Bibliography for BLU.org Crypto History 2017: Fish rotors (W.Ricker)

Books

- *The Codebreakers: The Story of Secret Writing,* By David Kahn ISBN 9780684831305 "An updated and revised history of codes offers new information on techniques used to break machine and computer ciphers, as well as the speculation of scientists on how messages from outer space might be solved and a study of the use of codes during the Vietnam War."
- *Colossus: The Secrets of Bletchley Park,* Jack Copeland. OUP 2010 ISBN 0-19-284055-X (Hardcover), 0-19-957814-X (Paperback) online
- *Decrypted Secrets: Methods and Maxims of Cryptology* ISBN 3662034522 Friedrich L. Bauer - 2013
- *The History of Information Security: A Comprehensive Handbook,* Karl Maria Michael de Leeuw, Jan Bergstra. (*not used, but has interesting looking chapters on ENIGMA and TUNNY*)
- *Breaking Teleprinter Ciphers at Bletchley Park: An Edition of I.J. Good, D. Michie and G. Timms: General Report on Tunny With Emphasis on Statistical Methods (1945),* "This book is an edition of the General Report on Tunny with commentary that clarifies the often difficult language of the GRT and fitting it into a variety of contexts arising out of several separate but intersecting story lines, some only implicit in the GRT. Original authors I.J. Good, D. Michie and G. Timms. Modern additions by Whitfield Diffie (introduced by), J. V. Field (contributor) and James A. Reeds (editor) isbn 9780470465899 google

Websites

- cryptomuseum.com; Tape adding images
- CipherMachines.com One Time Pad
- Frode Weierud, "BP's Sturegeon, The FISH That Laid No Eggs," excerpted from *The Rutherford Journal,* Volume 1, 2005-2006. link (*included in Colossus book*)
- "Vernam, Mauborgne, and Friedman: The One-Time Pad and and the Index of Coincidence," Steve Bellovin, CUCS-014-14
- A Cryptographic Compendium incl T-52 circuits index
- Alan Turing Archive G.R.Tunny
- codesandciphers.org.uk G.R.Tunny
- TICOM reports on German SIGINT
- HackaDay demo of Baudot with steel balls
- CDVandT another virtual museum
- Damm cylinder was precursor to Hagelin and Crypto AGc6 US patents 1917 - 1928

Software

- CryptoGL github C++ library for classic and many modern algos but not WW2 machnies *not used but interesting*

PATENTS

- T-52 Siemens patent 1933
- Parker Hitt, precursor of SZ T 40 e.g. Printing telegraph system 1932
- Mechanical deciphering system, Keiber, A.H.,
- Secret signaling system
- Ciphering and deciphering mechanism Wilhelm Hagelin Boris Caesar

- Vernam
- Friedman e.g. * Typewriters for ciphering or deciphering cryptographic text
- IBM Inventor Harry J Nichols
- US1502376A Damm Arvid Gerhard Production of ciphers

- US1912983A 1930-07-18 1933-06-06 Siemens Ag Secret telegraph system
- US2406024A 1942-05-28 1946-08-20 Bell Telephone Labor Inc Key tape device for enciphering telegraph signals (the 999*1000 dual-tape
- US2351014A 1942-12-30 1944-06-13 Postal Telegraph Cable Co Alarm for synchronous telegraph circuits
- US2406023A 1944-03-25 1946-08-20 Bell Telephone Labor Inc Teletypewriter signal enciphering system