

# BLETCHLEY PARK REPORTS

## Booklets in this Series

- No.1 Codebreaking with the Colossus Computer; an introduction by Frank Carter
- No. 2 The German Battleships; an account of the part played by Bletchley Park in dealing with the larger German warships, by Peter Jarvis
- No. 3 Codebreaking with Colossus; finding the K wheel settings, by Frank Carter
- No. 4 Codebreaking with Colossus; finding the K wheel patterns; the mathematics involved and an example from 1944, by Frank Carter
- No. 5 Getting back into SHARK; the capture of the cyphers from U559 by HMS *Petard*, by John Gallehawk and Peter Wescombe
- No. 6 Japanese Codes; the Background to the air attacks on Pearl Harbor and Ceylon, the diplomatic codes which gave away the German defences in the West, and the German transfers of uranium to Japan, by Sue Jarvis.
- No. 7 Convoys and the U-boats; the critical events in the Battle of the Atlantic during March 1943, by John Gallehawk
- No. 8 Bletchley Park and the Luftwaffe; the Fall of France, the Battle of Britain and the defence of Crete, by Peter Wescombe
- No. 9 Enigma and the Bombe; an introduction to breaking the cypher by the poles and the British, by Frank Carter
- No.10 The first breaking of Enigma; the pioneering work of the Polish Cypher Bureau, by Frank Carter
- No.11 How the Enigma secret was nearly revealed, by J. Gallehawk
- No.12 The Post Office at War, & Fenny Stratford Repeater Station, the GPO Telephones and their connections with Bletchley Park, by John Pether
- No.13 Black Propaganda; a description of wartime radio broadcasting around Woburn, by John Pether
- No.15 Some Polish contributions in the Second World War; epic stories of Polish skill and heroism, by John Gallehawk
- No.16 The Turing Bombe; how it worked; by Frank Carter
- No.17 Funkers and Sparkers, the Y Service, by John Pether

## HISTORIC GUIDES

- No. 1 Early History of Bletchley Park, 1235 - 1938 by Edward Legg
- No. 2 Guide franpis ä Bletchley Park, par "J'Equipe"

*Other booklets are in preparation*

# The Bletchley Park Trust Reports



## Codebreaking with The Colossus Computer

### Finding the K-wheel Patterns

An account of some of the techniques  
used, with a full illustrative example.

by

Frank Carter

**Report No. 4 June 1997**

# The Bletchley Park Trust Reports



## Codebreaking with the Colossus Computer

by

Frank Carter

**Report No. 1 November 1996**

# Contents

Introduction	3
International Teleprinter Code	4
The Lorenz Cipher machine	5
A decisive development	7
Breaking the cipher	7
A first step	8
"Pseudo plant text"	8
Pulse streams	9
The second step	10
Finding the correct K-wheel settings	12
Finding the wheel patterns ("wheel breaking")	15
Description of process	16
Acknowledgements	21
Conclusion	22



# **Codebreaking with The Colossus Computer**

An account of the statistical methods  
used for finding the settings for all the  
wheels an the Lorenz Cipher machine.

**(Including a full set of illustrative examples.)**

by

Frank Carter

**Report No. 3 (Second Edition) December 1997**

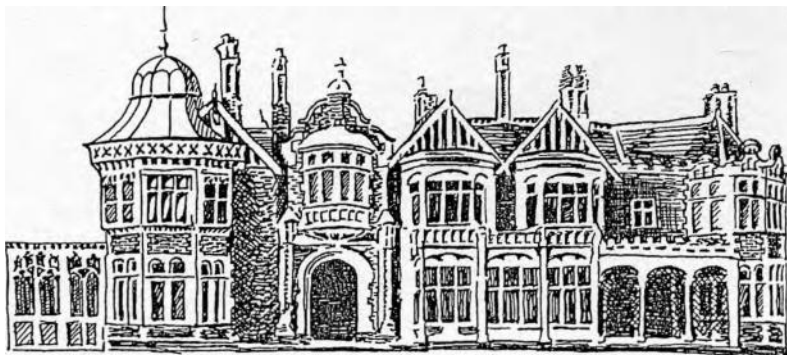
# Contents

Introduction	1
The relationship between A P and ä D	1
Statistical properties of A D	2
Wheel setting algorithms	3
Notation	3
Estimating the Power of an algorithm	<b>4</b>
Minimum length of message required for wheel setting	5
Estimation of evidence	6
Printing out the results of a run	7
A practical example	7
Finding the settings of the Motor and S-wheels	9
Finding the S-wheel settings	11
Appendices i - vii (practical examples)	12

*Frank Carter was Senior Lecturer in Mathematics at Bletchley Park Train, College and subsequently Principal Lecturer at Oxford Polytechnic.*

© Frank Carter and Bletchley Park Trust  
First published 1996. Second revised edition 1997

# The Bletchley Park Reports



## Fishing for Tunny

Interception of enemy radio  
teleprinter transmissions

by

John Pether

# Fishing for Tunny

Interception of enemy radio teleprinter transmissions

## Contents

1	Introduction	3
2	Telegraph Codes	6
3	Lorenz Schusselzusatz 42	11
4	First Intercepts and Denmark Hill	14
5	The first break	16
6	Copy and reading the transcripts	17
7	Knoekholt	18
8	Improvements to the process	21
9	Outstations	24
10	Staff	25
11	Summary	26
12	Bibliography	28



# The Bletchley Park Trust Reports



## Getting back into "SHARK"

H.M.S. Petard and the George Cross

by

Peter Wescombe & John Gallehawk

Report No. 5 June 1997

# CONTENTS

Getting back into 'Shark', the four rotor Enigma code

HMS *Pelard* and the George Cross

Tommy Brown, G.M.

16

John Gallehawk B Sc is a statistician by profession.  
Peter Wescombe B.A is late of IIM Diplomatic Wireless Service.  
F30th are volunteers with the 131etchley Park Trust.

# The Bletchley Park Trust Reports



## Getting back into "SHARK"

H.M.S. Petard and the George Cross

by

Peter Wescombe & John Gallehawk

Report No. 5 June 1997

# CONTENTS

Getting back into 'Shark', the four rotor Enigma code

HMS *Pelard* and the George Cross

Tommy Brown, G.M.

16

John Gallehawk B Sc is a statistician by profession.  
Peter Wescombe B.A is late of IIM Diplomatic Wireless Service.  
F30th are volunteers with the 131etchley Park Trust.

The Bletchley Park Trust Reports



# **How the Enigma Secret was nearly revealed**

by  
**John Gallehawk**

**Report No.11 October 1998**

# **HOW THE ULTRA SECRET WAS NEARLY REVEALED**

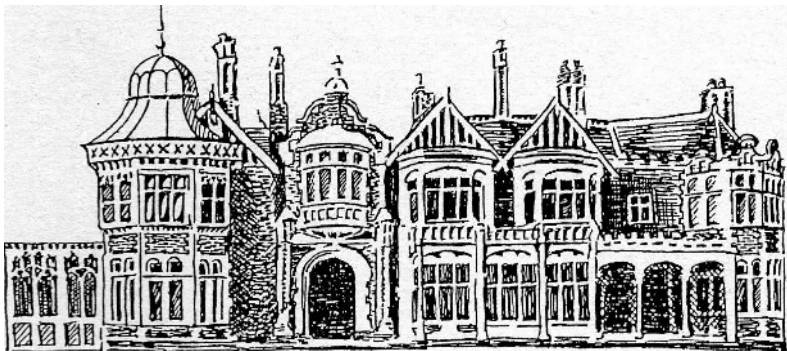
**by John Gallehawk**

This booklet, which is based upon a Bletchley Park Lecture given in January 1998, describes three situations that came very close to revealing the Allies most precious secret in World War II, the ULTRA intelligence based on the decryption of the German Enigma cipher messages.

## **CONTENTS**

3	The U-boat War in the Atlantic
6	American and Canadian waters
9	The Invasion of Crete
15	Back at Base
17	Sources
18	Figures 1 - 10

The Bletchley Park Reports



# The Admiralty Operational Intelligence Centre

by

Peter Jarvis

**Report No.20**

**June 2003**

## Contents

Introduction	4
The Admiralty	4
Setting up the OIC from 1937	5
Incoming information	9
Weaknesses of both sides	10
B-dienst; German codebreaking	11
Y service (radio interception)	12
The Submarine Tracking room	13
Collaboration between German Navy and Air Force	13
Intelligence as an aggressor	15
Intelligence without SIGINT	15
Joint Intelligence and the Invasion of Europe	17
Political self-deception	19
Rotation of Staff	19
Conclusions; Abolition of the Admiralty	20
N.I.D. Policy, 1942	21 by <i>Rear Admiral J.H. Godfrey R.N.</i>
Acknowledgements	26
Bibliography	26



## The Bletchley Park Trust Reports



# The first Breaking of Enigma

Some of the pioneering techniques  
developed by the Polish Cipher Bureau

by

Frank Carter

Report No.10 July 1999

# Table of Contents

1.	Introduction and Preamble	3
2.	The Polish Catalogue Method	
i	Mathematical Theory	5
ii	The Cyclometer	8
iii	A modern reconstruction of the Polish Catalogue	10
iv	Summary	11
v	Finding the 'Stecker' connections	12
3.	New Problems confronting the Poles	
	The discovery of some useful message key characteristics	13
4.	The Polish Bomba	
i	Principles of operation	14
ii	Electrical configuration	16
iii	Limitations on its use	16
5.	The Zygalski Perforated Sheets	
i	Introduction - another riile for the cyclometer	17
ii	The theoretical background	17
iii	Their practical design	21
iv	A modern illustrative example of their use	22
6.	Supplementary notes on the mathematics	23
7.	Appendices	
i-ii	Some illustrative permutation cycles	27-28
iii	The theoretical probability of a 'fernale'	29
iv-viii	Zygalski sheets - illustrative examples	30-34

Note: To appreciate the content of this publication, some prior knowledge of the Enigma machine is required, together with the operational procedures that were used with it.

The Bletchley Park Trust Reports



# The Turing Bombe

An account of how the machine  
functioned, together with some  
illustrative examples.

(Second edition, revised and enlarged.)

by

Frank Carter

Report No. 16 September 2001