Colossus

Colossus

Colossi waren frühe Computer, die in England während des Zweiten Weltkriegs speziell zur Dechiffrierung von geheimen Nachrichten des deutschen Militärs gebaut wurden. Mit ihrer Hilfe wurde ab 1943 in die Entzifferung Bletchley Park der deutschen Lorenz-Schlüsselmaschine möglich.

Colossus Mark II

Motivation

Die Verschlüsselungsmethode – Erzeugung von Pseudozufallszahlen und exklusive Veroderung - wurde durch einen schwerwiegenden

Fehler der Deutschen bereits beim 1. Erprobungsversuch erkannt: Eine etwa 4000 Zeichen lange Nachricht wurde mit leicht unterschiedlichem Text, jedoch mit derselben Pseudozahlenfolge zweimal übertragen, was eigentlich streng verboten war.

Die Deutschen verwendeten einen täglich wechselnden Schlüssel, der unterschiedliche Zahlenfolgen erzeugte. Jede Nachricht musste daher getrennt entziffert werden. Eine manuelle Dechiffrierung einer Nachricht nahm mehrere Monate in Anspruch. Die enthaltene Information ist dann in der Regel wertlos. Max Newman erkannte, dass die Entzifferung mit Maschinenhilfe wesentlich beschleunigt werden kann.

Der Entwurf der Maschine stammte von Max Newman, einem in Bletchley-Park beschäftigten Mathematiker, aufbauend auf den Ideen zu einer universellen Maschine von Alan Turing. Gebaut wurde die Maschine von Tommy Flowers im Forschungszentrum der britischen Post in Dollis Hill.

Aufbau und Leistungsfähigkeit

Colossus bestand zunächst (1943) aus 1.500 Röhren, später aus 2.500. Bei einer Leistungsaufnahme von 4500 W konnten von der Maschine erstaunliche 5.000 Zeichen (à 5 Bit) pro Sekunde verarbeitet werden. Der Speicher bestand aus 5 Zeichen von je 5 Bit in Schieberegistern. Die Zeichen wurden photoelektrisch von einem Lochstreifen gelesen, die Lochreihe in der Streifenmitte erzeugte den Takt, bei 5.000 Zeichen/sek also 200 µs. Innerhalb eines Taktes konnten etwa 100 Boolean-Operationen auf jeder der fünf Lochreihen und anschließend auf einer Zeichenmatrix parallel durchgeführt werden. Die Treffer wurden dann gezählt.

Zwischen 1943 und 1946 wurden insgesamt zehn Geräte gebaut. Colossus erlaubte die Entzifferung einer Nachricht innerhalb weniger Stunden.

Colossus

Erster speicherprogrammierbarer Computer

Die Colossus gilt zwar als der erste speicherprogrammierbare Computer, war jedoch fest an eine bestimmte Aufgabe angepasst und nicht im heutigen Sinn frei programmierbar. Das Gerät wurde unter strengen Geheimhaltungsrichtlinien gebaut, so dass keinerlei Aufzeichnungen oder Handbücher darüber existieren. Alle britischen Colossus wurden 1946 aus Geheimhaltungsgründen demontiert und vernichtet, jedoch überlebte eine US-Variante.

Nachbau durch Tony Sale

Erst 1970 wurde die Existenz von Colossus öffentlich bekannt. Ab 1990 baute Tony Sale, Ingenieur und ehemaliger Mitarbeiter des Nachrichtendienstes MI5 den Colossus für das Computermuseum in Bletchley Park nach. Am 6. Juni 1996 hatte er seinen ersten erfolgreichen Lauf. Zur offiziellen Einweihung des Gerätes am 16. November 2007 sandten deutsche Funkamateure einen mit einer original *Lorenz* verschlüsselten Text. Colossus "knackte" die Nachricht in drei Stunden und 35 Minuten, sie enthielt eine Einladung zu einer Ausstellung mit historischen Computern im Heinz Nixdorf MuseumsForum, Paderborn. Die Entzifferung verzögerte sich um rund 45 Minuten, da eine der 2400 Röhren des Rechners geplatzt war. [1] Im parallel zur Übertragung veranstalteten Wettbewerb gelang es einem Funkamateur, das Signal mit der Antenne seines Clubs aufzufangen, akustisch zu bearbeiten und es mit einem Laptop unter FreeBSD



Tony Sale 2006 bei einer Entzifferung mit der fertiggestellten Maschine.

schließlich in 46 Sekunden zu entziffern. Der Nachbau des Colossus ist im Museum von Bletchley Park zu sehen.

Colossus – der Film

1970 entstand der Science-Fiction-Thriller "Colossus: The Forbin Project" nach einem Roman von Dennis Feltham Jones. Er bezieht sich zwar nicht ausdrücklich auf seinen älteren Namensvetter, dennoch sind Parallelen erkennbar: Ein gigantischer Supercomputer, eingebettet in das Innere eines Berges, soll helfen, den Weltfrieden zu sichern. Professor Forbin (dargestellt von Eric Braeden), der geniale Entwickler des Computergiganten, welcher sogar einen Nuklearkrieg überstehen soll, rechnet nicht mit dem gefahrvollen Potential seiner Kreation.

Vergleich mit anderen frühen Computern

Eigenschaften der ersten Computer

Computer	Land	Inbetriebnahme	Gleitkomma- arithmetik	Binär	Elektronisch	Programmierbar	Turingmächtig
Zuse Z3	Deutschland	Mai 1941	Ja	Ja	Nein	Ja, durch Lochstreifen	Ja
Atanasoff-Berry-Computer	USA	Sommer 1941	Nein	Ja	Ja	Nein	Nein
Colossus	UK	1943	Nein	Ja	Ja	Teilweise, durch Neuverkabelung	Nein
Mark I	USA	1944	Nein	Nein	Nein	Ja, durch Lochstreifen	Ja
Zuse Z4	Deutschland	März 1945	Ja	Ja	Nein	Ja, durch Lochstreifen	Ja

Colossus

ENIAC	USA	1946	Nein	Nein	Ja	Teilweise, durch Neuverkabelung	Ja
		1948	Nein	Nein	Ja	Ja, durch eine Matrix aus Widerständen	Ja

Literatur

- Bengt Beckmann, K. O. Widmann: *Arne Beurling und Hitlers Geheimschreiber. Schwedische Entzifferungserfolge im 2. Weltkrieg.* Springer, Berlin u. a. 2006, ISBN 3-540-23720-8.
- B. Jack Copeland: Colossus. The Secrets of Bletchley Park's Codebreaking Computers. Oxford University Press.
 Oxford u. a. 2006, ISBN 0-19-284055-X.
- Paul Gannon: Colossus. Bletchley Park's Greatest Secret. Atlantic Books, London 2006, ISBN 1-84354-330-3.

Weblinks

- Der wiedererbaute Colossus [2]
- Offizielle Seite von Bletchley Park [3]
- Neue Zürcher Zeitung, (2. März 2007) ^[5]: Colossus, der erste elektronische Computer, ist in Bletchley Park als Nachbau zu besichtigen.
- Colossus: The Forbin Project [6] in der Internet Movie Database (englisch)

Quellen

- [1] Der Code-Knacker Briten rekonstruieren Computer aus dem Zweiten Weltkrieg, Süddeutsche Zeitung, Nr.265, S. 24, 17./18. November 2007
- [2] http://www.codesandciphers.org.uk/lorenz/rebuild.htm
- [3] http://www.bletchleypark.org.uk/
- [4] http://www.sueddeutsche.de/digital/verschluesselung-code-knacker-1.333646
- [5] http://www.nzz.ch/nachrichten/panorama/articleeyv3k_1.120963.html
- [6] http://www.imdb.com/title/tt0064177/

Quelle(n) und Bearbeiter des/der Artikel(s)

Colossus Quelle: http://de.wikipedia.org/w/index.php?oldid=117639128 Bearbeiter: 39343B, Andlaus, Andreas S., Archiv, Ath, Aths, BuSchu, Bukk, Capaci34, Coaster J, Cologinux, Corrigo, DH8JF, Diba, DutiesAtHand, Echoray, Eschweiler, Fedi, Fkoch, Fusslkopp, GottschallCh, Grenzdebiler, HaSee, Hafenbar, He3nry, Htews, Hubi, Hukukçu, Hystrix, Jailbird, Kungfuman, LKD, Lautringer Atsche, Leonach, Liberatus, MAK, Markus Hagenlocher, Matthäus Wander, Michail, Nemissimo, Nikkis, Nina, OS, P UdK, Peter 200, Phrood, Priwo, Rat, RedWyverex, Revolus, Rudolf453, Small Axe, Sternenjaeger, Terabyte, Thomas Landauer, Tönjes, Vernanimalcula, WAH, Wnme, Woches, Yarin Kaul, Zollernalb, 58 anonyme Bearbeitungen

Quelle(n), Lizenz(en) und Autor(en) des Bildes

Datei:Colossus.jpg Quelle: http://de.wikipedia.org/w/index.php?title=Datei:Colossus.jpg Lizenz: Public Domain Bearbeiter: Conscious, Edward, FSII, Fæ, Hellisp, Ian Dunster, Ibonzer, Man vyi, Mr impossible, Nixón, PKM, TedColes, 3 anonyme Bearbeitunger

Datei:ColossusRebuild_11.jpg Quelle: http://de.wikipedia.org/w/index.php?title=Datei:ColossusRebuild_11.jpg Lizenz: GNU Free Documentation License Bearbeiter: Original uploader was

Lizenz

Wichtiger Hinweis zu den Lizenzen

WICHILGET FILINGELS ZU (DEN LIZE/IZE)

Die nachfolgenden Lizzenze bezieht sich auf den Artikeltext. Im Artikel gezeigte Bilder und Grafiken können unter einer anderen Lizenz stehen sowie von Autoren erstellt worden sein, die nicht ir erscheinen. Durch eine noch vorhandene technische Einschränkung werden die Lizenzinformationen für Bilder und Grafiken daher nicht angezeigt. An der Behebung dieser Einschränkung wird gearbei Das PDF ist daher nur für den privaten Gebrauch bestämmt. Eine Weiterverbreitung kann eine Urberrechtsverlung bedeuten.

Creative Commons Attribution-ShareAlike 3.0 Unported - Deed Diese "Commons Deed" ist lediglich eine vereinfachte Zusammenfassung des rechtsverbindliche in allgemeinverständlicher Sprache. Sie dürfen: . hen Lizenzvertrages (http://de.wikipedia.org/wiki/Wikipedia:Lizenzbestimmungen_Commons_Attribution-ShareAlike_3.0_Unported)

- das Werk bzw. den Inhalt **vervielfältigen, verbreiten und öffentlich zugänglich machen Abwandlungen und Bearbeitungen** des Werkes bzw. Inhaltes anfertigen
 Zu den folgenden Bedingungen:

- Namensennung Sie müssen den Namen des Autors/Rechteinhabers in der von ihm festgelegten Weise nennen.
 Weitergabe unter gleichen Bedingungen Wenn Sie das lizenzierte Werk bzw. den lizenzierten Inhalt bearbeiten, abwandeln oder in anderer Weise erkennbar als Grundlage für eigenes Schaffen verwenden, dürfen Sie die darauffin neu entstandenen Werke bzw. Inhalte nur unter Verwendung von Lizenzbedingungen weitergeben, die mit denen dieses Lizenzvertrages identisch, vergleichbar oder kompatibel sind.
 Wobei gilt:
- Verzichtserklärung Jede der vorgenannten Bedingungen kann aufgehoben werden, sofern Sie die ausdrückliche Einwilligung des Rechteinhabers dazu erhalten Sonstige Rechte Die Lizenz hat keinerlei Einfluss auf die folgenden Rechte:
- Die gesetzlichen Schranken des Urheberrechts und sonstigen Befugnisse zur privaten Nutzung;
 Das Urheberpersönlichkeitsrecht des Rechteinhabers;
 Rechte anderer Personen, entweder am Lizenzgegenstand selber oder bezüglich seiner Verwendung, zum Beispiel Persönlichkeitsrechte abgebildeter Personen
- Hinweis Im Falle einer Verbreitung müssen Sie anderen alle Lizenzbedingungen mitteilen, die für dieses Werk gelten. Am einfachsten ist es, an entsprechender Stelle einen Link auf http://creativecommons.org/licenses/by-sa/3.0/deed.de einzubinden.

Haftungsbeschränkung
Die "Commons Deed" ist kein Lizenzvertrag. Sie ist lediglich ein Referenztext, der den zugrundeliegenden Lizenzvertrag übersichtlich und in allgemeinverständlicher Sprache, aber auch stark vereinfacht wiedergibt. Die Deed selbst enfaltet keine juristische Wirkung und erscheint im eigentlichen Lizenzvertrag nicht.

GNU Free Documentation License

Copyright (C) 2000,2001,2002 Free Software Foundation, Inc

51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA

Everyone is permitted to copy and distribute verbatim copies

of this license document, but changing it is not allowed.

0. PREAMBLE

The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially on noncommercially. Secondarily, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.
This License is a kind of "copyleft", which means that derivative works of the document must themselves be sense. It complements the GNU General Public License, which is a copyleft license designed for free

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instru

1. APPLICABILITY AND DEFINITIONS

1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A "Modified Version" of the Document mans any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "Secondary Section" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (for to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part at extbook of mathematics, a Secondary Section may not explain any mathematics). The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical opticities and possible or regarding them.

The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. In the notice that says that the Document is released under this License. A Front-Cover Text may be at most 25 words.

A "Transparent" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revisi

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

2. VERDATING COLING
You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. COPYING IN QUANTITY

3. COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

Lizenz 5

A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.

B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.

C. State on the Title page, as authors, one or more persons or entities responsible for authorship of the modified Version, as the publisher.

C. State on the Title page the name of the publisher of the Modified Version, as the publisher.

C. State on the Title page the name of the publisher of the Modified Version, as the publisher.

E. Ladd an appropriate copyright notice a flores notice for your modifications adjacent to the other copyright notices.

F. Include, immediately after the copyright notices a flores notice for your modifications and required Cover Texts given in the Document's license notice.

H. Include an unaltered copy of this License.

1. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.

1. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document and likewise the network locations given in the Document for public access to a Transparent copy of the Document, and likewise the network locations as stated in the previous sentence.

1. Preserve the network location, if any, given in the Document for public access to a Transparent

5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of lowering the bicomes notice of the combined work.

title of each such section unique by adding at me ento of it, in parentinees, me name of the original adding of parentine or the original adding or the original adding

6. COLLECTIONS OF DOCUMENTS

Volumay make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim conving of that document

7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation is users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document is less than one half of the entire aggregate, the Document Sover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is nectional covers that bracket the whole aggregate.

8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of this License or a notice or disclaimers, the original version will prevail. If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

9. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See hittp://www.egm.org/copyleft/.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.

ADDENDUM: How to use this License for your documents

copy of the License in the document and put the following copyright and license notices just after the title page:

Copyright (c) YEAR YOUR NAME.

Permission is granted to copy, distribute and/or modify this document

under the terms of the GNU Free Documentation License, Version 1.2

or any later version published by the Free Software Foundation;

with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts.

A copy of the license is included in the section entitled

"GNU Free Documentation License". If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the "with...Texts." line with this:

with the Invariant Sections being LIST THEIR TITLES, with the

Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST.

Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.

Cument contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free