Secret crypto code that helped end apartheid cracked, open-sourced

Cloudflare chief technology officer John Graham-Cumming has cracked a 33-year-old password that protected the source code to a secure communications system used by anti-apartheid activists.

5 min. read · View original

Cloudflare chief technology officer John Graham-Cumming has cracked a 33-year-old password that protected the source code to a secure communications system used by the ANC during Operation Vula.

This has finally allowed the system's designer and programmer, Tim Jenkin, to open source the code he developed in the 1980s that had helped ANC leaders negotiate a peaceful end to apartheid.

Operation Vula was a mission to infiltrate key leaders such as Mac Maharaj and Charles Nqakula into South Africa while ensuring good lines of communication between them and the ANC's headquarters-in-exile in Lusaka, Zambia.

The ANC was using a simple but undefeated paper-based one-time pad (OTP) system for cryptography, which Jenkin had trained operatives in.

Jenkin was living in exile in London after escaping Pretoria Central Prison with two other inmates in 1979 by reverse-engineering the keys of ten separate doors and creating copies of them from wood.

He and co-conspirator Stephen Lee were arrested after being caught moving their equipment for manufacturing pamphlet bombs with anti-apartheid messaging, which they had set off around Cape Town between 1975 and 1978.

Their caper was immortalised in the 2020 film *Escape from Pretoria*, in which Harry Potter star Daniel Radcliffe played Jenkin.

After reaching London, Jenkin became the ANC's communications officer and developed the OTP-based system for secure communication between operatives and their handlers.

While the encryption itself is uncrackable, provided keys are properly randomly generated, one-time pad systems have several other vulnerabilities.

If an adversary gets their hands on the pre-generated keys and are able to intercept every message from then on, they can decrypt them.

Operatives must also adhere to strict operational security protocols, such as destroying decrypted messages, old key pages, and old enciphered messages.

However, the main problem, Jenkin found, was that encryption and decryption were laborious.

To fix this problem, it had to be easy for operatives and their handlers to send much longer messages.

In the early eighties, computers were getting cheaper, and Jenkin believed a program to automate the cryptography could solve their communications problem.

Toshiba T1000, personal computer used during Operation Vula

Together with new partner-in-crime Ronnie Press, they began work on a system that would eventually become a fully-fledged underground electronic communications network.

Although one of the first rules of cryptography is “don’t invent your own”, Jenkin said that due to the unique circumstances under which they operated, they could not use cryptographic software that was already available.

“Even in those days, 25 years before Edward Snowden, there was talk about ‘backdoors’ in encryption software,” Jenkin previously told MyBroadband.

Jenkin and Press decided it was too complex to build their own public-key system, so they opted for a computerised version of the one-time pad.

While their cryptography would remain simple, the whole communications system ended up having a lot more moving parts than just the software, as most of the Internet did not yet exist.

Encrypted messages were transmitted into a signal that could be played over a regular telephone call and recorded. This allowed operatives to easily receive messages via public telephones.

The recorded message could then be played back into a computer via a modem and decrypted.

However, keys had to be distributed to the two communicating parties to encrypt or decrypt messages.

For this, Jenkin wrote random data to 1.44MB “stiffy” disks. These keys and the encryption program itself then had to be delivered to operatives in the field.

Enter Conny Braam, head of the Dutch anti-apartheid movement, who found a KLM air hostess sympathetic to their cause.

The hostess, Antoinette Vogelsang, helped smuggle the computers, disks, and other equipment ANC operatives in South Africa needed.

Vogelsang’s role was critical if the system was going to work. Had she provided copies of the disks to the South African authorities, the whole endeavour would have been compromised.

With everything in place, the ANC kicked off Operation Vula.

Tim Jenkin — then and now

In 1989, Operation Vula would achieve its greatest victory — re-establishing secure communications between Nelson Mandela in South Africa and ANC president Oliver Tambo in Lusaka, Zambia.

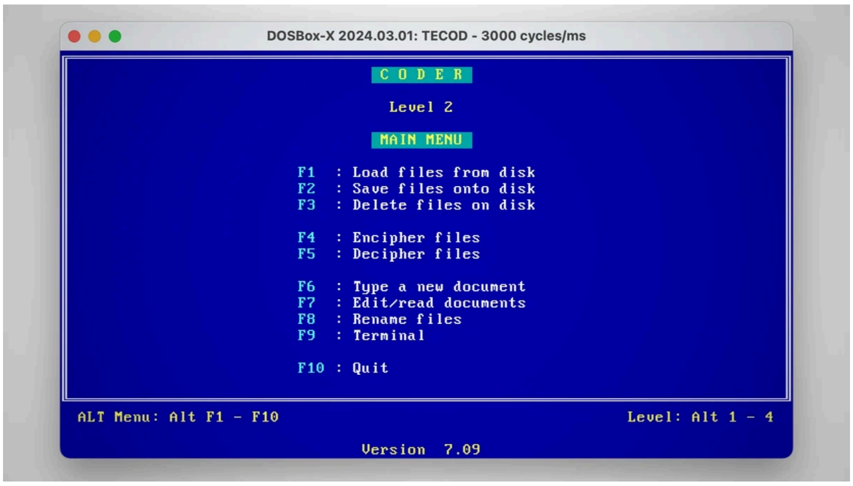
Mandela had been transferred from prison to house arrest as part of negotiations to transition to a democratic South Africa.

However, the apartheid government kept Mandela isolated from the rest of the ANC in the hopes of securing more favourable terms by creating the impression they were negotiating solely with him.

While it was not possible to smuggle a computer and disks to Mandela, messages were relayed in the covers of books.

Mandela's replies could then be smuggled out, encrypted using the software, and transmitted to Tambo in Lusaka.

“Messages from Mandela became a regular feature and in response there were long memos from Oliver Tambo in Lusaka,” said Jenkin.



DOSBox-X 2024.03.01: TECOD - 3000 cycles/ms

```
                         C O D E R

                          Level 2

                         MAIN MENU

                  F1  : Load files from disk
                  F2  : Save files onto disk
                  F3  : Delete files on disk

                  F4  : Encipher files
                  F5  : Decipher files

                  F6  : Type a new document
                  F7  : Edit/read documents
                  F8  : Rename files
                  F9  : Terminal

                  F10 : Quit

 ALT Menu: Alt F1 - F10                             Level: Alt 1 - 4

                        Version  7.09
```

Screenshot of TECOD.EXE, the one-time pad-based encryption and decryption software Tim Jenkin developed for Operation Vula

Graham-Cumming wrote that he became interested in Operation Vula a while ago and reached out to Jenkin to find out if the code had ever been open-sourced.

Jenkin explained that the only reason he hadn’t published the code until now was because he had compressed it into a password-protected ZIP file in 1991 when he returned to South Africa.

Negotiations between the ANC and the apartheid regime were still in full swing, and it was far from certain that they would be successful — hence the need to encrypt the code.

Unfortunately, when Jenkin tried to unzip the file years later, he realised he had forgotten the password.

“I thought I would never forget the password, but when I tried to decode it a few years later, I couldn’t remember it,” he said.

After Graham-Cumming cracked the password, Jenkin uploaded the nearly 40-year-old PowerBASIC code to Github.

Cracking it was no easy feat, even though the ZipCrypto scheme used in PKZIP from that era has a known plain text vulnerability. There is also an open-source implementation of an exploit for it called bkcrack.

Graham-Cumming explained that all he had to do was predict 12 bytes of plain text at a known location inside the ZIP file.

After crafting an attack on the ZIP files, aided by Jenkin’s knowledge of their contents, bkcrack ran for 23 minutes to return with a decryption key.

Graham-Cumming compiled and ran two of Jenkin’s lost programs and posted screenshots and videos of them in action on his blog.

The first generated disks with the random keys necessary for one-time pad encryption, while the other performed the encoding and decoding.

“There are lots of interesting details of how these programs work that deserve another longer blog post when I have time. Or a detailed study by someone else,” Graham-Cumming said.

“For example, the key material is destroyed after use, the RANDOM.EXE program has multiple ways of making randomness and code to check the distribution of the random bytes created. There’s an emphasis on using the RAM disk for all cryptographic operations.”