Catalogue of the papers and correspondence of

Donald Watts Davies FRS

(1924-2000)

By Peter Harper and Timothy E. Powell

NCUACS catalogue no.143/8/05

Title:	Catalogue of the papers and correspondence of Donald Watts Davies (1924-2000), computer scientist
Compiled by:	Peter Harper and Timothy E. Powell
Date of material:	1936-2004
Extent of material:	*ca* 850 items
Deposited in:	College Archives, Imperial College London
Reference code:	GB 0098 B/DAVIES

NCUACS catalogue no. 143/8/05

The work of the National Cataloguing Unit for the Archives of Contemporary Scientists in the production of this catalogue is made possible by the support of the following societies and organisations:

Biochemical Society

British Computer Society

Institute of Physics

Needham Charitable Trust

Royal Society

Royal Society of Chemistry

Trinity College Cambridge

Wellcome Trust

NOT ALL THE MATERIAL IN THIS COLLECTION
MAY YET BE AVAILABLE FOR CONSULTATION.
ENQUIRIES SHOULD BE ADDRESSED IN THE
FIRST INSTANCE TO:

THE COLLEGE ARCHIVIST
IMPERIAL COLLEGE, LONDON

LIST OF CONTENTS

GENERAL INTRODUCTION

PROVENANCE

The papers were received from the family of Mr Donald Davies in June 2004.

OUTLINE OF THE CAREER OF DONALD WATTS DAVIES

Donald Watts Davies was born in Treorchy in the Rhondda Valley in Wales on 7 July 1924. In July 1925 his father died and Davies moved with his mother and twin sister to Portsmouth to live with his maternal grandmother and aunt. In 1941, on the completion of his school education at the Portsmouth Boys Southern Secondary School, he took up a 'Royal' Scholarship at Imperial College London where he studied physics. In 1943 he graduated with first-class honours and was directed to work at Birmingham University as a research assistant in the Tube Alloys Project (the British contribution to the development of nuclear weapons) under R.E. Peierls and later A.H. Wilson. Davies's main work was concerned with the stability and control problems for the gaseous diffusion plant. In 1944 he continued to work for the Tube Alloys Project at ICI, Billingham, on Teeside and in 1945 at the close of the project he returned to Birmingham to work in the Physics Department under M.L.E. Oliphant. The overlap between the courses at Imperial College allowed Davies to complete the requirements for a mathematics degree in a year and he resumed the scholarship for that purpose, graduating with first class honours in 1947.

The National Physical Laboratory was setting up a group to build a stored program computer under the direction of A.M. Turing and Davies joined this group and began working on the logic design and later the building of the ACE Computer. When the Pilot ACE was built, Davies became a user, working on a variety of simulations, including the behaviour of road junctions controlled by traffic lights. In 1954 Davies was awarded a Harkness Fellowship to study in the USA. He came to view his choice of MIT as an error because all the interesting computer work was classified. The period at MIT was interrupted by a special mission for the United Nations, investigating a request from the Indian Statistical Institute, Calcutta for funds to buy equipment from the USSR. Subsequently he was involved for a number of years on two new projects. One was the development of the cryotron, a superconducting device with potential for the large-scale integration of logic and storage. However, efforts in this area foundered on engineering problems of many kinds. The other was the translation by computer from Russian to English. Davies concluded that although 'we were not able to set up a service based on this work ... it is noteworthy that our real experience ... was very different from the accepted public view of machine translation'.

In the early 1960s time-sharing whereby a large computer gave an online service to a number of users was very much the coming thing. In 1965 Davies proposed, in a privately circulated paper, the principle for a data communication network which he subsequently named 'packet switching'. In March of the following year he lectured to a large audience, advocating the use of this technique in a public switched data network. In 1966 Davies was appointed Superintendent of the Division of Computer Science where the programme of research included data communication systems, information systems, pattern recognition and man-computer interaction. The data communication proposals for specialised networks using packet switching were widely publicised in 1967 and greatly influenced the early development of the ARPA Network. Davies successfully promoted packet switching for public networks at the CCITT (International Consultative Committee for Telephones and Telegraphs) and elsewhere. In 1973 he published (with D.L.A. Barber) *Communication Networks for Computers* and in 1979 (with Barber, W.L. Price and C.M. Solomonides) *Computer Networks and their Protocols*. In 1975 Davies received the John Player Award of the British Computer Society for his work in packet switching and shared the IEEE (Institute of Electrical and Electronics Engineers) Internet Award for 2000 for work on packet switching.

In 1978 Davies was given the status of an 'individual merit' appointment at the NPL enabling him to relinquish administrative responsibilities, and he led a small research team concerned with security of data in networks. The team developed the application of cryptographic methods to the practical work of network security, especially the use of asymmetric (public key) cryptography. Consulting work under contract to financial institutions and others provided the practical experience. After Davies retired from the NPL in 1984, he provided consultancy to financial institutions on high value payment systems and advised suppliers and users of secure systems of many kinds, for example mobile telephony and direct broadcast satellite television. In 1984 he published (with W.L. Price) *Security for computer networks: an introduction to data security in teleprocessing and electronic funds transfer.* Davies also pursued his interests in cryptography as a hobby with research on Second World War cipher machines and published a number of articles on the topic.

Davies was appointed CBE in 1983 and elected to the Fellowship of the Royal Society in 1987.

In 1955 Davies married Diane Burton with whom he had three children. He died on 28 May 2000.

This biographical account draws on Davies's curricula vitae and similar material which form part of the archive collection and on the memoir by Roger M. Needham, 'Donald Watts Davies, C.B.E.', *Biographical Memoirs of Fellows of the Royal Society*, volume 48 (2002), 89-96.

DESCRIPTION OF THE COLLECTION

The material is presented in the order given in the List of Contents. It covers the period 1936-2004.

Section A, Biographical, is not extensive. An overall sense of Davies's life and work is provided by the contents of his 'Personal' folder of biographical notes, curricula vitae, lists of publications, examples of projects undertaken, etc. There is a little material recording Davies's schooling and university education and some documentation of his career. An unusual insight into the companies for which Davies acted and individuals with whom he came into contact later in his career is given by a collection of his business cards, some annotated. Also documented in this section is Davies's interest in various types of puzzles. There is a little posthumous material, including obituaries. As a number of biographical papers have been retained in family hands, some of the material is photocopy only.

Section B, Research, is the largest in the collection. These materials were found in Davies's labelled 'transfer cases' or box files which form the basic unit of organisation. There is a sequence of 'Notes of Miscellaneous Scientific Work', covering an extended period, 1952-1996. The contents of many of the containers relate to Davies's security interests with material from the 1970s onwards, for example 'Data Security MS Notes', 1978-1984 and 'Public Key Ciphers' (two containers), 1970-1997. Papers relating to packet switching are to be found in Section F Historical Topics.

Section C, Lectures and publications, presents sequences of papers designated by Davies as either lectures or publications. The lectures sequence covers a relatively short period, 1990-1995, and relates to computer history and security questions. The publications material covers a much more extended period, 1956-2000, and includes off-prints, photocopied papers and copies of the journals in which publications by Davies appeared. There may be additional material relating to Davies's lectures and publications in other sections of the catalogue, especially Research and Historical topics and Correspondence.

Section D, Societies and organisations, is not extensive comprising just four bodies, covering the period 1987-2000: British Computer Society, International Council for Computer Communication (ICCC), Royal Society and Worshipful Company of Information Technologists.

Section E, Consultancies, provides documentation, 1986-1998, relating to a small number of consultancies which Davies held after his retirement from the National Physical Laboratory.

Section F, Historical topics, presents important documentation of some of Davies's most important research, such as packet switching, as well as interests he pursued in his spare time such as Second World War cipher machines. These materials were found in Davies's labelled 'transfer cases' or box

files which form the basic unit of organisation. There are interesting records relating to early computers organised in relation to a meeting held to celebrate the 50th anniversary of the Pilot Model ACE (Automatic Computing Engine) in the year 2000. Packet switching is represented by a sequence 'Historical Notes / Early Packet Switching etc', 1949-2000, which includes copies of original documentation and historical reflections by Davies and others. There is an extensive record of Davies's interests in the history of cryptography including correspondence with others who shared his interests, typescript drafts of articles by Davies, photographs and photocopies of original documentation. Also represented in the section are Davies's interests in the history of the National Physical Laboratory itself and the Turing Machine

Section G, Correspondence, is not extensive and is presented in four sequences. The first is the contents of Davies's folder of 'Misc. Correspondence', 1970-2000. Although the great bulk comes from the last fifteen years of Davies's life, the sequence also includes three letters from Sara Turing, mother of Alan Turing, 1970-1971. There are also separate sequences of correspondence with W.W. Mache, 1991-2000, relating principally to their mutual interest in Second World War German cipher machines; of publications correspondence, 1988-1999; and of correspondence relating to a patent case, 1994-2001.

There is also an index of correspondents.

Some biographical papers and photographs are retained in family hands.

P. Harper
T.E. Powell
Bath 2005

SECTION A **BIOGRAPHICAL, A.1-A.43** **1936-2004**

A.1-A.15 **'PERSONAL'**

Contents of Davies's folder so inscribed divided into fifteen for ease of reference: biographical notes, curricula vitae, lists of publications, examples of projects undertaken, etc.

At A.14 is Davies's 'short diatribe on the matter of how kilometre should be pronounced'.

A.16-A.18 **EDUCATION** **1936-1940s**

A.16 Portsmouth Southern Secondary School for Boys School Reports

Photocopies. Originals retained by family.

The reports cover Davies's secondary education 1936-1941.

Biographical, A.1-A.43

A.17, A.18 Imperial College London

In 1941 on the completion of his school education at the Portsmouth Boys Southern Secondary School, Davies took up a 'Royal' Scholarship at Imperial College London where he studied physics, graduating in 1943 with first class honours. After war work Davies took advantage of the overlap between the courses at Imperial College which allowed him to complete the requirements for a mathematics degree in a year. He resumed the scholarship for that purpose, graduating with first class honours in 1947.

A.17 Binder of notes N.d.

Inscribed with Davies's name and address in Southsea, Hampshire inside front cover.

Contents include contents list and from page 1 notes on ? lecture course by Dr Kebby on 'Differential Equations in Mathematical Physics'.

A.18 Softback notebook N.d.

With Imperial College Bookstall label on front cover where the name given is 'Roth' and the date 'Post-Grad'.

Used for notes on mathematics topics.

Leonard Roth was a member of the Mathematics Department at Imperial College, 1931-1965.

A.19 CAREER 1941-1987

Photocopied pages from photograph album used for newspaper cuttings and photographs documenting Davies's career over this period.

Album retained in family hands.

Biographical, A.1-A.43

A.20, A.21	**ARTICLES ABOUT DAVIES'S CAREER**	**N.d., 1998**
A.20	'Packet switching: the history lesson', *The Guardian* Photocopy of article by Davies.	N.d.
A.21	'Almost an accident', *IEE Review*, July 1998 Typescript draft of interview with Davies and copy of the *IEE Review* in which the interview appeared.	1998
A.22	**OPEN UNIVERSITY** Papers *re* Open University courses taken by Davies.	**1991-1997**
A.23-A.35	**'PUZZLES'** Contents of folder so inscribed divided into thirteen for ease of reference: papers *re* Davies's longstanding interest in puzzles. Includes correspondence, programs, photographs, catalogues, manuscript working, etc.	**1973-1995**
A.36-A.39	**PHOTOGRAPHS**	**1961, 1972, n.d.**
A.36	Group photograph taken at the Symposium 'Machine Translation of Languages and Applied Language Analysis', NPL, Teddington, Middlesex, UK With key.	1961
A.37	Group photograph of staff of Davies's National Physical Laboratory Division	N.d.

Biographical, A.1-A.43

A.38, A.39	Copies of a selection of the photographs retained in family hands	
A.38	Copies of six photographs taken at Post Office (1972), National Physical Laboratory and Science Musem London occasions Includes portrait photograph of Davies and group photograph of computer pioneers including Grace Hopper and Konrad Zuse.	1972, n.d.
A.39	Copies of five photographs illustrating early computer history at the National Physical Laboratory The original photographs were lent to the BBC and returned to Davies in 1992.	N.d.
A.40	**BUSINESS CARDS**	**N.d.**
	Three bundles in original envelope.	
A.41-A.43	**POSTHUMOUS MATERIAL**	**2000-2004**
A.41	Obituaries: *The Times*, 31 May 2000. Martin Campbell-Kelly, *The Guardian*, 2 June 2000. Jack Schofield, *The Independent*, 7 June 2000. 'Metromnia' [NPL Newsletter], Summer 2000.	
A.42	Biography of Davies from 'The History of Computing Project' website	2001

Biographical, A.1-A.43

A.43	Reports on tributes to Davies:	2003, 2004
	Plaque in honour of Davies, Treorchy, 2003.	
	Imperial College Donald Davies Prize for best final year project by a student of Mathematics and Computing, 2004.	

SECTION B **RESEARCH, B.1-B.313** **1952-1999**

The materials presented in this section were kept by Davies in a number of 'transfer cases' and box files with labels indicative of their content. These containers have been used as the basic unit of organisation of the section.

The contents of the containers are presented in the order found. This may mean that later material comes first and earlier material towards the end of the sequence though this is rarely a straightforward reverse chronological sequence. The technical nature of the papers and the frequency of undated material makes the reordering of material unsafe. The contents are therefore divided only for ease of reference.

The materials comprise typescript and manuscript notes and drafts by Davies, calculations, computer print-outs, technical drawings, correspondence including printed-out emails and much background material including papers by others, often with annotations or manuscript notes by Davies attached.

The first container presented here covers many aspects of his work at the National Physical Laboratory from the early 1950s although described by Davies simply as 'Notes of Miscellaneous Scientific Work'. This is followed by a sequence of containers presented in alphabetical order by topic or topics as indicated on the labels.

B.1-B.41	'Notes of Miscellaneous Scientific Work' Contents of transfer case so labelled.	1952-1996
B.1	Technical drawings *re* noughts and crosses machine	1957
B.2	Correspondence with M.L. Minsky *re* article by Minsky on universal Turing machines with Davies's manuscript notes and copies of article by Minsky and of Turing's 1937 article on computable numbers	1964
B.3	Contents of Davies's plastic folder: correspondence and papers *re* article by Davies and R.B. Standler on ball lightning including off-print of published article, *Nature*, vol. 240, p. 144, 17 November 1972	1970, 1972, n.d.

Research, B.1-B.313

B.4	Includes typescripts by Davies on 'Packing a Circular Suitcase' and 'Theories of Games', also headed 'For NPL News' and 'Article for NPL News', respectively	1976, n.d.
B.5	Includes six photographs of oil rings	N.d.
B.6	'Non-Blocking Switching Networks' Photocopied manuscript, n.d. and typescript copy, 3 December 1996. Davies explains at the head of the typescript copy: 'This note was written some time in the fifties or sixties and has been transcribed from an almost illegible photocopy of a manuscript.	1950s or 1960s, 1996
B.7	Includes letters '76:10:28' and 9 May 1979	1976, 1979
B.8	Computer print-out, calculations	N.d.
B.9	Illustrative material for publication or lecture	N.d.
B.10	Computer print-out, calculations, etc	N.d.
B.11	Photocopied material from a published source	N.d.
B.12	Manuscript draft on 'Dijkstras Generalisation of the 'Dining Philosophers' Problem'	N.d.
B.13	'Simplified Description of Implicit Sort of Survey Point Numbers' Typescript by 'Maurice Cox DNACS, NPL 13/12/78'.	1978
B.14	Two sequences of manuscript notes by Davies 'Etymological Lessons' and 'Some Useful Kanji Characters'	N.d.

Research, B.1-B.313

B.15	Untitled typescript draft ?by Davies beginning 'Given a connected graph and one of the nodes as starting point, a path is defined which traverses all edges of the graph exactly twice and ends at the starting point'	N.d.
B.16	Includes manuscript draft by Davies 'The Poisson Distribution and a Simple Queuing Problem'	N.d.
B.17	'Notes on Some Work on an Algebraic Treatment of Graphs' by Hsu Kung-shih, Autonomics Division, National Physical Laboratory, December 1965	1965
B.18	'Programming Project', photocopied typescript by D.A. Bell, October 1971	1971
B.19	Photocopied papers by others	1973, 1974
B.20	'On-the-fly garbage collection A method devised by Dijkstra, Lamport, Martin, Scholten and Steffens (EWD496, 30 May 1975)'	1975
B.21	Photocopied typescript 'Simple example of "functional segregation" ', manuscript working	N.d.
B.22	Photocopied article on mathematical games	1971
B.23	Manuscript notes *re* 'Poisson arrivals ...'	N.d.
B.24	Manuscript workings: 'Fourier transforms' 'Power Spectrum of a "Periodic" message-carrying wave' ? bibliographic reference 'Nov 1958'.	c.1958, n.d.

Research, B.1-B.313

B.25	Includes manuscript and typescript drafts titled 'Calculations of the Spectral Density at HDB3'	N.d.
B.26	Miscellaneous manuscript notes including 'Power Spectra Etcetera' and 'Electronic Computers at N.P.L: Chronology' The chronology begins in 1945 with Turing joining the staff of the NPL and continues in the same style to 1952 with a final note 'Deuce delivered May ? 1955'	N.d.
B.27	Manuscript and typescript notes: 'Sprouts program', 'Address Mechanism of XL12', 'Address Mechanism of PDP8', etc	N.d.
B.28	Manuscript notes: 'Effect of Fan-in / Fan-out on Reliability of Triplicated Systems', 'Transistor Geometries - Electronics Sept 29 1961', 'Fairchild Micrologic Lecture by Dr Robert Norman 13 December 1961', 'Features of the SIMBOL Language', etc	1961, n.d.
B.29	Includes manuscript note for Davies from P. Vigoureux, 26 October 1964, and off-print of short paper by Vigoureux on 'Electromagnetic levitation forces', 1965	1964-1965, n.d.
B.30	Manuscript notes: 'Electronic Combination Lock', 'Average Number of Runs in a Random Time Series', etc Includes bibliographic reference, 1964.	c.1964, n.d.
B.31	Manuscript draft titled 'The Universal Calculating Machine'	N.d.
B.32	Manuscript notes headed 'Nanosecond Pulse Transformers' Include bibliographic reference 1959.	1959 or later
B.33	Manuscript notes titled 'Elementary Problem in Theory of Games - Two Salesmen'	N.d.

Research, B.1-B.313

B.34	Correspondence and papers *re* puzzles published in the *New Scientist*	1962-1963
B.35	Manuscript notes: 'Helices for Offset Right-Angle Bends (A hypothetical plumber's problem)' and 'Conical Problem'	N.d.
B.36	Manuscript drafts: 'Multiple Reflection Delay Lines based on the Diagonals of a Cube' and 'Information Preserving Transformations of 2 binary channels to give minimum ones'	N.d.
B.37	Manuscript notes and drafts: 'Directional Rotation Signals', 'Reversible Linear Transformations of Three Binary Variables' and 'Error Correcting Codes' The draft on error correcting codes includes bibliographical reference January 1956.	N.d. , c. 1956
B.38	Includes circuit diagram and off-print	1952-1953
B.39	Miscellaneous manuscript notes, NPL Electronics Section Information sheets	N.d , 1956
B.40	Patent specification for 'Electronic Pulse Counting Circuits' Complete specification was published 20 July 1955. Davies was the inventor	1955
B.41	NPL Autonomics Division off-print on 'The Hexagonal Floor Pattern'	N.d.
B.42-B.62	'Data Security MS Notes' Contents of transfer case so labelled.	1978-1984, n.d.
B.42	Manuscript notes: 'The apparent impossibility of a time-memory trade-off in the repeated encipherment attack on	1978

Research, B.1-B.313

RSA', 'The Complementary Property of the DES [Data Encryption Standard]', etc.

B.43 'Bibliography of public key cryptosystems' c.1978

Latest bibliographical reference, 1978.

B.44 Typescript draft titled 'Limits to Computation' with manuscript inscription at the top of the first page 'From D.W. Davies, NPL' c.1978

Undated but includes reference to 'Professor Hellman's lectures to Infotech in October / November 1978'

B.45 Manuscript draft titled 'The control of operations on keys by tagging keys with a "type" '. c.1978

Undated but includes bibliographical reference, 1978.

B.46 Typescript draft titled 'The Birthday Problem', 7 November 1978 and related papers 1978

B.47 Manuscript draft titled 'Some properties of random functions', signed by Davies and dated '25.11.78' 1978

B.48 Untitled manuscript notes, one sheet dated '16.5.79' 1979

B.49 Typescript note titled 'Some structure in the "transpositions" used in the DES', 30 May 1979 1979

B.50 Typescript note titled 'An evaluation of Public Key Cryptosystems Addendum at June 1979' 1979

B.51 Typescript draft by Davies and G.I.P. Parkin titled 'The Average Cycle Size of the Key Stream in Output Feedback Encipherment' 1981 or later

/...

Research, B.1-B.313

/...	Latest bibliographical reference, 1981	
B.52	Typescript draft titled 'The So-Called "Weak" Keys of the Data Encryption Standard (DES) Algorithm' Signed by Davies and dated '18.2.'83'.	1983
B.53	Typescript paper by D.A. Bell titled 'The "Guardian" Technique for Document Protection', 23 January 1984 and typescript paper by Davies titled 'Donald Bell's "Guardian" ', 13 February 1984 Donald A. Bell was Director of the National Engineering Laboratory, East Kilbride.	1984
B.54	Manuscript notes: 'Transformations of the DES algorithm for software implementation', 'Lecture Bristol (Revised)', 'Ralph C. Merkle Some communications over insecure channels', etc	N.d.
B.55	Typescript paper titled 'A simple introduction to Galois fields'	N.d.
B.56	Manuscript notes: 'Software Security', 'Time-memory trade-off for analysis of the RSA Cipher', 'Time-memory trade-off for the discrete exponential', 'Treatment of final short blocks in cipher block chaining', etc.	N.d.
B.57	Manuscript and typescript notes: 'Sixteen funny keys for the DES', 'Quadratic residues', etc.	N.d.
B.58	Typescript draft titled 'Some Regular Properties of the "Data Encryption Standard" Algorithm'	N.d.
B.59	Manuscript notes: 'A problem related to the Birthday Problem', 'One-way Function Derived from the DES', 'Cryptanalysis problem - to find a plaintext P given n enciphered values', etc	N.d.

Research, B.1-B.313

B.60	Typescript drafts: 'The authentication of transactions' and 'A note on passwords'	N.d.
B.61	Figures	
B.62	Manuscript and typescript drafts by colleagues	1981, n.d.
B.63-B.78	'Elliptic Curves European Scrambling Syst. Misc. Crypto' Contents of transfer case so labelled divided into sixteen for ease of reference: principally duplicated and printed background material. Includes pages printed from the web. 16 folders. Manuscript working by Davies is at B.67 and typescripts by Davies at B.68, B.71, B.73, B.75-B.77 *re* Videocrypt system, attacks on smart cards, architecture for trusted third parties, linear and differential cryptanalysis, etc.	1993-1998
B.79-B.88	'Hash functions' Contents of box folder so labelled divided into ten for ease of reference: printed and duplicated background material. At B.80 is a typescript by Davies titled 'Collision-Free Functions and Damgard's Principle'.	1988-1996
B.89-B.109	'Key MGT [Management] & Encipherment US + ISDN etc' Contents of transfer case so labelled divided into twenty-one for ease of reference: printed and duplicated background material, with some annotation, manuscript notes by Davies (see especially B.101).	1974-1988
B.110-B.134	'Number Theory and Algorithms' Contents of transfer case so labelled.	1974-1999
B.110	Typescript draft by Davies titled 'A Brief Tutorial on Elliptic	1996

Research, B.1-B.313

	Curves'	
B.111-B.112	Background papers including pages printed from the web Two folders.	1996-1999, n.d.
B.113	Typescript draft by Davies titled 'The Significance of New Methods for Factoring Large Numbers', February 1990; background papers	1982-1990
B.114	Correspondence, manuscript notes, typescript draft titled 'The Need for Selecting Primes used for the RSA Modulus', etc	1974-1990, n.d.
B.115	NPL Technical Memorandum TTCC 25/86 by Davies titled 'Fast RSA Operations using the Chinese Remainder Theorem', November 1986	1986
B.116	Includes copy of manuscript letter from Davies, 6 February 1990: 'I am sending 'a brief report on the "number sieve" method of factoring large numbers ...'	1990, 1994
B.117	Typescript draft by Davies titled 'Evaluation of Odlyzko's Projection for the Future of Factoring'	1996
B.118	Includes photocopied 'preliminary draft' of paper by A.M. Odlyzko on the future of integer factorization and discrete logarithms	1995-1996
B.119	Typescript draft by Davies titled 'Minimum Difference between the Factors of an RSA Modulus', November 1994 and copy of letter from Davies on the same topic, 8 April 1995	1994-1995
B.120	Letter from J.M. Pollard on 'State of the Number Field Sieve', 23 October 1992 and background papers including copies of manuscript notes on quadratic sieve by 'DH'	1982-1993

Research, B.1-B.313

[Don Hunter], May-June 1993

B.121	Duplicated and printed background papers	1978-1988
B.122	Includes manuscript notes by Davies on 'Carmichael Numbers'	N.d.
B.123	Includes correspondence	1986-1987
B.124	Duplicated papers including 'Postscript to my letter of 29 June' from J.M. Pollard, 25 July 1985	1985
B.125	Duplicated papers, manuscript notes by Davies	N.d.
B.126-B.127	Duplicated papers Two folders. B.127 includes a little correspondence.	1975-1984
B.128	Papers *re* 'Crypto 83 A Workshop on the Theory and Application of Cryptographic Technique', University of California, Santa Barbara, 21-24 August 1983': programme, letter from C.P. Schnorr *re* submitted paper and Davies's report on the meeting	1983
B.129-B.134	Duplicated and printed papers Six folders. B.132 includes manuscript notes from J.M. Pollard, August 1982.	1977-1983
B.135-B.145	'Programmes' Contents of folder so labelled.	1984-1995, n.d.

Research, B.1-B.313

B.135	Computer print-outs	N.d.
B.136	Computer print-outs, typescript draft by Davies titled 'An Algorithm for a Cryptographic Sum'	N.d.
B.137	Computer print-outs	N.d.
B.138	Typescript draft by Davies titled 'Proposed cryptographic check algorithm for Lanis and Gyr'	N.d.
B.139	Typescript draft by Davies titled 'Testing an S-Box for Absence of Linearity', August 1995, computer print-outs	1995
B.140	Typescript draft by Davies 'Proposed Cryptographic Check Algorithm for Landis and Gyr', July 1995, computer print-outs	1995
B.141	Computer print-outs	N.d.
B.142	Computer print-outs	N.d.
B.143	Computer print-outs	1984-1985
B.144	Computer print-outs	N.d.
B.145	Typescript draft by Davies and D.G. Clayden titled 'A Message Authenticator Algorithm for an 8-Bit Microprocessor', 27 January 1984, manuscript notes	1984
B.146-B.162	'Public Key Ciphers Part 1'	1970-1982
	Contents of box folder so labelled divided into seventeen	

Research, B.1-B.313

for ease of reference: duplicated and printed background papers.

B.159 includes manuscript notes by Davies.

B.163-B.184 'Public Key Ciphers Part 2 except Signature Number theory' 1976-1997

Contents of transfer case so labelled divided into twenty-two for ease of reference: predominantly duplicated and printed background papers.

At B.164 is typescript draft by Davies titled 'Brief Statement of the LUC Cipher', 5 November 1992.

At B.167 is typescript draft titled 'Minimum Difference between the Factors of an RSA Modulus', November 1994.

At B.179 is 'Crypto 84 - Report by D.W. Davies'.

B.181 includes manuscript notes by Davies.

B.185-B.190 'S.E.T.[Secure Electronic Transaction] + slides + Internet Open Trading' 1997-1998, n.d.

Contents of transfer case so labelled: predominantly background material.

Three bound volumes and three folders.

At B.188 is illustrative material ? for presentation by Davies.

B.191-B.212 'Signatures Authentication Log-on' 1978-1992

Contents of transfer case so labelled

B.191-B.192 Duplicated background papers 1980-1992

Two folders.

B.193 Typescript draft by Davies titled 'El Gamal's Signature', 25 April 1990 1990

Research, B.1-B.313

B.194	Typescript draft by Davies titled 'The Zero-knowledge Protocol of Guillou and Quisquater'	N.d.
B.195-B.197	Duplicated and printed background papers Three folders.	1984-1989
B.198	Includes manuscript notes by Davies	1982-1983, n.d.
B.199	Includes manuscript notes by Davies including sheet headed 'A Note on"Sedlak's Condition" ', signed by Davies and dated 8 March 1987	1985-1987
B.200-B.202	Duplicated and printed background papers Three folders.	1979-1984
B.203	NPL Technical Memo TTCC 11/83 by Davies titled 'Digital Signatures Using Approximation by Quadratic Forms', August 1983	1983
B.204	NPL Technical Memo TTCC 27/86 by Davies titled 'Registration of Public Keys for a large number of terminals', November 1986	1986
B.205	Manuscript notes by J.M. Pollard, 17 May 1984, attached to paper by H. Ong, C.P. Schnorr and A. Shamir which is annotated on its first page by Davies	1984
B.206	Typescript draft by Davies titled 'Further Developments in Public Key Signatures', 9 January 1984 with sheet of manuscript notes attached and manuscript notes etc by J.M. Pollard, 14 April 1984	1984
B.207	Includes typescript draft by Davies titled 'Update for the Paper Digital Signatures Using Approximation by	1983, n.d.

Research, B.1-B.313

	Quadractic Forms'	
B.208-B.212	Duplicated and printed background papers Five folders	1978-1983
B.213-B.248	'TTCC [Tokens and Transactions Control Consortium] Published Notes etc + DITC [Division of Information Technology and Computing] + MAA [Message Authenticator Algorithm]' Contents of box folder so labelled. Principally NPL technical memoranda and reports by Davies and others.	1982-1992
B.213	NPL Report TTCC 3/82 by Davies and W.L. Price titled 'Security of Tokens used for Identification', July 1982	1982
B.214	NPL Report TTCC 4/82 by Davies titled 'Tokens used for the Storage and Transport of Keys', July 1982	1982
B.215	NPL Report TTCC 5/82 by Davies and W.L. Price titled 'Security of Tokens used for Identification Supplementary Report', October 1982	1982
B.216	NPL Report DITC 17/83 by Davies and D.O. Clayden titled 'A Message Authenticator Algorithm Suitable for a Main Frame Computer', February 1983	1983
B.217	NPL Report TTCC 9/83 by Davies titled 'The Use of Tokens to Store Data and Control Access to Stored Data', April 1983	1983
B.218	NPL Report TTCC 10/83 by Davies titled 'Recent Developments in Public Key Cryptosystems', June 1983	1983
B.219	NPL Technical Memo TTCC 11/83 by Davies titled 'Digital	1983

Research, B.1-B.313

	Signatures Using Approximation by Quadratic Forms', August 1983	
B.220	NPL Technical Memo TTCC 12/83 by Davies titled 'Use of the "Signature Token" to create a negotiable document', August 1983	1983
B.221	NPL Technical Memorandum TTCC 24/86 by Davies titled 'A General Description of the Transaction Key Method', June 1986	1986
B.222	NPL Technical Memorandum TTCC 25/86 by Davies titled 'Fast RSA Operations using the Chinese Remainder Theorem', November 1986	1986
B.223	NPL Technical Memorandum TTCC 26/86 by Davies titled 'Chaining Methods for RSA Encipherment and Signature', November 1986	1986
B.224	NPL Technical Memorandum TTCC 27/86 by Davies titled 'Registration of Public Keys for a large number of terminals', November 1986	1986
B.225	NPL Technical Memorandum TTCC 28/86 by Davies titled 'Tokens for Personal Identity Verification', November 1986	1986
B.226	NPL Technical Memorandum TTCC 30/87 by Davies titled 'Fiat and Shamir's Methods for Identification and Signature'. 'Revised' June 1987	1987
B.227	NPL Technical Memorandum TTCC 31/87 by Davies titled 'A Proposed Standard for Digital Signature of Multi-Block Messages', June 1987	1987
B.228	NPL Report DITC 109/88 by Davies and D.O. Clayden titled 'The Message Authenticator Algorithm (MAA) and its Implementation', February 1988	1988

Research, B.1-B.313

B.229	NPL Technical Memorandum TTCC 50/88 by Davies titled 'An Investigation of the Effect of "False Witnesses" on the Reliability of Algorithm P', October 1988	1988
B.230	NPL Technical Memorandum TTCC 51/88 by Davies titled 'Further Results Concerning False Witnesses in Algorithm P', October 1988	1988
B.231	NPL Technical Memorandum ATTC [Advanced Token Technology Club] 01/89 by Davies titled 'The Security of the "Message Authenticator Algorithm" ISO 8731-2', March 1989	1989
B.232	NPL Technical Memorandum ATTC 03/89 by Davies titled 'The Need for Selecting the Primes used for the RSA Modulus', March 1989	1989
B.233	NPL Technical Memorandum ATTC 04/89 by Davies titled 'Fixed Points in the RSA Cipher', March 1989	1989
B.234	NPL Technical Memorandum ATTC 02/89 by Davies titled 'A Review of Eurocrypt '88 and Crypto '88 Papers', June 1989	1989
B.235	NPL Technical Memorandum ATTC 07/89 by Davies titled 'Schnorr's Exponential Signature Method and New Random Number Generator', November 1989	1989
B.236	NPL Technical Memorandum ATTC 08/89 by Davies titled 'A Review of Eurocrypt '89 and Crypto '89 Papers', November 1989	1989
B.237-B.245	NPL Reports and Technical Memoranda in which Davies does not appear as an author Nine documents.	1982-1989

Research, B.1-B.313

B.246-B.248	Duplicated background papers Three folders	1992
B.249-B.282	'Zero Knowledge / RSA Program / Life Program' Contents of transfer case so labelled.	1983-1995
B.249-B.254	Duplicated and printed background papers Six folders.	1986-1995
B.255	NPL Technical Memorandum TTCC 49/88 by Davies titled 'New Forms of Digital Signature using the Fiat-Shamir Principle', April 1988	1988
B.256-B.258	Duplicated background papers Three folders.	1986-1988
B.259	Manuscript notes, typescript draft by Davies 'The Zero-knowledge Protocol of Guillou and Quisquater'	N.d.
B.260-B.268	Contents of unlabelled plastic folder divided into nine for ease of reference: computer print-outs annotated by Davies, typescripts by Davies, duplicated background papers etc *re* the game 'Life' invented by J.H. Conway	1983, n.d.
B.269	Computer printout with manuscript inscription 'ASSY 14 May '84'	1984
B.270	Typescript draft by Davies titled 'RSA Program for the BBC Microcomputer', 'Copyright 1984'	1984
B.271	Computer printout with manuscript inscription 'RSA 14 May '84'	1984

Research, B.1-B.313

B.272	Typescript draft ? by Davies titled 'Version RSAY dated July 1986'	1986
B.273	Figures, manuscript notes, computer printout, etc	N.d.
B.274	'RSA Keys for Signature with Public Exponent 3', 7 September 1993	1993
B.275	Computer printout with manuscript inscription 'RSAY'	N.d.
B.276	Letter from D.G.N. Hunter, 27 July 1986, etc	1986
B.277	Computer printout with manuscript inscription 'RSA', manuscript notes, etc	1984, n.d.
B.278	Manuscript notes, computer printout	1984, n.d.
B.279	Computer printouts with manuscript inscriptions 'PKSF', 'RSA', 'ASSY', etc	N.d.
B.280	Computer printouts with manuscript inscriptions 'RSA' and 'PKS'	N.d.
B.281	Computer printout with manuscript inscription 'RSAZ renumbered'	N.d.
B.282	Duplicated papers and computer printout with manuscript inscription 'PKSF'	N.d.
B.283-B.296	'Copies of Miscellaneous Scientific Papers from Journals Plus RSA Papers and Patents'	1960-1995

Research, B.1-B.313

Contents of transfer case so labelled divided into fourteen for ease of reference: printed and duplicated background papers.

Manuscript notes by Davies are at B.288 and B.289.

B.297-B.306 — Contents of box folder divided into ten for ease of reference: predominantly printed and duplicated background papers including draft international standards. — 1977-1999

Papers at B.302-B.305 were found together in a plastic folder within the box folder.

B.301 includes typescript draft by Davies titled 'The cipher and signature of El Gamal as alternative to RSA', n.d.

B.302 includes typescript drafts by Davies titled 'The So-Called "Weak" Keys of the Data Encryption Standard (DES) Algorithm', 18 February 1983; 'Some Regular Properties of the "Data Encryption Standard" Algorithm', n.d. and 'A New Look at the DES Complementation Property and Weak Keys', December 1984.

B.307-B.313 — Contents of box folder divided into seven for ease of reference: financial telecommunications documentation. — 1982-1995

Most of the documentation is retained in the orginal covers or binders.

Manuscript notes by Davies are at B.313.

SECTION C **LECTURES AND PUBLICATIONS, C.1-C.101** **1956-2000**

C.1-C.6 LECTURES

C.7-C.101 PUBLICATIONS

C.1-C.6 **LECTURES** **1990-1995, n.d.**

'Lectures - Past'. Contents of folder so inscribed.

C.1 'Security in payment systems', Hewlett-Packard Colloquium on Information Security, Royal Holloway University of London, 19 December 1990 — 1990

Typescript and illustrative material for Davies's lecture, programme and letter *re* arrangements.

C.2-C.3 'The Transition from Mechanisms to Electronic Computers, 1940-1950', Asiacrypt '91, Japan, 11-14 November 1991 — 1991

Typescript and illustrative material for Davies's lecture, correspondence *re* arrangements, programme, list of participants, etc.

Two folders.

C.4 'Information Security in Banking', presentation to the Parliamentary and Scientific Committee, 20 July 1993 — 1993

Typescript and illustrative material for Davies's paper, 'current draft' of paper of fellow participant, background material *re* the Committee.

C.5 'Smart Card Europe', 13-14 December 1994 — 1995

Davies contributed to the discussion.

Correspondence and papers arising.

Lectures and publications, C.1-C.101

C.6	'Summary for Talk on May 20th' Typescript for talk on early NPL computer developments. See also F.37.	N.d.
C.7-C.101	**PUBLICATIONS** Contents of two containers labelled 'Own Publications or Reports' and 'Publications Part 2' presented in a single chronological sequence. The sequence includes off-prints, photocopied papers and copies of the journals in which publications appeared. C.86-C.89 are undated papers that it was not possible to assign a place in the chronological sequence. Additionally, C.90-C.101, are numbers of the journal Cryptologia in which Davies published, found separately from the papers at C.7-C.89.	**1956-2000**
C.7	'Sorting of Data on an Electronic Computer', *Proceedings Institution of Electrical Engineers*, vol. 103, part B supplement no. 1	1956
C.8	'Discussion on "Business Applications of Digital Computers', *Proceedings Institution of Electrical Engineers*, vol. 103, part B supplement no.1 Davies contributed to the discussion.	1956
C.9	'The 1956 Eastern Joint Computer Conference and Exhibition', 28 December 1956	1956
C.10	'The Limitations of Computers', *Impulse*, May 1957	1957
C.11	'Switching Functions of Three Variables', *IRE [Institute of Radio Engineers] Transactions on Electronic Computers*, Volume EC-6, December 1957	1957

Lectures and publications, C.1-C.101

C.12	'Mechanization of Thought Processes', *Nature* vol. 183, January 24, 1959	1959
C.13	'Report by D.W. Davies on the 1959 Eastern Joint Computer Conference and Visits in USA', December 1959	1959
C.14	'Electronic Digital Computers: how they work', *FBI [Federation of British Industries] Review*, March 1960	1960
C.15	'The Organization of a Russian-English Stem Dictionary on Magnetic Tape', *Language and Speech*, vol. 3, part 4, October-December 1960	1960
C.16	'A Technique for Consistent Splitting of Russian Words' (with A.M. Day), NPL Paper 23 Latest bibliographical reference, 1960.	N.d.
C.17	Language Translation by Machine', *The Times Science Review*, Winter 1961	1961
C.18	'Report on the 1961 conference on machine translation and applied language analysis', *Rev. Int. Doc.*, vol. 29, 1962, no.2	1962
C.19	'Report on a Visit to USA - June, 1962'	1962
C.20	'Parallel binary adders using the crossed-film cryotron', *Proceedings Institution of Electrical Engineers*, vol. 110, no.6, June 1963	1963
C.21	'An 11-Cryotron Full Adder', *IEEE Transactions on Electronic Computers*, vol EC-12, June 1963	1963

Lectures and publications, C.1-C.101

C.22	Review of: 'Digital Storage Computers' by W. Renwick (London:1964), *Mathematical Gazette*	N.d.
C.23	'Longest "Separated" Paths and Loops in an N Cube', *IEEE Transactions on Electronic Computers*, vol. EC-14, April 1965	1965
C.24	'Remote on-line Data Processing and its Communication Needs', 10 November 1965	1965
C.25	'Further Speculations on Data Transmission', 16 November 1965	1965
C.26	'Proposal for the Development of a National Communication Service for on-line Data Processing', 15 December 1965	1965
C.27	'Proposal for a Digital Communication Network', June 1966	1966
C.28	'New Uses for Computers', *Security Gazette*, vol. 9 no. 6, June 1967	1967
C.29	'A Digital Communication Network for Computers Giving Rapid Response at Remote Terminals', (with K.A. Bartlett, R.A. Scantlebury and P.T. Wilkinson), ACM [Association for Computing Machinery] Symposium on Operating Systems Principles, Gatlinburg, Tennessee, USA, October 1967	1967
C.30	'A Communication Network for Computers and their Remote Peripheral Devices', P.O. / Industry Joint Symposium on PCM Transmission and Switching Systems, Brighton, Sussex, 12/13 December 1967	1967
C.31	'Proposal for an Experimental Low Speed Data Communication Network', 15 July 1968	1968

Lectures and publications, C.1-C.101

C.32	'A Communication Network for Real-time Computer Systems', *The Radio and Electronic Engineer*, vol. 37, no.1, January 1969	1969
C.33	Un réseau de transmission de données à grande souplesse d'emploi', *L'Onde Electronique*, October 1969 Davies gave this paper at a Colloque International sur la Téléformatique, Paris, France, 25 March 1969.	1969
C.34	'A Decomposition Theorem for Crossbar Switching with Transient Blocking', NPL Com.Sci. T.M. 32, December 1969	1969
C.35	'Communication Networks to Serve Rapid-Response Computers', *Information Processing 1968*, North Holland Publishing Company, Amsterdam (1969)	1969
C.36	'The Principles of a Data Communication Network for Computers and Remote Peripherals', *Information Processing 1968*, North Holland Publishing Company, Amsterdam (1969)	1969
C.37	'Computers and Communications', *Spectrum British Science News*, 1969 no.62	1969
C.38	'Algorithm for Exploring a Hexagonal Pattern and Determining its Topology', NPL Com. Sci.T.M. 48, October 1970	1970
C.39	Paper by Davies published in Russian Latest bibliographical reference, 1970.	N.d.
C.40	'The Control of Congestion in Packet Switching Networks', NPL Com Sci TM 56, September 1971	1971

Lectures and publications, C.1-C.101

C.41	'Teleprocessing and data communication of the future', *Electronics & Power*, vol. 17, December 1971	1971
C.42	'Design for a Public Network', *Data Processing*, Data Transmission Supplement, January-February 1972	1972
C.43	'Measurement of the topology of a picture from samples taken on a regular array' With manuscript inscription 'From Inst. of Physics Conf. on Perception of Pattern and Pictures held at NPL, April 1972'.	N.d.
C.44	'Packet Switching in a Public Data Network', *Information Processing 1971,* North Holland Publishing Company (1972)	1972
C.45	'A Review of Computer Communication Technology' With manuscript inscription 'NATO meeting at Sussex University Sept '73'.	N.d.
C.46	'Introduction to the Post Office Experimental Packet Switched Service' The paper is undated but describes the service 'as it was envisaged in early 1973'. With manuscript inscription 'Now available as COM 70'.	N.d.
C.47	'Packet Switching, Message Switching and Future Data Communication Networks', *Information Processing 74*, North-Holland Publishing Company (1974)	1974
C.48	'New Data Networks in Europe', *Telecommunications*, vol. 9, no.6, June 1975	1975
C.49	'Future Networks - Public or Private?', *Data Processing*, July-August 1975	1975

Lectures and publications, C.1-C.101

C.50	'A Review of Computer Communication Technology', NATO Advanced Study Institutes Series Series E: Applied Sciences vol 4 - Computer Communication Networks	1975
C.51	'Exploitation of Seismograph Networks', NATO Advanced Study Series Series E Applied Sciences Exploitation of Seismograph Networks	1975
C.52	'Packing a Circular Suitcase', *NPL News*, no 327, 21 July 1977	1977
C.53	Three articles in *Computer Weekly*: 'The need for private data networks', 12 May 1977; 'Breakthrough in cryptography', 15 September 1977; and 'Practical public-key cryptosystem simply explained', 22 September 1977	1977
C.54	'Network Security by Encryption' With manuscript inscription 'Future Networks' Lecture 1977.	1977
C.55	Untitled typescript divided into titled sections: 'Cryptographic Capability'; 'The DES Block Cipher Algorithm'; 'Application of Cryptography for Data Transmission'; 'Application of Cryptography in Networks'; 'Security of Keys' With manuscript inscription 'NATO - BONAS'. Probably relates to presentation at NATO Advanced Study Institute, Bonas, France. It formed NPL Report Com 98 January 1978, see C.56, and was published in 1980 in *Information Privacy,* see C.64. Latest bibliographic reference, 1977	N.d.
C.56	'The Protection of Data by Cryptography' (with D.A. Bell), NPL Report Com 98, January 1978 See also C.55, C.64.	1978

Lectures and publications, C.1-C.101

C.57	'Human Factors in Display Terminal Procedures' (with D.M. Yates) Latest bibliographical reference, 1978	N.d.
C.58	'An Evaluation of Public Key Cryptosystems' (with W.L. Price and G.I. Parkin), NPL Report CTU 1, March 1979 See also C.65.	1979
C.59	'A decade of development in computer communications', *Alta Frequenza*, August 1979, vol. 18, no.8	1979
C.60	'New Techniques for Data Security', Congresso AICA [Associazione Italiana per il Calcolo Automatico], Bari, October 1979	1979
C.61	Christopher Evans', obituary for *Computer Bulletin*, Series 2, no. 22, December 1979	1979
C.62	'An Annotated Bibliography of Recent Publications on Data Security & Cryptography' (with W.L. Price), NPL Report DNACS [Division of Numerical Analysis and Computer Science] 25/80, January 1980	1980
C.63	'An Evaluation of Public Key Cryptosystems' (with W.L. Price and G.I Parkin), NPL Report CTU [Computer Technology Unit] 1, (Revised) April 1980	1980
C.64	'Protection of Data by Cryptography' (with D.A. Bell), *Information Privacy*, vol. 2 , no. 3, May 1980 See also C.55, C.56.	1980
C.65	'Evaluation of public-key cryptosystems' (with W.L. Price and G.I. Parkin), *Information Privacy*, vol. 2, no.4, July 1980	1980

/...

Lectures and publications, C.1-C.101

/... See also C.58.

C.66 'The Application of Digital Signatures Based on Public Key Cryptosystems', Proc. Fifth ICCC [International Council for Computer Communication], Atlanta, October 1980 — 1980

This is an abbreviated version of the NPL Report at C.68.

C.67 'Selected Papers in Cryptography and Data Security', NPL Report DNACS 38/80, November 1980 — 1980

C.68 'The Application of Digital Signatures Based on Public Key Cryptosystems' (with W.L. Price), NPL Report DNACS 39/80 December 1980 — 1980

See also C.66.

C.69 'Enhancement of Teletex Procedures to Incorporate Encipherment and Signatures' — N.d.

Latest bibliographical reference, 1980

C.70 'Standards for Privacy and Authentication Systems' (with W.L. Price) — N.d.

Latest bibliographical reference, 1981

C.71 'Encipherment and Signature in Teletex' (with I.K. Hirst), *Proc ICCC '82*, North Holland, 1982 — 1982

C.72 'The Siemens and Halske T52E Cipher Machine', *Cryptologia*, October 1982 — 1982

See also C.90.

C.73 'Security Aspects of Teletex Communications' — N.d.

With manuscript inscription 'Oslo, Nov' 82'.

Lectures and publications, C.1-C.101

C.74	'Applying the RSA Digital Signature to Electronic Mail', *Computer*, February 1983 vol. 16, no.2	1983
C.75	'The So-Called "Weak" Keys of the Data Encryption Standard (DES) Algorithm', February 1983	1983
C.76	'The Early Models of the Siemens and the Halske T52 Cipher', *Cryptologia*, July 1983 See also C.91.	1983
C.77	'The Average Cycle Size of the Key Stream in Output Feedback Encipherment' (with G.I. Parkin), *Lecture notes in Computer Science*, vol. 149, Berlin: Springer-Verlag), 1983	1983
C.78	'Public key ciphers and signatures', *Information Age*, vol. 6, no.1, January 1984	1984
C.79	'A New Look at the DES Complementation Property and Weak Keys', December 1984	1984
C.80	'Digital Signatures - An Update' With manuscript inscription 'ICCC Sydney 1984'.	N.d.
C.81	'COMNET '85 A Personal View of the Origins of Packet Switching'	1985
C.82	'How to use the DES Safely' With manuscript inscription 'IFIP Sec '85 Dublin'.	N.d.
C.83	'A Proposed Standard for Digital Signature of Multi-Block Messages', NPL Technical Memorandum TTCC [Tokens and Transactions Control Consortium], 31/87, June 1987	1987

Lectures and publications, C.1-C.101

C.84	'EFT-POS Security', IBC Seminar, 6 September 1988	1988
C.85	'Security in Electronics and Computers II: Special Problems in Banking', *Science in Parliament*, Oct/Nov 1993	1993
C.86-C.89	Undated papers	N.d.
C.86	'Discussion on Symposium on Monte Carlo Methods'	N.d.
C.87	'Modes of Use for a Block Encipherment Algorithm'	N.d.
C.88	'Some Regular Properties of the "Data Encryption Standard" Algorithm'	N.d.
C.89	'A Theory of Chess and Noughts and Crosses'	N.d.
C.90-C.101	Davies's publications in the journal *Cryptologia*	1982-2000
C.90	'The Siemens and Halske T52E Cipher Machine', *Cryptologia*, vol. 6, no.4, October 1982 See also C.72.	1982
C.91	'The Early Models of the Seimens and Halske T52 Cipher Machine', *Cryptologia*, vol. 7, no.3, July 1983 See also C.76.	1983
C.92	'The Mysterious Autocryptograph' (with J. Gillogly), *Cryptologia*, vol. 8, no.1, January 1984	1984
C.93	'Sidney Hole's Cryptographic Machine', *Cryptologia*, vol. 8, no.2, April 1984	1984

Lectures and publications, C.1-C.101

C.94	'Sir Percy Scott's Cipher', *Cryptologia*, vol. 8, no.3, July 1984	1984
C.95	'Charles Wheatstone's Cryptograph and Plett's Cipher Machine', *Cryptologia*, vol. 9, no. 2, April 1985	1985
C.96	'Cipher Equipment - Bolton's Cypher Wheel', *Cryptologia*, vol. 10, no.1, January 1986	1986
C.97	'New Information on the History of Siemens and Halske T52 Cipher Machines', *Cryptologia*, vol. 18, no.2, April 1994	1994
C.98	'The Lorenz Cipher Machine SZ42', *Cryptologia*, vol. 19, no.1, January 1995	1995
C.99	'The Bomb - A Remarkable Logic Machine', *Cryptologia*, vol. 23, no.2, April 1999	1999
C.100	'Effectiveness of the Diagonal Board', Cryptologia, vol. 23, no. 3, July 1999	1999
C.101	'An Unidentified Cipher Device', *Cryptologia*, vol. 24, no.2, 2000	2000

SECTION D **SOCIETIES AND ORGANISATIONS, D.1-D.37** **1987-2000**

D.1-D.23 **BRITISH COMPUTER SOCIETY (BCS)** **1997-2000**

D.1-D.7 'BCS' 1997-2000

Contents of folder so inscribed divided into seven for ease of reference.

General correspondence and papers *re* the affairs of the Society.

Topics include data protection, register of information security practitioners, working party on plastic banking systems and computer history.

D.8-D.21 Security Committee 1998-2000

Correspondence and papers.

Topics include electronic signatures, strategic export control, dual-use goods and technology and electronic commerce.

Fourteen folders.

Davies was a member of the Committee.

D.22, D.23 Miscellaneous information about the Society 1997, n.d.

Two folders.

Includes compact disc (D.22).

Societies and organisations, D.1-D.37

D.24-D.30 **INTERNATIONAL COUNCIL FOR COMPUTER COMMUNICATION (ICCC)** **1990-2000**

Correspondence, miscellaneous information, newsletters, brochures etc.

Seven folders.

Davies was an ICCC Governor (first elected 1985).

D.31-D.33 **ROYAL SOCIETY** **1987-1999**

Correspondence and papers.

Three folders.

Davies was elected to the Fellowship in 1987.

D.34-D.37 **WORSHIPFUL COMPANY OF INFORMATION TECHNOLOGISTS** **1992-2000**

Correspondence and papers.

Four folders.

Davies was admitted to the freedom of the Company of Information Technologists, 12 October 1992

SECTION E **CONSULTANCIES, E.1-E.28** **1986-1998**

Davies worked as a Data Security Consultant after his retirement from the NPL in 1984.

E.1-E.10	ARM [ADVANCED RISC MACHINES] LTD
E.11	EASYCHIP BV
E.12-E.16	HOUSLEY COMMUNICATION CONSULTANTS PTY, LTD
E.17-E.23	TELENOR CONAX AS
E.24-E.27	'VISA CHIP CARD'
E.28	WEGENER COMMUNICATIONS

E.1-E.10 **ARM [ADVANCED RISC MACHINES] LTD** **1994-1997**

Documentation principally relates to a research project funded by the European Commission through the Esprit Programme (EP8670) under the name CASCADE (Chip Architecture for Smart CArds and portable intelligent DEvices).

Ten folders.

E.11 **EASYCHIP BV** **1997-1998**

Correspondence and papers.

Consultancies, E.1-E.28

E.12-E.16 **HOUSLEY COMMUNICATION CONSULTANTS PTY, LTD** **1986-1990**

Housley was based in New South Wales, Australia. Davies gave a number of seminars on computer network security in association with Housley in Australia, New Zealand, Hong Kong and Singapore.

Correspondence *re* arrangements, publicity material etc.

Five folders.

E.17-E.23 **TELENOR CONAX AS** **1997-1998**

Correspondence and papers.

Seven folders.

Telenor Conax developed, produced and marketed intelligent cards and associated systems and services.

E.24-E.27 **'VISA CHIP CARD'** **1995, 1997**

Discussion document and specifications.

Four folders.

E.28 **WEGENER COMMUNICATIONS** **1998**

Includes printed out emails.

SECTION F **HISTORICAL TOPICS, F.1-F.265** **1949-2000**

The materials presented in this section were kept by Davies in a number of 'transfer cases' and box files with labels indicative of their content. These containers have been used as the basic unit of organisation of the section.

The contents of the containers are presented in the order found. The technical nature of the papers and the frequency of undated material makes the reordering of material unsafe. The contents are therefore divided only for ease of reference.

F.1-F.40	EARLY COMPUTERS
F.41-F.175	CRYPTOGRAPHY
F.176-F.190	NATIONAL PHYSICAL LABORATORY
F.191-F.236	PACKET SWITCHING
F.237-F.248	TURING MACHINE
F.249-F.265	MISCELLANEOUS

F.1-F.40 **EARLY COMPUTERS** **1955-2000**

F.1-F.15 'ACE 2000', Science Museum, 18 May and National Physical Laboratory, 19 May 2000 1955-2000

The meeting was held to celebrate the 50th anniversary of the Pilot Model Automatic Computing Engine ACE. The Pilot Model ACE ran its first program at the NPL on 10 May 1950.

Davies was to have given the opening address and a 'Demonstration of Pilot Ace Virtual Build'. The demonstration was a simulation program which Davies wrote in Microsoft Visual Basic. In fact he was not well and his paper was introduced by Derek Barber while Roger Scantlebury demonstrated the Virtual Rebuild of the Pilot Ace Computer.

Historical topics, F.1-F.265

F.1-F.4	Correspondence *re* arrangements (principally printed out emails), programme, list of particpants, etc. Four folders. The correspondence sequences include emails on the early history of networking. F.4 includes a 'draft' of D.O. Clayden's paper 'Advanced Aspects of the ACE Pilot Model Circuit for Design' sent to Davies for comment.	1998-2000
F.5-F.9	Typescript drafts of Davies's contributions, 'The ACE Pilot Model and its Creators, 'ACE Pilot Model Simulation Program', etc Five folders.	1999-2000
F.10-F.14	Manuscript working, typescript drafts, etc *re* ACE Pilot Model simulation Five folders	1999, n.d.
F.15	Printed papers	1955, 1981
F.16-F.40	'Early Computers (Babbage, Eniac, etc)' Contents of transfer case so labelled. Principally printed, typescript and photocopied background material relating to articles or talks by Davies.	1966-1995
F.16-F.18	Photocopied articles and off-print *re* Charles Babbage Three folders	1981-1983
F.19	'The Stormy Life of the world's first programmer', *Computer Weekly*, 10 January 1980 Published article by Davies on Ada, Countess of Lovelace and photograph of portrait used to illustrate the article. Folder also includes correspondence and papers *re*	1980-1995

Historical topics, F.1-F.265

exhibition, portrait, 1984, 1995.

The portrait hung in the entrance hall of Bushy House, part of the National Physical Laboratory.

F.20-F.28 Photocopied papers, off-prints *re* ENIAC, EDVAC, Turing, Zuse, etc 1966-1991

Nine folders.

F.29-F.32 NPL Reports *re* pioneers of computing with forewords by Davies 1972-1980

Four reports.

F.33 'A little light on the prehistory of ACE and EDSAC Extracts from correspondence on file at NPL' 1977

The typescript extracts were prepared by M. Woodger and are dated 1 February 1977. They cover the period 1945-1947. The principal correspondents are M.V. Wilkes at Cambridge and J.R. Womersley at the NPL.

The extracts include Wilkes's proposals for a pilot machine and Turing's internal note commenting on them.

The folder also includes copy of a letter from Wilkes to Woodger, 7 February 1977 with his 'Comments on extracts from correspondence on file at NPL' of the same date.

F.34 Extracts from NPL Reports for the period 1946 to 1956

F.35 'Use of ACE/DEUCE Computers at NPL (Summary based on extracts from NPL annual reports)' 1993

The summary was prepared by T. Vickers, May 1993. The period covered in the summary is from 1944 when the Mathematics Division at NPL was established to 1960.

F.36 Papers *re* Computer Conservation Society and meeting 'Design Decisions on Early Computers or Why we did what we did', Science Museum, London 24 May 1990 1989-1990

/...

Historical topics, F.1-F.265

/...	Davies with David Clayden talked on Pilot ACE.	
F.37	Typescript drafts by Davies: 'Summary for Talk on May 20th' and 'Alan Turing and the Foundations of Mathematics' The typescript draft for 'Talk on May 20th' has manuscript inscriptions at the top of the first page '1. Understand AMT[uring] contribution 2. Early history at NPL' and may relate to 24 May 1990 Computer Conservation Society meeting (see F.36)	N.d.
F.38-F.39	Illustrative material for talk or talks by Davies Two folders.	
F.40	Technical drawings	
F.41-F.175	**CRYPTOGRAPHY**	**1977-1999**
F.41-F.65	'Crypto History Cipher Machines' Contents of transfer case so labelled	1977-1999
F.41-F.50	'Historic Cipher Machine Papers' Contents of large envelope so inscribed: typescript papers and reports, figures, manuscript notes, correspondence, photographs, and printed papers.	1981-1994
F.41	Includes correspondence with W.W. Mache and photographs of cipher machines	1988-1994
F.42	Includes correspondence, 1983 (typescript copies of postcards) and 1992 and "Notes from IEE meeting on Colossus', 26 March 1987	1982-1992

Historical topics, F.1-F.265

F.43	'The Enigma Symposium 1992' by Hugh Skillen Published symposium proceedings.	1992
F.43A	Typescript draft by Davies entitled 'The Early Models of the Siemens and Halske T52 Cipher Machine' with figures attached. See also C.91 and F.98.	N.d.
F.44	Typescript draft by Davies entitled 'The Siemens and Halske T52e Cipher Machine' See also C.90 and F.99, F.100.	N.d.
F.45	Typescript draft by Davies entitled 'The Sequence of Development of the Siemens and Halske T52 Cipher Machine'	N.d.
F.46	Typescript draft by Davies entitled 'The Siemens and Halske T52e and some other cipher machines of World War II'	N.d.
F.47	Figures	N.d.
F.48	Typescript draft by Davies entitled 'The Method of Operation of the T52e Cipher Machine, One of the "Geheimschreiber" ' with figures attached	N.d.
F.49	'Master' typescript of 'The Method of Operation of the T52e Cipher Machine, One of the "Geheimschreibers" ' with two postscripts and figures.	
F.50	Typescript draft by B. Randell entitled 'The Enigma Cipher Machine', 20 March 1981	1981

Historical topics, F.1-F.265

F.51-F.65	Correspondence and papers found loose in the transfer case	1977-1999
F.51-F.53	Correspondence *re* cipher machines	1980-1988
F.51	1980, 1982	
F.52	Includes copy of lecture by W.W. Mache 'Der Siemens-Geheimschreiber in der Geschichte der Telekommunikation', 26 August 1984	1984
F.53	1987-1988	
F.54	Typescript draft by Davies entitled 'The Lorenz Schluesselzusatz Cipher Machine'	N.d.
F.55	Typescript draft by Davies entitled 'A Brief History of Cryptography', 3 July 1997	1997
F.56	Off-prints of three papers by Davies published in *Journal of Cryptology* and *Cryptologia*	1995, 1999
F.57	Manuscript notes	N.d.
F.58	Figures	N.d.
F.59-F.65	Printed and duplicated background material Seven folders. At F.60 is paper by W.W. Mache with Davies's manuscript 'remarks'. At F.65 are photocopies of Second World War material.	1976-1999

Historical topics, F.1-F.265

F.66-F.97	'Crypto History Enigma / Bombe' Contents of transfer case so labelled: correspondence including printed-out emails, typescripts and off-prints of papers by Davies, photographs, figures, diagrams, and duplicated and printed papers by others.	1977-1999
F.66-F.74	Duplicated and printed background papers Nine folders.	1977-1997
F.75-F.76	Photographs	1982, n.d.
F.75	Thirteen photographs found in envelope with postmark dated '1.12.82' and inscribed 'Oslo Photos Not Used'	1982
F.76	Seven photographs with negatives	N.d.
F.77	Computer print-out	N.d.
F.78	Contents of plastic folder: includes typescript draft by Davies entitled 'How Did the Polish Bombe Work?, 30 October 1997 and figures	1997
F.79	Contents of plastic folder: figures	N.d.
F.80	Figures	N.d.
F.81	Typescript draft by Davies entitled 'Notes for the Address on 19th March' Davies gave this address on the 30th Anniversary of the Computer Science Department at Royal Holloway University of London where he was Visiting Professor: 'The subject belongs to my hobby, which is the German cipher machines of WWII'.	N.d.

Historical topics, F.1-F.265

F.82	Includes 'Enigma and the Turing Bombe' by N. Shaylor, 17 April 1997 (pages printed from website)	1997
F.83	Correspondence including printed-out emails, July-August 1998	1998
F.84	Figures	
F.85-F.87	Correspondence, principally printed-out emails, and papers *re* 'The Enigma Uhr' Three folders. F.85 includes typescript draft by Davies entitled 'Principle of the Enigma Uhr', 29 August 1998	1984-1998
F.88	Correspondence, principally printed-out emails, and papers, *re* 'The diagonal board', 'Enigma rotor movement', 'Enigma; bombe; Welchman', etc	
F.89	Photocopied article on the deciphering of Enigma by Polish mathematicians, 1981	
F.90	Correspondence (printed-out emails), circuit diagrams, etc *re* Bombe rebuild project, sense circuits etc	1998
F.91	Correspondence (printed-out emails) and papers *re* 'Turing's Treatise on Enigma', etc	1998
F.92	Correspondence, principally printed-out emails, *re* the diagonal board, 'Papers about Alan Turing', Davies's 'bombe paper', visit to the USA, etc.	1998
F.93	Includes 'some genuine Hut 6 Cribs'	1998

Historical topics, F.1-F.265

F.94	Typescript draft by Davies entitled 'The Effectiveness of the Diagonal Board', 5 September 1998	1998
F.95	Typescript draft by Davies 'The Bombe - A Remarkable Logic Machine', 30 June 1998 with manuscript inscription 'Corrected 27 Oct 98'	1998
F.96	Correspondence *re* publication of papers by Davies	1999
F.97	Off-prints including two bombe papers by Davies	1999
F.98-F.139	'T52 Crypto History' Contents of transfer case so labelled. Typescripts, figures, correspondence, interviews, miscellaneous manuscript notes, technical drawings, photographs, patents, photocopied background material. A series of cipher machines designated T52 was manufactured by Siemens and Halske between 1934 and 1944. Davies researched and published a number of articles on the history of the Siemens and Halske T52 Cipher Machines.	1977-1997
F.98	Typescript draft by Davies entitled 'The Early Models of the Siemens and Halske T52 Cipher Machine' With manuscript inscription at the top of the first page 'Corrected'. See also C.91 and F.43.	N.d.
F.99-F.100	Two typescript drafts by Davies entitled 'The Siemens and Halske T52e Cipher Machine', one with manuscript revision Two folders. See also C.90 and F.44.	N.d.
F.101	Not used.	

Historical topics, F.1-F.265

F.102 — Off-print of Davies's paper 'New Information on the History of the Siemens and Halske T52 Cipher Machines', *Cryptologia*, vol 18, April 1994 — 1994

See also C.97.

F.103 — 'Artwork to Return to Davies July 83 Crypto' — 1983

Contents of folder so inscribed: figures.

F.104-F.109 — Figures — N.d.

Six folders.

See F.108 for photographs of T52 cipher machine.

F.110-F.112 — Correspondence — 1980-1997

F.110 — 1980-1981

Includes typescript by W. Mache entitled 'Siemens Cipher Teleprinters 1930-1945, primary G-Schreiber T52 a-f, the "Geheimschreiber" ', September 1981.

F.111 — 1982

Includes two photographs of 'Dieppe Model d'.

F.112 — 1983-1985, 1997

Includes typescript draft by Davies entitled 'Principle of the T52 cypher machines', 11 June 1984 and three photographs, one inscribed on verso 'Dieppe 5 July, 1984'.

F.113 — Includes notes of interviews and discussion — 1977, n.d.

Historical topics, F.1-F.265

F.114-F.117	Miscellaneous manuscript and typescript notes and drafts Four folders.	
F.118-F.122	Technical drawings Five folders.	
F.123, F.124	Patents Two folders.	
F.125-F.131	Photographs	1985, n.d.
F.125	Includes 'T52d in Oslo'	N.d.
F.126	Includes 'Siemens T25' and '10 April, 85, Bad Godesberg'	1985, n.d.
F.127	'T52D photographed in Norway'	N.d.
F.128, F.129	Unidentified Two folders.	N.d
F.130	'My Photos / T52 etc'	N.d.
F.131	'12 Photos / Some are my best or only (and original) copies / D.W. Davies'	N.d.
F.132-F.134	Papers sent to Davies by W.W. Mache including photocopied background material Three folders.	1981

Historical topics, F.1-F.265

F.135	Typescript draft ? sent to Davies for comment entitled 'Chapter VI Waiting for Baudot' With manuscript inscription at the top of the first page 'Replied ~ 26 Jan 1983'	1983
F.136-F.139	Photocopied background material Two folders and two bound items inscribed 'Valuable archival material / DWD'.	N.d.
F.140-F.175	Contents of unlabelled transfer case	1980-1995
F.140-F.164	'Crypto History SZ42' Contents of folder so labelled. The SZ42 was a German cipher machine. Davies researched and wrote an article 'The Lorenz Cipher Machine SZ42' for *Cryptologia*.	1980-1995
F.140-F.151	Photographs Twelve folders.	N.d.
F.152	Correspondence	1980, 1983
F.153	Reports by Davies on examination of SZ42 carried out on 28 April, 4 May, 8 June and 27 June 1994	1994
F.154	Typescript draft by Davies 'The Lorentz Cipher Machine SZ42', July 1994	1994
F.155-F.159	Correspondence	1994-1995
F.155	1994 May-June	

Historical topics, F.1-F.265

F.156 — 1994 July-August

Includes galleys of paper by Davies entitled 'The Lorenz Cipher Machine SZ42' and figures.

F.157 — 1995 January

F.158 — 1995 February-April

Includes typescript draft by Davies entitled 'Plan for Running the SZ42 Cipher Attachment at Bletchley Park', February 1995

F.159 — 1995 May-August

F.160-F.161 — Miscellaneous working notes and drafts, etc. — N.d.

Two folders.

F.161 includes typescript draft by Davies 'The Lorenz Schluesselzusatz Cipher Machine'

F.162 — Photocopied background papers

F.163-F.164 — Contents of plastic folder — 1994

Letter from A.E. Sale, manuscript working, programs, two computer disks, etc *re* Lorenz SZ42 Simulator.

Two folders.

F.165-F.175 — 'Crypto History T52 Papers + Copies (Jon Paul)' — N.d.

Contents of padded envelope so labelled.

Jon D. Paul was the Curator of the Crypto-Museum of Marin, Novato, California.

F.165 — Business card and compliments slip for J.D. Paul, and photograph of cipher machine, found clipped together

Historical topics, F.1-F.265

F.166-F.175	Photocopied technical drawings and other technical documentation Nine folders and one bound volume.	
F.176-F.190	**NATIONAL PHYSICAL LABORATORY**	**1962-1998, n.d.**
	'Historical Notes NPL etc'. Contents of transfer case so labelled.	
F.176-F.181	Admin Historical Notes 1-6	1969-1970
F.176	'The Origin of the Laboratory' by H.J. Hadow	March 1969
F.177	'NPL Archives A plan and a plea for help' by H.J. Hadow	January 1970
F.178	'Expenditure and Staff in Post 1900 to 1968' by H.J. Hadrow	February 1970
F.179	'Bushy Park and Bushy House' by H.J. Hadow	February 1970
F.180	'The Development of the NPL Site at Teddington 1900-1970' by H.J. Hadow	March 1970
F.181	'The Newton's Apple Tree' by H.J. Hadow	April 1970
F.182	'Teddington Laboratories Children's Party An Anecdotal History: 1923-1998' by Colin Lea	1998
F.183-F.186	Printed and duplicated background material *re* NPL and	1962-1972, n.d.

Historical topics, F.1-F.265

Bushy House

Four folders

At F.183 is 1970 reprint of lecture by Sir Richard Glazebrook, 'Early Days at the National Physical Laboratory', 23 March 1933.

F.187-F.188 — Two typescript drafts, slides, and background material for talk by Davies about William IV — N.d.

Two folders.

William IV (as Duke of Clarence) was a former resident of Bushy House.

F.189-F.190 — Miscellaneous papers of historical interest

F.189 — Photocopied papers — 1957, 1980, n.d.

Typescript draft by Davies entitled 'Augusta Ada, Countess of Lovelace'; off-print of D.R. Hartree's address to the British Computer Society at their inaugural meeting, 12 October 1957; 'Draft outline of Turing's Collected Works'; and signed menu of dinner to mark the retirement of M.V. Wilkes, 18 July 1980.

F.190 — Includes manuscript notes.

F.191-F.236 — **PACKET SWITCHING** — **1949-2000**

'Historical Notes / Early Packet Switching etc'.

Contents of transfer case so labelled.

F.191 — Off-prints of papers by Davies: 'Communication networks to serve rapid-response computers' and 'The principles of a data communication network for computers and remote peripherals', *Information Processing 68*, North-Holland Publishing Company, Amsterdam (1969) — 1969

Historical topics, F.1-F.265

F.192	Correspondence including printed-out emails *re* history of packet switching concept and IEEE Internet Award, March 2000	2000
F.193-F.194	Two typescript drafts of paper by Davies entitled 'An Historical Study of the Beginnings of Packet Switching', March 2000 Two folders. Davies's opening sentence explains that the purpose of the paper was 'to help those who study the early history of computer networking by providing pointers to primary documents concerning one of the first steps in the new technology - the introduction of packet switching'.	2000
F.195	Typescript draft by Davies entitled 'Notes from the Early History of Packet Switching', January 2000	2000
F.196	Correspondence including printed-out emails *re* history of packet switching	1999-2000
F.197	Pages printed from the internet: 'Internet Chronology Lawrence G. Roberts March 22 1997 - updated Aug 29, 1997' and 'Brief Summary of Firsts, Key Accomplishments and Contributions for Len Kleinrock'	1999-2000
F.198	Copy (printed from the internet) of 'Information Flow in Large Communication Nets Proposal for a PH.D Thesis' by Leonard Kleinrock, 31 May 1961	
F.199	Correspondence, principally printed-out emails, with P. Baran, J. Gillies and L. Kleinrock and others *re* internet history, February-March 2000	2000
F.200	Photocopy of 1964 paper by Paul Baran entitled 'On Distributed Communication Networks' with manuscript notes by Davies attached.	

Historical topics, F.1-F.265

F.201	Manuscript notes by Davies on 'Communication Nets (Stochastic Message Flow and Delay) By Leonard Kleinrock McGraw-Hill 1964'	
F.202	Correspondence (printed-out emails) principally with P. Baran *re* IEEE Internet Award nomination, history of packet switching, etc., December 1999-February 2000	1999-2000
F.203-F.206	Papers *re* ACM [Association for Computing Machinery] Symposium on Operating System Principles, Gatlinburg, Tennessee, USA, 1-4 October 1967	1967
F.203	Programme and list of 'registered attendees'	
F.204	Photocopy of conference paper by L.G. Roberts entitled 'Multiple Computer Networks and Intercomputer Communication'	
F.205	Copy of conference paper by Davies, K.A. Bartlett, R.A. Scantlebury and P.T. Wilkinson entitled 'A Digital Communication Network for Computers giving Rapid Response at Remote Terminals'	
F.206	'Report on Visit of R.A. Scantlebury to the 1967 A.C.M. Symposium U.S.A.'	1967
F.207	Typescript draft by Davies entitled 'Historical Note on the Early Development of Packet Switching' Davies states that there were two purposes in writing this note: 'One is to help the Science Museum project on the history of computing and the other is to provide material for the historical paper in the forthcoming IEEE Proceedings on Packet Switching. Davies states that some of the events in this undated note 'are now more than ten years away'.	N.d.
F.208	Copy of typescript note by Davies entitled 'Further Speculations on Data Transmission', 16 November 1965	1965

Historical topics, F.1-F.265

With manuscript inscription at the top of the first page 'Early History - Preserve!'.

F.209 — Copies of papers by Davies entitled 'Remote on-line Data Processing and its Communication Needs' and 'Proposal for the Development of a National Communication Service for on-line Data Processing', 15 December 1965 — 1965

The papers were found stapled together. Both have the manuscript inscription 'Early History - Preserve!' at the top of their first pages.

F.210 — Photocopied pages headed '18.3.1966' and 'Mr D.W. Davies: The Future Digital Communication Network' with signatures of those attending Davies's presentation and the names of the organisations they represented — 1966

F.211 — NPL paper by Davies entitled 'Proposal for a Digital Communication Network', June 1966 — 1966

With manuscript inscription on the title page 'Early History - Preserve!'.

F.212 — Photocopy of paper by B.W. Boehm and R.L. Mobley, 'Adaptive Routing Techniques for Distributed Communications Systems', *IEEE Transactions on Communication Technology*, June 1969

F.213-F.214 — Correspondence etc *re* paper by M. Campbell-Kelly on the NPL data communications network — 1987-1988

Two folders.

The paper was published in the *Annals of the History of Computing*, vol. 9, 1988.

F.215 — Booklet of papers for Hardware 1, IFIP [International Federation for Information Processing] Congress 68, Edinburgh, August 1968 — 1968

Includes paper by Davies entitled 'The principles of a data communication network for computers and remote peripherals'

Historical topics, F.1-F.265

F.216	Proceedings of Session on Resource Sharing Computer Networks, Spring Joint Computer Conference, Atlantic City, New Jersey, USA, 7 May 1970 Includes papers by L.G. Roberts and L. Kleinrock.	1970
F.217	NPL Report Com 85 by R.A. Scantlebury and P.T. Wilkinson on 'The National Physical Laboratory Data Communication Network', December 1976	1976
F.218	Paper by Davies, K.A. Bartlett, R.A. Scantlebury and P.T. Wilkinson entitled 'A Data Communication Network for Real-time Computers' Latest bibliographical reference November 1966	N.d.
F.219	Papers *re* CCITT [International Consultative Committee for Telephones and Telegraphs] meeting, Geneva, Switzerland, 23-27 November 1970: paper by Davies entitled 'C.C.I.T.T. Meeting at Geneva, November 23 to 27', 26 November 1970; paper by Davies entitled 'Preparation for the NRD meeting of November 1970, 16 November 1970; and 'Report on CCITT Meetings on New Data Networks 23-27 November 1970 at Geneva', December 1970	1970
F.220	Duplicated typescript entitled 'A Communication Network for Computers and their Remote Peripheral Devices', October 1967	1967
F.221	Photocopy of paper by Davies entitled 'A Store-and-Forward Communication Network for Real-time Computers and their Peripherals'	N.d.
F.222	Photocopy of paper by Davies entitled 'Some Design Aspects of a Communication Network Rapid-Response Computers'	N.d.
F.223	Photocopy of paper by Davies entitled 'Transfer of Data from one Node Computer to Another', August 1966	1966

Historical topics, F.1-F.265

F.224	Photocopy of paper by Davies entitled 'The Control of Congestion in Packet Switching Networks' Latest bibliographical reference 1970.	N.d.
F.225	Photocopy of paper by R.A. Scantlebury entitled 'A model for the local area of a data communication network objectives and hardward organization' Latest bibliographical reference, October 1969.	N.d.
F.226	Photocopy of paper by P.T. Wilkinson entitled 'A model for the local area of a data communication network Software organization' Latest bibliographical reference October 1969.	N.d.
F.227	'Report on Visit to USA, October 16-27, 1972' by Davies, 14 November 1972 Davies explained that the purpose of the visit was 'to renew contacts with those engaged in the ARPA network project, see the present state of the network and experience its use, visit establishments engaged in work relevant to [NPL] Computer Division and attend the first International Computer Communications Conference'.	1972
F.228	NPL Report Com. Sci. T.M. 47 by D.L.A. Barber and Davies entitled 'The NPL Data Network', October 1970	1970
F.229	Papers by Davies's NPL colleagues: off-print entitled 'A note on Reliable Full-Duplex Transmission over Half-Duplex Links' by K.A. Bartlett, R.A. Scantlebury and P.T. Wilkinson, *Communications of the ACM* [Association for Computing Machinery], vol 12, May 1969 and duplicated typescript entitled 'A Review of the Performance of the N.P.L. Data Communications Network' by D.L.A. Barber, K.A. Bartlett and I.G. Dewis, with manuscript inscription 'Symposium on Networks - Bonn 1972'.	1969, 1972
F.230	Brief correspondence with Janet Abbate *re* early history of computer networks	1996

Historical topics, F.1-F.265

F.231	Two letters from J. von Neumann, 'May 4, 1949' (photocopy) and '8.2.50' (original and photocopy)	1949-1950
F.232	'Origins of Packet Switching and the Early ARPA Network - Talk to CCS [Computer Conservation Society] on 12/3/98 Transparencies	1998
F.233-F.236	Duplicated and printed background material Four folders.	1969-1989
F.237-F.248	**TURING MACHINE** Contents of box folder: principally typescripts by Davies	**1996-1999**
F.237	Photocopy of Turing's 1936 paper entitled 'On computable numbers, with an application to the Entscheidungsproblem'	
F.238	Two typescript drafts by Davies entitled 'Documentation of Turing's Universal Computing Machine', May 1996	1996
F.239	Typescript draft by Davies entitled 'Explicit Form of Turing's Universal Computing Machine', May 1996	1996
F.240	Typescript draft by Davies entitled 'Verifying the Design of a Universal Turing Machine', June 1996	1996
F.241	Two typescript drafts by Davies entitled 'Repairs to Turing's Universal Computing Machine', 27 August 1996 and 30 September 1997	1996-1997

Historical topics, F.1-F.265

F.242	Typescript draft by Davies entitled 'Corrections to Turing's Universal Computing Machine', 2 October 1996	1996
F.243	Proof copy of 'Repairs to Turing's Universal Computing Machine' and related papers Davies's paper 'Repairs to Turing's Universal Computing Machine' was a contribution to Machine Intelligence 15 (Oxford University Press).	1999
F.244	'Turing Machine Software' Programming by Davies.	N.d.
F.245-F.247	Contents of plastic folder divided into three for ease of reference: typescript draft by Davies entitled 'Guide to the Documentation', programming etc.	N.d.
F.248	Manuscript sheet headed 'Dependencies of Abbreviated Tables'	N.d.
F.249-F.265	**MISCELLANEOUS**	**1964-2000**
F.249-F.257	Contents of box folder divided into nine for ease of reference: printed and duplicated material *re* early computers, communication networks and cryptosystems There are copies of papers by Davies at F.250, F.251 and F.254.	1964-1979
F.258-F.265	Contents of folder divided into eight for ease of reference: correspondence (including printed-out emails) and papers *re* history of cryptography, the internet and early computers Includes photocopies of earlier material. At F.259 is typescript of paper by Davies entitled 'How did the Polish bombe work?'	1997-2000

Historical topics, F.1-F.265

At F.261 are Davies's comments on the first two chapters of *How the Web was born: the story of the World Wide Web* by James Gillies and Robert Cailliau (Oxford University Press, 2000), sent to Gillies.

At F.264 are a list of papers of historical interest concerning electronic digital computers, 1945-1959 held by M. Woodger in the Division of Numerical Analysis and Computer Science, National Physical Laboratory and a catalogue of the papers of M. Woodger at the time of his retirement, 31 March 1983.

SECTION G **CORRESPONDENCE, G.1-G.60** **1970-2001**

G.1-G.9	MISCELLANEOUS CORRESPONDENCE
G.10-G.24	CORRESPONDENCE WITH W.W. MACHE
G.25-G.36	PUBLICATIONS CORRESPONDENCE
G.37-G.60	PATENT CORRESPONDENCE

G.1-G.9 **MISCELLANEOUS CORRESPONDENCE** **1970-2000**

Contents of folder inscribed 'Misc. Correspondence'.

G.1 1970-1971

Three letters from Sara Turing.

G.2 1985-1991

G.3 1993-1996

G.4 1997

Includes copy of letter from Davies on bar codes, 20 April 1997, and article by Davies on 'Packet switching: the history lesson' published in *The Guardian*, 21 August 1997

G.5-G.6 1998

Two folders.

Includes correspondence *re* possible role for Davies as an expert witness, historical cryptology, current cryptosystem, etc.

Correspondence, G.1-G.60

G.7-G.8 1999

Two folders.

Includes correspondence and papers *re* historical cryptology and current internet topics.

G.9 2000

Includes letter from Institute of Electrical and Electronics Engineers, Inc (IEEE), 6 March 2000, informing Davies of his being named as a co-recipient of the 2000 IEEE Internet Award along with Paul Baran, Leonard Kleinrock, and Lawrence G. Roberts, with the following citation:

'For their early, preeminent contributions in conceiving, analyzing and demonstrating packet-switching networks, the foundation technology of the internet'.

G.10-G.24 CORRESPONDENCE WITH W.W. MACHE 1991-2000

Contents of folder inscribed 'W. Mache'.

Correspondence principally *re* historical cryptology and German cipher machines. Mache was a German engineer working for Siemens in Munich who shared Davies's interests. In 1991 Davies was proposing a book on German cipher machines of the Second World War with Mache as collaborator. For 1996-1997 there is also correspondence and papers *re* a documentary film made by Davies's son Michael on the First World War German flying ace von Richthofen.

G.10 1991

G.11 1992

G.12 1993 January-February

Includes 'New Book Proposal by D.W. Davies and W.W. Mache'.

Correspondence, G.1-G.60

G.13 — 1993 March

Includes article by F.-P. Heider entitled 'A Colossal Fish' sent to Davies for his comment.

G.14 — 1993 May-December

Includes 'newest version' of Heider's article.

G.15 — 1994 January-May

G.16-G.19 — 1995 May-August

Includes copies of German patents.

Four folders.

G.20-G.21 — 1996

Two folders.

G.22 — 1997

G.23 — 1998

G.24 — 1999-2000

G.25-G.36 — PUBLICATIONS CORRESPONDENCE — 1988-1999

G.25-G.30 — *ICL Technical Journal* — 1993-1999

Correspondence and papers *re* the business of the Editorial Board.

Six folders.

/...

Correspondence, G.1-G.60

/... Davies was a member of the Board for the period covered by the papers.

G.31-G.36 John Wiley & Sons Ltd 1988-1993

Six folders.

Principally *re* Davies's book (with W.L. Price) *Security for Computer Networks*, Second Edition, 1989.

Davies was also asked to advise on a number of book proposals.

G.37-G.60 PATENT CORRESPONDENCE 1994-2001

Contents of transfer case labelled 'Patent': correspondence and papers.

The material relates to the invention by Davies of a method and apparatus for transmitting and receiving encrypted signals and a dispute in respect of patent application.

G.37 1994 April-May

G.38 1994 July-August

G.39, G.40 1994 September

Two folders.

At G.40 are two typescript drafts entitled 'Method and Apparatus for Transmitting and Receiving Encrypted Signals'.

G.41 1994 October-November

Includes typescript note by Davies entitled 'The invention and patenting of the "Difference Method" ', November 1994. See also G.47 and G.50.

Correspondence, G.1-G.60

G.42	1994 December
G.43	1995 January-March
G.44	1995 April-September
G.45-G.46	1995 October Two folders.
G.47	1996 February-March
G.48-G.49	1996 April Two folders.
G.50	1996 May-June
G.51	1996 July-December
G.52	1997 January
G.53	1997 February-March
G.54	1997 April, June
G.55	1997 July-August
G.56	1997 September-December

Correspondence, G.1-G.60

G.57 1998 February-October

G.58 1999

G.59 2000-2001

G.60 Photocopy of European Patent Application filed '17.09.90', annotated by Davies

The patent application was for a system for controlling access to broadcast transmission. Davies was not a party to the application.

INDEX OF CORRESPONDENTS

Index of correspondents

Index of correspondents

Index of correspondents

Index of correspondents