An Enigma Replica and its Blueprints

Article *in* Cryptologia · January 2011

DOI: 10.1080/01611194.2010.533256 · Source: DBLP

Cryptologia, 35:16–21, 2011

ISSN: 0161-1194 print
DOI: 10.1080/01611194.2010.533256

Taylor & Francis
Taylor & Francis Group

An Enigma Replica and its Blueprints

WOLFGANG ERTEL, LUCIA JANS, WALTER HERZHAUSER, AND JOACHIM FESSLER

Abstract We present an Enigma replica project with the goal of producing ten fully functional machines, one of them dedicated for demos in a cryptology course, the others to be sold to musea or universities. The first replica is in an advanced stage. Most parts are produced and a majority of them is assembled. We intend to present the fully functional machine in 2011. For this project we created a comprehensive set of 130 drawings. We decided to share these blueprints with others and provide them online under a free public licence on http://www.enigma.hs-weingarten.de

Keywords blueprints, cryptography course, Enigma, replica

1. Introduction

In his course on applied cryptography [5], the first author uses the historic cipher machine Enigma as an example to introduce various important principles and ideas of classical ciphers. The Enigma is an ideal example for the struggle between cryptologists trying to make a crypto system secure and cryptanalysts trying to break the code. The three elements that led to successful cryptanalysis were espionage, faulty handling of the Enigma and mathematical analysis. In order to make this whole story more plastic and to show how the machine was used, the first idea was to buy a real Enigma. Since the remaining historic machines on the market are very rare and too expensive for our university budget, we decided to build a replica.

In 2003 when the project started, no blueprints of any Enigmas were available and to our knowledge no replica projects were in an advanced stage.[1] We contacted a number of museum directors and finally were successful at the Wehrtechnische Studiensammlung in Koblenz [10], where Lothar Simon, the director, allowed us to disassemble his Enigma I and measure all its parts (Figure 1). With a collection of hand drawings (Figure 2) and digital images our student returned from Koblenz after four days in the basement of the museum.

A second student then started, as a scientific project, to construct a complete set of CAD plans [7]. This collection includes 130 drawings. Many of the parts to be constructed are difficult to produce, even with modern CNC machines. At this point,

[1]Meanwhile, at the time of submission we know of some replica projects such as [2, 8, 1, 3]. But they either provide simple electronic replicas only or no blueprints or complete machines are available or affordable.

Address correspondence to Wolfgang Ertel, Hochschule Ravensburg-Weingarten, Postfach 1261, Raum: K004, Weingarten, D-88241, Germany. E-mail: ertel@hs-weingarten.de

Figure 1. Images of the Enigma from the Wehrtechnische Sammlung in Koblenz that served as the model for our replica project.

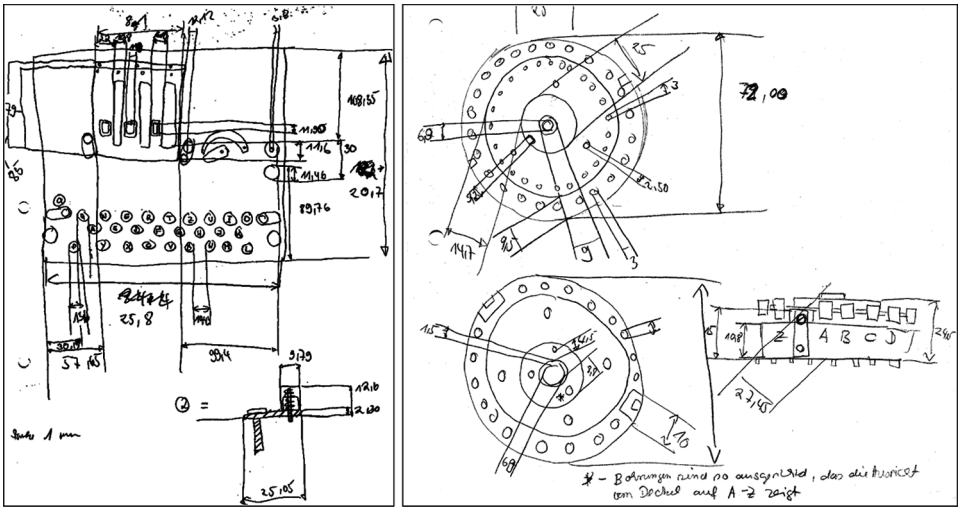

Figure 2. Two of the hand drawings.

we were able to roughly estimate the true dimension of this project. Producing all the 2698 parts (275 different types of parts) [8] is a real challenge.[2]

With CNC machines well equipped, the project could now start in the workshop of our university. Just at that time however, our workshop was facing a serious problem. The major engineer was seriously ill and thus not able to support us. The human ressources of our workshop were by far not sufficient for such a ''hobby project'' of a computer science professor. As a consequence, the production of the replica had to be outsourced. We contacted a number of precision engineering companies in Upper Swabia, the county around our university.

Finally, in February 2004, KaVo, one of the leading manufacturers of dental practice equipment, could be motivated for the project. Since that time, foremen and young apprentices are working on the replica in their training department with great enthusiasm. The Enigma is now part of the education program for precision engineers and mechtron-ics engineers. KaVo and our university agreed that, of all

[2]These figures are lower bounds on the numbers of parts. For example, the lock of the wooden box is counted here as one part, although it is built up of 12 parts.

Figure 3. The produced rotors in different views and completely mounted.

Enigma parts, enough copies should be produced to finally assemble ten complete and working machines: one for our university, one for KaVo, and eight to be sold to museums and universities.

In October 2007, all rotor parts were produced and one set of rotors and a reflector could be mounted and successfully tested as shown in Figure 3. Many other parts, for example the ground plate, the compensator and parts of the keyboard, could be finished and mounted by now (Figure 4). The production of the parts not only brings the replica project forward, but it also helps in verifying or correcting

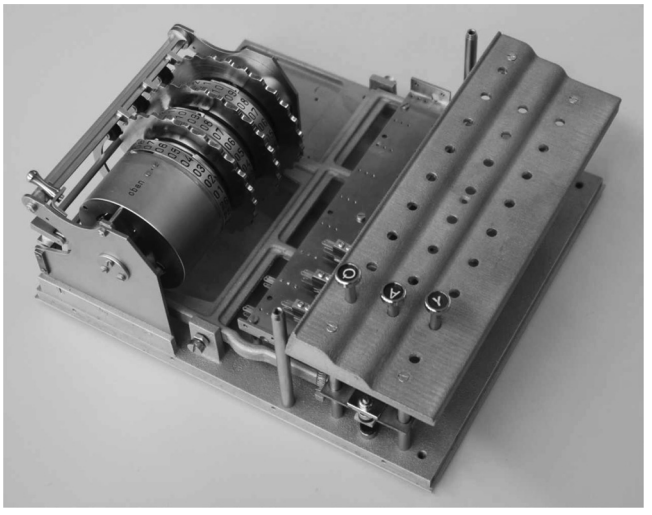

Figure 4. The partially mounted replica with compensator, rotors, parts of the keyboard and some contacts.

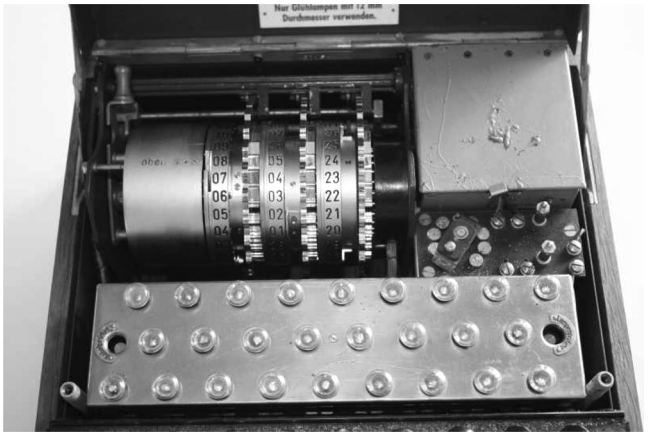

Figure 5. The original Enigma with the replica rotors and reflector mounted.

the blueprints. For example, we mounted our replica rotors and the reflector on an original enigma (Figure 5) which is different from the one we used to produce the drawings (for example, the rotors of this enigma are made of bakelite). And the old Enigma with the replica rotors worked perfectly!

2. The Blueprints

The primary focus of this project is to produce a machine that is faultless and true to the original functionality. Some Enigma collectors, however, put high emphasis on genuine materials or surface treatments. Since this is not our focus, we use modern plastic materials such as insulation material in the rotor body or high grade steel for the rotor rings. As a consequence, not all material specifications in our blueprints are genuine.

The blueprints refer to the original Enigma in the Wehrtechnischen Studiensammlung Koblenz. This is an Enigma I with the rewirable reflector D (Umkehrwalze D) [9] and device number 24b 656, produced in the year 1943 by Chiffriermaschinen AG Heimsoeht & Rinke Berlin Wilmersdorf.

The blueprints are arranged in three groups; the rack, the reflector (called reverse roll) and the rotors (called rolls). As an example, in Figure 6, we show an explosion drawing of a rotor. All 93 drawings of the rack parts are numbered ZG-10*, the 10 drawings of the reflector parts have the prefix ZG-300 and the 27 drawings of the rotor parts are numbered ZG-400*. Drawings of the battery housing and details of the contacts are still missing. We intend to deliver the contact drawings in the near future. Of course we would be grateful for additional drawings (or links to such) provided by members of the Enigma community which we could integrate into our collection.

All blueprints, in DXF-format and as PDF-files can be downloaded free of charge on http://www.enigma.hs-weingarten.de after registration [6]. Here you can also find the comprehensive report [7] and a list of all blueprints together with their level of verification which is defined as:

V0: not verified
V1: parts produced
V2: parts produced, assembled to a functional unit and tested
V3: Enigma completely assembled and working.

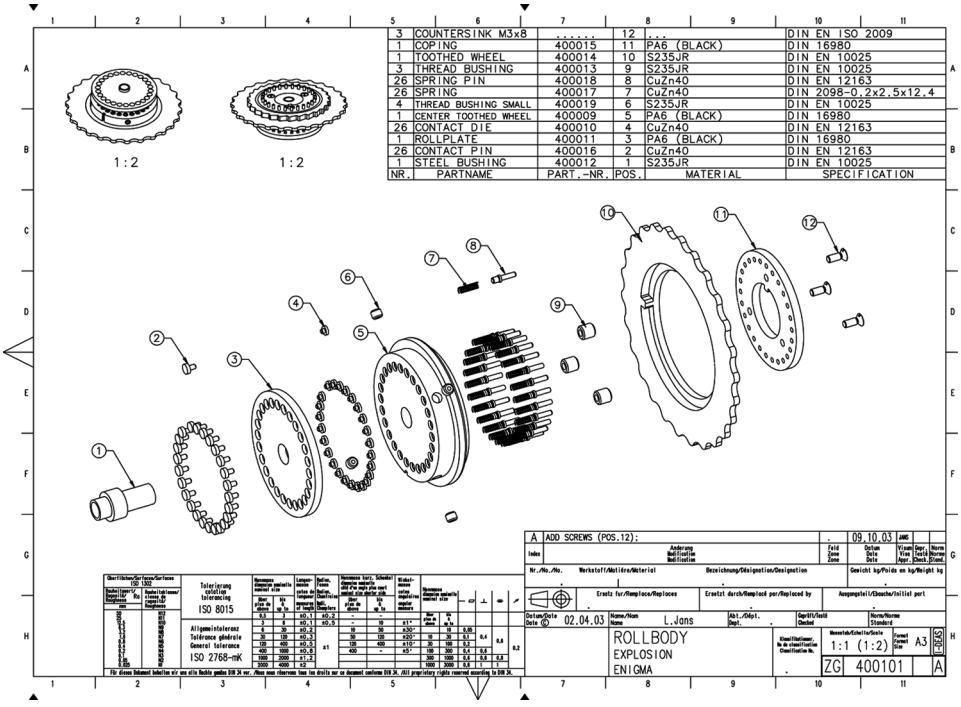

Figure 6. Explosion-drawing of a rotor.

This information will continuously be updated on the web site. Blueprints known to be faulty will be corrected and documented. A higher version number will then be attached to the file name.

Obviously, we can give no guarantee for correctness and completeness of the blueprints. Any utilization of the blueprints is at the users own risk. The drawings are available freely under the Creative Commons Licence model ''Attribution-Noncommercial-Share Alike 3.0 Unported'' [4]. This means you are free to copy, distribute, transmit and adapt the blueprints for noncommercial use, if you attribute (cite) the work appropriately. Transformed or adapted plans may be distributed under the same license only.

3. Conclusion and Acknowledgments

During the seven years of this replica project, we learned a lot about the mechanical complexity of the Enigma, and in particular, about the problems of producing Enigma parts even with modern CNC machine tools. In order to make similar projects a little easier for others, we now share our blueprints with the world wide Enigma community. And of course we welcome any additional drawings or information about Enigma replicas.

We are grateful to all persons who volunteered in our Enigma replica project. In particular, we like to express our thanks to Lothar Simon from the Wehrtechnische Studien-sammlung Koblenz for allowing us to inspect their original Enigma, to Serkan Ermurat for measuring the Enigma and producing the photos and hand drawings, to all the foremen and apprentices involved in the project at KaVo,

Biberach for the production of parts and the correction of the drawings as well as to Thomas Handtmann and his company in Biberach for the production of casting parts. We also want to thank Klaus Kopacz for his many hints and advice on difficult detail questions, Oskar Stuürzinger from the Crypto AG in Zug for Enigma documentation and a Hagelin CD-57 hand cipher machine (pocket Enigma), and Dr. Helmut Otto for a hand crafted wooden Enigma box. Last, but not least we are thankful to our former students Maximilian Gaerber and Elias Drotleff for maintaining the website and to Chris Lobenschuß for establishing the contact to KaVo.

About the Authors

Wolfgang Ertel is a computer science professor at Ravensburg-Weingarten University of Applied Sciences in Germany. Besides his primary research and teaching efforts on machine learning in robotics, he is involved in cryptography. His cryptograhpy lecture notes are published as a German textbook. His textbook on artificial intelligence will soon be published in English. More information is available at http://www.hs-weingarten.de/~ertel.

Lucia Jans studied mechanical engineering and mechatronics. As her scientific project in the master mechatronics course, she prepared the complete set of CAD drawings of the Enigma presented here. Today she is working as a project manager in the area of plant engineering. The company located in Altshausen, Germany, is specialising in building waste sorting plants Europe-wide.

Walter Herzhauser is a certified electrical engineer and works as foreman in the apprenticeship department for mechanical engineering and mechatronics at KaVo Dentaltechnik in Biberach, Germany. He, his colleagues, and their apprentices are volunteering in building the Enigma replica.

Joachim Fessler did an apprenticeship as toolmaker and then studied physical engineering. Currently he works as an engineer at Ravensburg-Weingarten University of Applied Sciences. His main areas of work are the construction design, embedded programming, board design and the Enigma replica project. He maintains the Enigma website and the repository with the blueprints on http://www.enigma.hs-weingarten.de.

References

1. Crypto Museum, Enigma Electronic self build kits. March 2010. http://www.cryptomuseum.com/kits
2. Oram, J. Enigma replica. March 2010. http://www.enigma-replica.com
3. Ideen zum Sammeln. March 2010. http://www.top-collect.de (enter "Enigma" in the search box!).
4. Creative Commons. March 2010. Attribution-noncommercial-share alike 3.0 unported. http://creativecommons.org/licenses/by-nc-sa/3.0/
5. Ertel, W. 2007. *Angewandte Kryptographie*, 3rd ed. Hanser Verlag, Munich.
6. Ertel, W. March 2010. Enigma Replica Project at Hochschule Ravensburg-Weingarten, University of Applied Sciences, Weingarten. http://www.enigma.hs-weingarten.de
7. Jans, J. 2004. Die Enigma, Nachbau der legendäaren Chiffriermaschine. Scientific Project, Hochschule Ravensburg-Weingarten.
8. Kopacz, K. March 2010. Personal communication.
9. Marks, P. April 2001. Umkehrwalze D: Enigma's rewirable reflector – part 1. *Cryptologia* 25(2): 101–141.
10. Simon, L. March 2010. Die Wehrtechnische Studiensammlung im BWB. http://de.wikipedia.org/wiki/Wehrtechnische_Studiensammlung_Koblenz