestros, an odd musician or two, and numerous wireless telegraphy experts.

Another book appeared in 1973, Philby: The Long Road to Moscow by Patrick Seale and Maureen McConville, which included a fifteen-page chapter titled ‘The Golf Club and Chess Society’. This was apparently a jokey name coined by GC&CS personnel in the late 1930s. The chapter summarised the whole story of Sigint including the creation of the British naval codebreaking section, Room 40, at the beginning of WW1. It also included personal details about the family of the first head of GC&CS, Alastair Denniston.

Even mainstream television got into the act. The classic 1970s BBC television series Colditz followed the lives of Allied servicemen imprisoned at the supposedly escape-proof Colditz Castle. In Series 2, Episode 3 the prisoners were trying to get a message to British intelligence services. One sent a coded letter
The Bletchley Park Codebreakers
to his wife who, being good at crossword puzzles, recognised it as such and took it to MI5. One of the MI5 officers said to a colleague ‘We could try sending it to Bletchley.’ The programme was broadcast on 21 January 1974 well before Winterbotham’s book appeared. One of the creators of the series had previously drawn on his WW2 RAF experiences to produce, in 1963, a drama about an RAF squadron which ferried agents in and out of occupied Europe. In all likelihood, he knew about BP and was tempted to drop the name into the script. One year before the Foreign Secretary’s announcement to Parliament, the BBC broadcast a seven-part series called The Secret War. Episode 6, broadcast on 9 February, was called Still Secret and told the story of Germany’s Enigma machine and the production of Ultra intelligence. By 1999, Channel 4 was able to broadcast a four-part series called Station X which told the story of BP and included contributions from BP veterans.

Documents released to the PRO in January 1978, presumably along with others still classified, had already been made available to historians writing an official history that would discuss British Sigint. The first volume of this work, British Intelligence in the Second World War, was published in 1979. A number of BP veterans who had been in senior positions at BP during the war were still alive and keen to write their own memoirs. However, the government’s position was that the documents they wanted access to as part of their research were with the ‘official historians’ and would remain so until their work was finished. While some of the ‘official historians’ were themselves BP veterans, it appears that none of these veterans who wanted to produce their own accounts were consulted by those working on the official history. More official histories have appeared since the original Sigint history was published between 1979 and 1990. They include a sanctioned history of SIS, MI6: The History of the Secret Intelligence Service 1909–1949 which appeared in 2010 and one of GCHQ, Behind the Enigma: The Authorised History of GCHQ, Britain’s Cyber-Intelligence Agency, which was published in 2020. As histories, they are understandably missing the personal and honest views of those who were involved. It is not clear why the
authors of the 1979 history and its subsequent volumes chose not to reach out to some knowledgeable veterans who were keen to contribute. The authors of the later histories did not have that option as all of the key people involved were no longer alive. So access to official documents alone does not guarantee that the complete story of BP and the work of GC&CS can be told.

Official documents supplemented by the personal views of those involved, as expressed in their letters and correspondence, may well lead to a more complete story. A considerable amount of wartime correspondence has been available to the authors of all of the histories since the mid-1970s. However, in most cases, workplace protocols were followed and those involved kept their personal views to themselves. The one exception to this was the veteran cryptanalyst Dillwyn (Dilly) Knox, who was more than happy to say exactly what he thought to his colleagues and superiors. As for his colleagues, their personal correspondence remained stored in the lofts and cupboards of their families after their death. Much of this was written thirty years or more after the end of WW2 and relied on the quality of individual memory. Gordon Welchman’s unsanctioned memoir *The Hut Six Story* included an extraordinary amount of technical detail, yet was written almost entirely from memory. Remarkably, his correspondence revealed that he had no memory of writing the famous ‘Action This Day’ letter to Winston Churchill in October 1941. David Rees was a brilliant mathematician who worked on breaking German Air Force and Army Enigma messages. He is generally credited with making the first break of a German encrypted message using a technique developed by his fellow Cambridge mathematician and BP colleague John Herivel. Yet writing to Herivel in 1999, fourteen years before his death, Rees thought that someone else had made that first break and that he was on leave at the time!

So while one must read this correspondence with some reservations, it does provide a unique insight into the work of GC&CS, warts and all, and adds to an understanding of how the organisation was able to achieve such remarkable success.
Chapter 1

Between the Wars

On the 11th hour of the 11th day of the 11th month of 1918, the cacophony of artillery fire along the Western Front in France suddenly fell silent. Both sides agreed to stop fighting and to declare an armistice and the Allies faced choosing between peace with a partial victory or continuing the carnage and pushing on to Berlin. The cost of the latter was far too high in terms of morale, logistics and resources.

British intelligence departments had enjoyed a successful war. The Admiralty’s section, known as Room 40 OB, had decrypted a telegram from the German Foreign Secretary to his ambassador in Mexico which would eventually bring the USA into the war. It had contributed intelligence to Navy commanders from the first naval battle of WW1 at Heligoland Bight in August 1914 through the war’s biggest naval combat at Jutland in 1916, and beyond. The War Office’s section, known as MI1b, had also produced Sigint from the first to the last month of the war. Along with aerial reconnaissance, it had proved, according to the official history of GCHQ, ‘more valuable for the British Army than every other source put together’. Once the trenches were established, Sigint was not of much use on the Western Front and of varied use elsewhere. This changed in 1917–18, particularly in Palestine and Iraq, where Britain read most of the wireless traffic of the German and Turkish forces. The greatest successes of Sigint in WW1, particularly in 1916–18, were of significant enough quality to match some of the most successful periods in WW2.

In November 1918, as well as a scheme for an amalgamated secret service, the Director of Military Intelligence, Major-General William Thwaites had proposed to his naval counterpart, Rear-Admiral Sir Reginald ‘Blinker’ Hall (soon to be replaced by Hugh Sinclair), that the two signals intelligence sections in the
Admiralty and the War Office should be united into a single ‘School’, so called to provide cover by stressing the organisation’s positive side, for example by studying ways to achieve secure communications.

The Admiralty wrote to Lord Drogheda of the Foreign Office giving its view of the newly formed GC&CS:

_Private and confidential_
28 March 1919

Dear Lord Drogheda,

I had a few minutes conversation with Lord Curzon yesterday on the subject of the new Cypher Department which it is proposed to establish, and concerning which a memorandum is now in his hands, containing the views of the Admiralty and the War Office.

Lord Curzon told me that he hoped to summon a conference at the Foreign Office one day next week to consider the matter, when I should have an opportunity of stating my opinions, and he asked me to send you in advance a memorandum of the points I wished to raise. I therefore send you herewith the following notes of matters which the Admiralty consider essential in any scheme that may be adopted.

1. We have in the Section of the Naval Intelligence Department which has dealt with enemy wireless during the war, a great deal of material, some of which is worked out and filed for reference or historical purposes and some of which will require further study. We also have a small remaining nucleus of the expert staff which has done its work during the war. If the Admiralty is to join the new Department, we regard it as essential that this material and staff should be kept together.

2. Wherever the new Department may be located in peace time, we should have to stipulate that on the outbreak of war the naval portion of its staff should immediately be mobilised and take up their work in the Admiralty. Our experience has proved that in war the deciphering staff must be in the closest possible proximity to the War Staff.
The Bletchley Park Codebreakers

We have had to work day and night all the year round, and as immediate action has often had to be taken in consequence of the information which we have supplied, no avoidable delay in transmitting the information to the Operations Division can be allowed.

3. We should only consent to pool our staff with that of the War Office on condition that Commander A. G. Denniston is placed in charge of the new Department. I do not say this on account of any jealousy of the War Office, or any reluctance to accept a War Office man, but because no one who has not been trained in the conditions under which we have to work could meet the requirements of the Admiralty in time of war. Our work has been done in the face of the enemy and always against time. The messages we have had to decipher were from ships at sea, engaged in actual operations, or from airships also operating. We have had to master a new key every morning before we could begin to read the messages, and sometimes we have had to grapple with two or three keys in one day!

This has of necessity developed a particular kind of aptitude for the work, which depends for its success more on a study of the psychology of the persons sending out the messages and a sort of instinctive ‘flaire’ [sic] for the kind of things they are saying, than upon careful study and analysis for which there is no time.

In the War Office they have dealt with cables which are far more accurate than wireless, and have never had to work against time, and the aptitude they have developed is different from – I do not for a moment suggest it is inferior to that of which the conditions of our work have produced.

Denniston is not only the best man we have had, but he is the only one we have left with special genius for this work. We shall not be able to retain him in a subordinate capacity, and no advantages of concentration and
co-operation with the War Office would compensate us for the loss of his services. If the War Office people are not willing to accept this condition, we should prefer to retain our staff in the Admiralty, but should of course co-operate with them in every other way that is possible.

4. Provision would have to be made for the payment of temporary salaries to ex-members of the staff who are willing to come up at intervals when required to give the benefit of their expert knowledge for say a fortnight to three months. They would thus both help the permanent staff in emergencies and keep their hands in for the day they may once more be required.

5. I presume the staff of the new Department would have the status of Civil Servants.¹

At a meeting on 25 August 1919, due consideration was given to who should head up the new organisation. The Admiralty had made it clear that Denniston was their choice and the War Office had put forward their own candidate, Major Malcolm Vivian Hay, who had headed up MI1(b). It was agreed that Denniston would head up the new organisation and R. R. Scott of the Foreign Office duly wrote to key people, informing them of the decision.

24 October 1919

Sir,

1. I am commanded by my Lord Commissioners of the Admiralty to acquaint you for the information of –

   1. The Army Council
   2. The Air Council
   3. The Secretary of State for Foreign Affairs
   4. The Secretary of State for India, India Office
   5. The Secretary of State for the Colonies
   6. The Minister of Munitions
   7. The Minister of Food
   8. The Minister of Transport
   9. The Postmaster-General

¹
The Bletchley Park Codebreakers

that the War Cabinet has now given approval for the formation of a Government Code & Cypher School under the control of the Director of Naval Intelligence, and that it is proposed that it should commence its duties on the 1st November, 1919.

2. It has been decided to appoint Commander A. G. Denniston, O.B.E., R.N.V.R. as Head of the Government Code & Cypher School, which will be accommodated in Watergate House, Adelphi, W.C.I.

3. The duties of the Code & Cypher School will be as follows:-

(a) To compile and be responsible for printing all codes and cyphers used by the British Government Departments with the sole exception of those mentioned in paragraph 5 below.

(b) To examine all the British Government codes and cyphers now in force and the purpose for which they are used, mainly with a view to ascertaining and, where necessary, increasing their degree of security; but also so as to ensure that messages shall be free from ambiguity and undue delay ensuing from mutilation in transit, and that they shall be coded in the most economical manner possible.

(c) To maintain the closest liaison with all British Government Departments using codes and cyphers, and to advise them generally in matters relating thereto.

(d) To instruct as large a proportion of Officers as possible who may be employed at any time in coding or cyphering.

(e) To assist in the preparation of any hand-books or instructions relating to coding or cyphering, or of those concerning the handling of code and cypher messages in general.

4. I am therefore to suggest that each Department concerned should appoint a ‘Liaison Officer’, whose duties will be, approximately as follows:-

i. To keep in touch with the requirements of his Department as regards codes and cyphers and all matters
Between the Wars

in connection therewith, and to ensure that these requirements are met by the Government Code & Cypher School.

ii. To be responsible for the suitability of the ‘Dictionary’ (or ‘Vocabulary’) of the codes and cyphers compiled for his Department.

iii. To advise the Head of his Department on:-

(a) The institution of additional books to meet new developments.

(b) ‘Departmental Codes’ before and during their construction.

iv. To maintain a watch over his Departmental messages for faults in coding or cyphering, or any other defects, which might prejudice the security of the code or cypher used; in this connection he will work in close co-operation with the Head of the Coding and Cyphering Section of his Department.

v. To assist in the instruction of the Officers of his own Service who may be employed at any time in coding and cyphering.

5. The preparation, etc., of the ‘Signal Books’ and purely ‘Departmental Codes’ of the three fighting services will remain in the hands of the Services concerned.

6. In the case of Departments which require large numbers of codes and cyphers, it will be necessary to accommodate their ‘Liaison Officers’ in the Government Code & Cypher School but where the requirements are small, this should not be necessary.

7. If no objection is seen to these proposals, I am to request that arrangements are made to bring the foregoing scheme into force, so far as your Department is concerned, and that a Liaison Officer for the

1. War Office
2. Air Ministry
3. Foreign Office
4. India Office
The Bletchley Park Codebreakers

5. Colonial Office
6. Ministry of Munitions
7. Ministry of Food
8. Ministry of Transport
9. General Post Office

may be appointed.

I am, Sir,
Your obedient servant
R. R. Scott

Alastair Denniston

Alastair Guthrie Denniston was born on 1 December 1881. He enrolled at London University where he was awarded a BA in 1902 and then studied at both Bonn University and the Sorbonne in Paris. He took up a post as a Modern Languages teacher at Merchiston Castle School, Edinburgh, in 1907. He then moved to the Royal Naval College at Osborne, Isle of Wight, in 1910 and took up the post of Modern Languages Master. During WW1 he worked in the British Admiralty’s codebreaking section known as Room 40. At the end of the war he was appointed as the first Head of the newly created GC&CS. By 1938, knowledge of Germany’s territorial ambitions led Denniston to plan for a careful expansion of GC&CS. With an eye on quality over quantity, he drew up a list of men who agreed, in the event of war, to undertake secret work for the Foreign Office.

When Britain declared war on Germany on 3 September 1939, these men, along with a number of recruits from the Oxbridge women’s colleges, were summoned to report for duty at GC&CS’s new intelligence centre at BP. In the early days of WW2, Denniston encouraged innovation and oversaw the early development of GC&CS, the forerunner of modern-day GCHQ. He hosted the first meeting between British and American signals intelligence representatives in his office at BP in early February 1941. His trips to the USA and Canada in the latter part of 1941 played a significant role in establishing Anglo-American collaboration in signals intelligence and the ‘special relationship’ between the two
countries. In February 1942, following a restructure of GC&CS, Denniston was given a smaller role overseeing diplomatic and commercial cryptanalysis work. His new department moved to offices in Berkeley Street in London where he remained in charge until the end of 1944. He was then encouraged to retire with a pension much smaller than he had expected and his death on 1 January 1961, at the age of 79, was ignored by the intelligence community which he had served for thirty years.

The name of Denniston’s new organisation, GC&CS, was invented by Courtney Forbes, a member of the Communications Department of the Foreign Office. Publicly it was ‘to advise as to the security of codes and cyphers used by all Government departments and to assist in their provision’. However, its secret directive was ‘to study the methods of cypher communications used by foreign powers’. Pressure from the Director of Naval Intelligence and others forced the inclusion in the New Official Secrets Act of a clause instructing all cable companies operating in the UK to hand over scrutiny copies of all cable traffic passing over their systems within ten days of despatch or receipt. Interestingly, the three services were expressly excluded from needing GC&CS’s advice regarding their own codes.

GC&CS was up and running very quickly and its first decrypts were issued two days after its formation. The new organisation was housed as agreed in Watergate House in Adelphi. Lieutenant-Commander Edward Travis was appointed to run the Construction Section and act as Deputy Head. Travis had experience of naval codebook construction, so he took responsibility for cipher security while Denniston supervised cipher-breaking, Travis also advised the Admiralty on communications security. However, GC&CS had no authority to advise on good security practice so his role was limited. This may have led to his losing interest in security, hence the two Admiralty security staff assigned to GC&CS ended up working as cryptanalysts. In the end, the advice from GC&CS to the Admiralty about code and cipher security was very poor.

On 23 July 1921, the Foreign Office told the Treasury it was taking over GC&CS from the Admiralty along with its staff of 87
and operating costs of £31,464 per year. The change was put into effect on 1 April 1922 for Treasury budgetary reasons. Admiral Hugh Sinclair returned to Intelligence as Head of SIS following the death in June of Mansfield Cumming, the service’s first head. By September, he had arranged for GC&CS to come under his control. It was agreed that Denniston would report to Sinclair, who would serve as both Head of SIS and Director of GC&CS and in turn, Sinclair would report to the Foreign Office. These arrangements would remain in place for more than twenty years. While the armed services kept some collection expertise, SIS in effect acquired monopoly control over diplomatic Sigint and high-grade cryptanalysis. This proved to be an effective strategy and GC&CS provided Whitehall with a constant stream of intercepted and decrypted telegrams of foreign governments. It read the communications of Italy, the United States and Japan and those of many smaller countries. Between 1919 and 1935, GC&CS was probably the largest and most effective Sigint organisation the world had ever seen.

On 19 August 1934, a national referendum confirmed Adolf Hitler as sole Führer (Leader) of Germany. His Nazi government began making aggressive territorial demands on neighbouring countries and threatening war if these demands were not met. In response to this increasing threat to Britain, GC&CS almost doubled its cryptanalytical staff, particularly in its military sections, between 1935 and 1938. By 1938, Sinclair had become concerned that most of the British intelligence services were based in the middle of London and in the event of war were vulnerable to an air attack. He began looking for a site outside London to serve as a war station for intelligence activities. Bletchley Park was an ideal location as it was close to Bletchley station which was on the main north–south rail line, near the A5, a major arterial route along which ran trunk cabling connecting the north and south of the country and on to its worldwide cable and wireless network. It was also near the RAF’s main radio station at Leighton Buzzard, and thus also the Defence Teleprinter Network. There were direct rail links from Bletchley station to both Oxford and Cambridge which would prove useful.
Between the Wars

Denniston had already drawn up an emergency list of men who were approached in 1938 and agreed, in the event of war, to undertake secret work for the Foreign Office. Many of the men on this list, whom Denniston referred to as ‘men of the professor type’ would come from the great British universities of Oxford and Cambridge. A deal was struck for the site to be leased for a period of three months and it was subsequently purchased by Sinclair on 9 June 1938 for £6,000. During the Munich Crisis, partly as a precautionary measure and partly as a mobilisation exercise, Sinclair sent GC&CS and other Foreign Office staff to BP. Telecommunications engineers had already been working on the site since its purchase. At the end of September 1938 the Munich agreement was signed and most of the GC&CS staff returned to London.

On 15 July 1928 Polish radio-monitoring stations in Starogard Gdański, Poznań and Kraków-Krzesławice had intercepted German messages in a machine-generated cipher for the first time. During 1931 a Polish cipher bureau was created which was an amalgamation of the radio intelligence and cryptography sections. The new bureau was headed by Major (later Lieutenant-Colonel) Guido Langer. A small section under the command of Captain (later Major) Maksymilian Ciężki was set up for three recent recruits, mathematicians Marian Rejewski, Hendryk Zygalski and Jerzy Różycki. The Poles had learned that the Germans were modifying a commercial cipher machine, known as Enigma, for military purposes. By the end of December 1932, Rejewski, with the help of information provided by an employee of the German Defence Ministry Cipher Office in Berlin, had reconstructed the internal connections within the Enigma machine and worked out details of how it was currently being used by the German Army. The Polish Cipher Bureau began to read encrypted German Army messages and had considerable success for a number of years. The German Air Force began using Enigma machines at the end of 1934 and the number of different networks to monitor grew rapidly.

By early 1936 the Germans had introduced significant changes and the Enigma system became increasingly difficult
The Bletchley Park Codebreakers

to break. The following year the Polish General Staff transferred their German cryptographic section BS4 to a camouflaged and high-security new headquarters in the Kabacki Woods near Pyry outside Warsaw. As the Germans changed procedures or tightened their security, the Poles would invent technologies to counter them. When the German Air Force and Army issued their Enigma operators with two additional encryption wheels to use in their Enigma machines, on 15 December 1938, the Poles began to struggle even more. With three wheels available, these could be used in the machine in six possible orders. By being able to choose three wheels from five, the number of different configurations increased to sixty. To make matters worse, the number of possible connections in another important component, the plugboard, was also substantially increased.

In London, GC&CS was also having little success in breaking the newer models of the Enigma machine. It is likely that, following the lead of the Poles, Denniston began headhunting mathematicians amongst his new recruits to GC&CS. He recognised that he needed to supplement his staff which consisted mainly of the old guard from Room 40 and MI1b and 'newer' recruits such as John Tiltman who, after a one year secondment to GC&CS in 1920, rejoined the organisation in 1929. The first mathematician to arrive was Peter Twinn, recruited through the Civil Services Commission. It was not essential that those approached from the universities were mathematicians. It was more important that they could apply their academic expertise to cryptanalysis. They would also need to tackle machines with machines, not the paper and cardboard tools that had been used against lesser machines.

Denniston was in effect recruiting computer scientists and foremost amongst them would be Alan Turing and Gordon Welchman. Both attended training courses in London in March 1939 presided over by Denniston, Tiltman and Oliver Strachey, a veteran of MI1b. Once the courses ended, the 'men of the professor type' returned to their normal university lives. Turing was the one exception to this, making visits to the GC&CS headquarters in Broadway every two or three weeks. He was introduced to Dilly Knox, a veteran of Room 40 who headed a research team which
**Between the Wars**

included Twinn, and was even allowed to take back to Cambridge some of the ongoing work on the Enigma system.

In late 1938, French intelligence proposed that the Polish Cipher Bureau meet with their British and French counterparts. Lack of resources was making the task of breaking the Enigma system increasingly difficult for the Poles. They agreed to the meeting in the hope that the British and French would have something to contribute to their work. The first trilateral meeting between representatives of the cryptographic services of France, Britain and Poland was held in Paris on 9 and 10 January 1939. In attendance on the Polish side were Langer and Ciężki; on the French side Bertrand and a French cryptanalyst, Henri Braquenie; on the British side, Denniston, Knox, Tiltman and Hugh Foss, a cryptanalyst who had joined GC&CS in 1924. The Poles had been instructed not to reveal anything unless they got something in return. As the British and the French had nothing to offer, the meeting, while cordial, was a waste of time.

By May, tensions between Poland and Germany were close to breaking point and, on 30 June, Langer contacted London and Paris with the news that something new had come up since January. He proposed a second trilateral meeting in Warsaw on 24–27 July. As Knox had been included in the invitation, Sinclair instructed Denniston to include him in the British delegation. Also included was Commander Humphrey Sandwith, head of the Admiralty’s interception service. Knox and Denniston arrived on the morning of 24 July (see Plate 3) and stayed at the Hotel Bristol.

The key meeting took place the next day at the Pyry Centre, 14 km from Warsaw. Much to the astonishment of the British and the French, the Poles demonstrated several machines and techniques which they had developed to help break Enigma keys. The news that the Poles were breaking German Enigma keys quite regularly was not received well by Knox who maintained a stony silence throughout the meeting. Knox, who arguably knew more about the Enigma machine than anyone in Britain, had been unable to break the new military version which included the plugboard.