Thursday, 2 March 2006, 08:23 GMT

Online amateurs crack Nazi codes

By Adam Blenford
BBC News

Three German ciphers unsolved since World War II are finally being cracked, helped by thousands of home computers.

The codes resisted the best efforts of the celebrated Allied cryptographers based at Bletchley Park during the war.

Now one has been solved by running code-breaking software on a "grid" of internet-linked home computers.

The complex ciphers were encoded in 1942 by a new version of the German Enigma machine, and led to regular hits on Allied vessels by German U-boats.

Allied experts initially failed to deal with the German adoption in 1942 of a complex new cipher system, brought in at the same time as a newly upgraded Enigma machine.

The advancement in German encryption techniques led to significant Allied losses in the North Atlantic throughout 1942.

"*Forced to submerge during attack. Depth charges. I am following the enemy*"
Kapt Hartwig Looks
25 November 1942

The three unsolved Enigma intercepts were published in a cryptography journal in 1995 and have intrigued enthusiasts ever since.

Although assumed to have little historical significance, they are thought to be among just a handful of German naval ciphers in existence still to be decoded.

Exponential growth

The latest attempt to crack the codes was kick-started by Stefan Krah, a German-born violinist with an interest in cryptography and open-source software.

Mr Krah told the BBC News website that "basic human curiosity" had motivated him to crack the codes, but stressed the debt he owed to veteran codebreaking enthusiasts who have spent years researching Enigma.

UNSOLVED CIPHER #1

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

He wrote a code-breaking program and publicised his project on internet newsgroups, attracting the interest of about 45 users, who all allowed their machines to be used for the project.

Mr Krah named the project M4, in honour of the M4 Enigma machine that originally encoded the ciphers.

There are now some 2,500 separate terminals contributing to the project, Mr Krah said.

"The most amazing thing about the project is the exponential growth of participants. All I did myself was to announce it in two news groups and on one mailing list."

Nevertheless, in little over a month an apparently random combination of letters had been decoded into a real wartime communication.

In its encrypted form the cipher makes no sense at all, reading as follows:

"NCZW VUSX PNYM INHZ XMQX SFWX WLKJ AHSH NMCO CCAK UQPM KCSM HKSE INJU SBLK IOSX CKUB HMLL XCSJ USRR DVKO HULX WCCB GVLI YXEO AHXR HKKF VDRE WEZL XOBA FGYU JQUK GRTV UKAM EURB VEKS UHHV OYHA BCJW MAKL FKLM YFVN RIZR VVRT KOFD ANJM OLBG FFLE OPRG TFLV RHOW OPBE KVWM UQFM PWPA RMFH AGKX IIBG"

Unencrypted and translated into English, the message suddenly comes to life:

"Forced to submerge during attack. Depth charges. Last enemy position 0830h AJ 9863, [course] 220 degrees, [speed] 8 knots. [I am] following [the enemy]. [barometer] falls 14 mb, [wind] nor-nor-east, [force] 4, visibility 10 [nautical miles]."

A check against existing records confirmed that the message was sent by Kapitanleutnant Hartwig Looks, commander of the German navy's U264 submarine, on 25 November 1942.

Sophisticated

During the war, teams of codebreakers based at Bletchley Park, in the UK, scrambled to unravel German communications in an attempt both to undermine the German war machine and to save the lives of soldiers and seamen.

Using early computers, Bletchley Park decoded thousands of intercepts in a knife-edge race to head off U-boat attacks.

German messages were encoded using the fearsome Enigma machine, which used a series of rotors, often augmented by a so-called "plugboard", to scramble transmissions not meant for Allied eyes.

The machines used ever-changing rotor wheel combinations and electrical currents to produce unique coded messages.

Plugboards further complicated matters by swapping pairs of letters over during the encoding process, greatly increasing the numbers of possible encryptions.

UNSOLVED CIPHER #2

- TMKF NWZX FFII YXUT IHWM DHXI FZEQ VKDV MQSW BQND YOZF TIWM JHXH YRPA CZUG RREM VPAN WXGT KTHN RLVH KZPG MNMV SECV CKHO INPL HHPV PXKM BHOK CCPD PEVX VVHO ZZQB IYIE OUSE ZNHJ KWHY DAGT XDJD JKJP KCSD SUZT QCXJ DVLP AMGQ KKSH PHVK SVPC BUWZ FIZP FUUP

Stefan Krah's computerised codebreaking software uses a combination of "brute force" and algorithmic attempts to get at the truth.

The combined approach increases the chances of stumbling across a match by recreating possible combinations of plugboard swaps while methodically working through combinations of rotor settings.

Proud milestone

Bletchley Park and its codebreakers have been immortalised on television, in film and in best-selling novels.

Now a museum, staff at the site are not attempting to close the book on World War II by solving any remaining ciphers. That they leave to the enthusiasts.

But a spokeswoman said that Bletchley Park followed the M4 project with interest, describing Mr Krah's work as a "great tribute" to the achievements of the wartime codebreakers.

Ralph Erskine, who submitted the original intercepts to the journal Cryptologia in December 1995, told the BBC News website that cracking the German codes after more than 63 years would be an important milestone for amateur cryptologists.

"I think there is more satisfaction for people engaged in the project to know that they have been able to do something that Bletchley Park couldn't do," he said.

E-mail this to a friend

Related to this story:
Code points away from Holy Grail (26 Nov 04 | Beds/Bucks/Herts)
Wartime code-breakers failed to click (20 Oct 04 | UK)
Science centre opens at Bletchley (15 Oct 04 | Beds/Bucks/Herts)
Enigma station is put up for sale (24 Jul 04 | Scotland)
Return of Colossus marks D-Day (01 Jun 04 | Technology)
Paxman returns Enigma machine (01 Apr 02 | England)
Code breaker reveals her secret (28 Sep 01 | Entertainment)

RELATED INTERNET LINKS:
BBC History - Enigma
M4 Project
Bletchley Park
CryptoCellar
The BBC is not responsible for the content of external internet sites

SEARCH BBC NEWS: search

News Front Page | Africa | Americas | Asia-Pacific | Europe | Middle East | South Asia | UK | Business | Health | Science/Nature | **Technology** | Entertainment | Have Your Say | Week at a Glance

NewsWatch | Notes | Contact us | About BBC News | Profiles | History

^ Back to top | BBC Sport Home | BBC Homepage | Contact us | Help | ©