

Amateur Cryptologists Crack German Naval Codes

Two secret German naval messages - undeciphered since the Second World War - have been broken by amateur cryptologists in the last few weeks with the help of hundreds of home computers.

The second of three unsolved messages published in the journal *Cryptologia* ten years ago was cracked on March 7, just two months after German-born violinist and amateur cryptologist Stefan Krahl launched an effort called the M4 Message Breaking Project.

Krahl coupled powerful code-breaking algorithms developed by Geoff Sullivan and Frode Weierud with the power of distributed computing. At least 2,500 people around the world have signed on to the project, allowing their computers' idle time to be used to crack the codes. One message from the M4 Message Breaking Project still remains to be cracked.

Sullivan and Weierud reported on the groundbreaking algorithms in their 2005 article "Breaking German Army Ciphers" (*Cryptologia* Volume 29, Number 3), as well as another dozen messages from 1941 and 1945 that remain to be broken. To view the article online free of charge, visit http://www.tandf.co.uk/journals/pdf/papers/ucry_06.pdf

"The main reason why these messages remained unsolved is simply that before we developed our algorithm, there was no known method of attacking authentic Enigma ciphers where the content was unknown," says Weierud, who together with Sullivan developed techniques to crack about 500 Enigma messages.

Krahl announced the cracking of the second code on his website on March 7. The decoded messages are reports intercepted from German U-boats in the North Atlantic in 1942, a time when the Germans had just adopted an advanced Enigma machine known as the M4.

One of the Nazi regime's most important weapons, the Enigma machine employed a series of continuously changing rotor wheel combinations, coupled with

letter swaps, to produce coded messages. This resulted in almost 16 billion ways to encrypt a message keeping the selected plug connections fixed.

The Germans thought the code was unbreakable, but Allied cryptologists cracked it and are credited with shortening the war by as much as two years. In recent years, however, some messages have come to light whose contents are unknown.

Unlike the famous wartime Allied code-breakers at Bletchley Park in the U.K., modern-day cryptologists have no clues to the content of the messages and have had to rely on statistical techniques and computing power.

“The first break on February 20 brought a large number of contributors to the project,” says Weierud. “Some probably do it out of a team spirit and to make a contribution to a community project. Others are really keen computer programmers and see this as an interesting challenge.”

“This breakthrough has given us valuable historical information on how the Enigma machines were used and misused by the Germans,” says Weierud. “For the first time we are able to see in real, authentic messages some of the flaws and errors that were heavily exploited at Bletchley Park.”

Cryptologia: A Quarterly Journal Devoted to All Aspects of Cryptology

is the only scholarly journal in the world dealing with the history, the technology, and the effect of communications intelligence. It fosters the study of all aspects of cryptology-technical as well as historical and cultural.

The journal's articles have told for the first time how a special agency prepared information from codebreaking for President Roosevelt, have described the ciphers of Lewis Carroll, and explained the linguistic basis of the Navajo language use by codetalkers in the Pacific.

Subscription information for *Cryptologia* or a sample copy can be obtained from the address below. The journal can be viewed online at

<http://www.tandf.co.uk/journals/titles/01611194.asp>.

For subscription information, or to order a sample copy, contact:
Taylor & Francis
Customer Service Department
325 Chestnut St., Ste 800

To submit an article, contact:
Dr. Brian Winkel, Editor
PRIMUS and Cryptologia
Department of Mathematical Sciences
United States Military Academy
West Point NY 10996 USA
845-938-3200
Brian.Winkel@usma.edu

Philadelphia, PA 19106
or Phone: 1-800-354-1420 Ext. 216
or Email: customerservice@taylorandfrancis.com

Additional information can be obtained at:

<http://cryptocellar.org/bgac/index.html>

Geoff Sullivan and Frode Weierud's website that explains how the codes were broken, places the M4 project in context and includes a copy of their 2005 *Cryptologia* article, "Breaking German Army Ciphers."

http://www.bytereef.org/m4_project.html

Website of the M4 Message Breaking Project, which contains the original coded text as well as the translation of the messages.

http://en.wikipedia.org/wiki/Enigma_machine

Information about the German Enigma machine

<http://www.tandf.co.uk/journals/titles/01611194.asp>

Further subscription and editorial information for *Cryptologia*

The messages

First message (cracked February 20, 2006):

Forced to submerge during attack, depth charges. Last enemy location 08:30h, Marqu AJ 9863, 220 degrees, 8 nautical miles, [I am] following [the enemy]. [Barometer] falls [by] 14 Millibar, [wind] north-northeast [force] 4, visibility 10 [nautical miles]. Looks.

Second message (cracked March 7, 2006):

Found nothing on convoy's course 55°, [I am] moving to the ordered [naval] square. Position naval square AJ 3995. [wind] south-east [force] 4, sea [state] 3, 10/10 cloudy, [barometer] [10]28 mb [and] rising, fog, visibility 1 nautical mile. Schroeder

The third message (still unsolved):

HCEY ZTCS OPUP PZDI UQRD LWXX FACT TJMB HDVC JJMM ZRPY IKHZ AWGL YXWT
MJPQ UEFS ZBCT VRLA LZWX VXTS LFFF AUDQ FBWR RYAP SBOW JMKL DUYU PFUQ
DOWV HAHC DWAU ARSW TKCF VOYF PUFH VZFD GGPO OVGR MBPX XZCA NKMO NFHX
PCKH JZBU MXJW XKAU OD?Z UCVC XPFT

Historical Background

The messages originate from German submarines that were attacking Allied ships in the North Atlantic in 1942. They were sent during a 10-month "blackout" period in which the Allies were unable to decode German naval messages because of the introduction of a new machine with more rotors called the M4

The messages are primarily of interest for the information they provide about the strengths and weakness of the German codes. Studies of a larger number of these messages have revealed that German telegraph operators created weaknesses in the code by repeatedly using their initials or other common letter combinations as the "key" to the coded message for the day.

The first message that was broken was sent by Kapitänleutnant Hartwig Looks, commander of a German submarine, and intercepted November 19th, 1942. The submarine survived the battle that day and continued in operation until all of its crew was captured in a battle with the Royal Navy in 1944.