mybroadband.co.za

How the ANC sent encrypted messages in the fight against apartheid

8–10 minutes

In the last decade of apartheid, the ANC faced many obstacles in its fight against the National Party's regime in South Africa.

ANC leaders were either in exile or imprisoned, and members of the underground resistance in South Africa had no easy way to communicate with leadership holed up elsewhere on the continent.

The need to encrypt messages so they couldn't be intercepted and read by South African security forces made communication difficult.

Encrypting and decrypting messages by hand using a system such as the one-time pad (OTP) that the ANC had adopted was time-consuming.

Cumbersome cryptography was also only part of the problem. The ANC leadership had been too far removed from operatives on the ground for too long.

Thus Operation Vula was born: Infiltrate key leaders such as Mac Maharaj and Charles Nqakula into South Africa, and ensure there were good lines of communication between them and the ANC's headquarters-in-exile in Lusaka, Zambia.

Prior to Operation Vula, though, the ANC used a method of encryption known as the one-time pad.

One-time pad encryption

How one-time pad encryption works

Sender

1. Randomly assign numbers to the various characters you wish to use

2. Randomly generate a page full of numbers between 0 and 9
(The ANC arranged digits in groups of 5)

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
28	76	79	04	77	47	90	64	28	56	53	37	60	93	82	26	80	59	69	16

U	V	W	X	Y	Z	#	.	,	?	0	1	2	3	4	5	6	7	8	9
98	01	66	81	95	12	27	31	11	43	72	33	28	87	57	92	42	25	45	28

★	63916	74006	97575	14174	30172	42795	56857	52163	76133	64882 ★
	21249	58238	78464	22649	02515	88976	19744	79293	17163	68622

• • •

3. Repeat steps 1 and 2 until you have a pad full of pages

4. Make a copy of the pad and give it to the person you want to communicate with

5. Write your message

(Plaintext)

MEET AT 10 TOMORROW.

6. Encode letters into their matching numbers

	M	E	E	T	#	A	T	#	1	0	#	T	O	M	O	R	R	O	W	.	
●	60	77	77	16	27	28	16	27	33	72	27	16	82	60	82	59	59	82	66	31	●

7. Take digits from the page you generated and write them underneath the numerically-encoded letters

8. Add the top numbers to the bottom numbers using modulo arithmetic

	M	E	E	T	#	A	T	#	1	0	#	T	O	M	O	R	R	O	W	.	
●	60	77	77	16	27	28	16	27	33	72	27	16	82	60	82	59	59	82	66	31	●
★	63	91	67	40	06	97	57	51	41	74	30	17	24	27	95	56	85	75	21	63	★
▲	23	68	34	56	23	15	63	78	74	46	57	23	06	87	77	05	34	57	87	94	▲

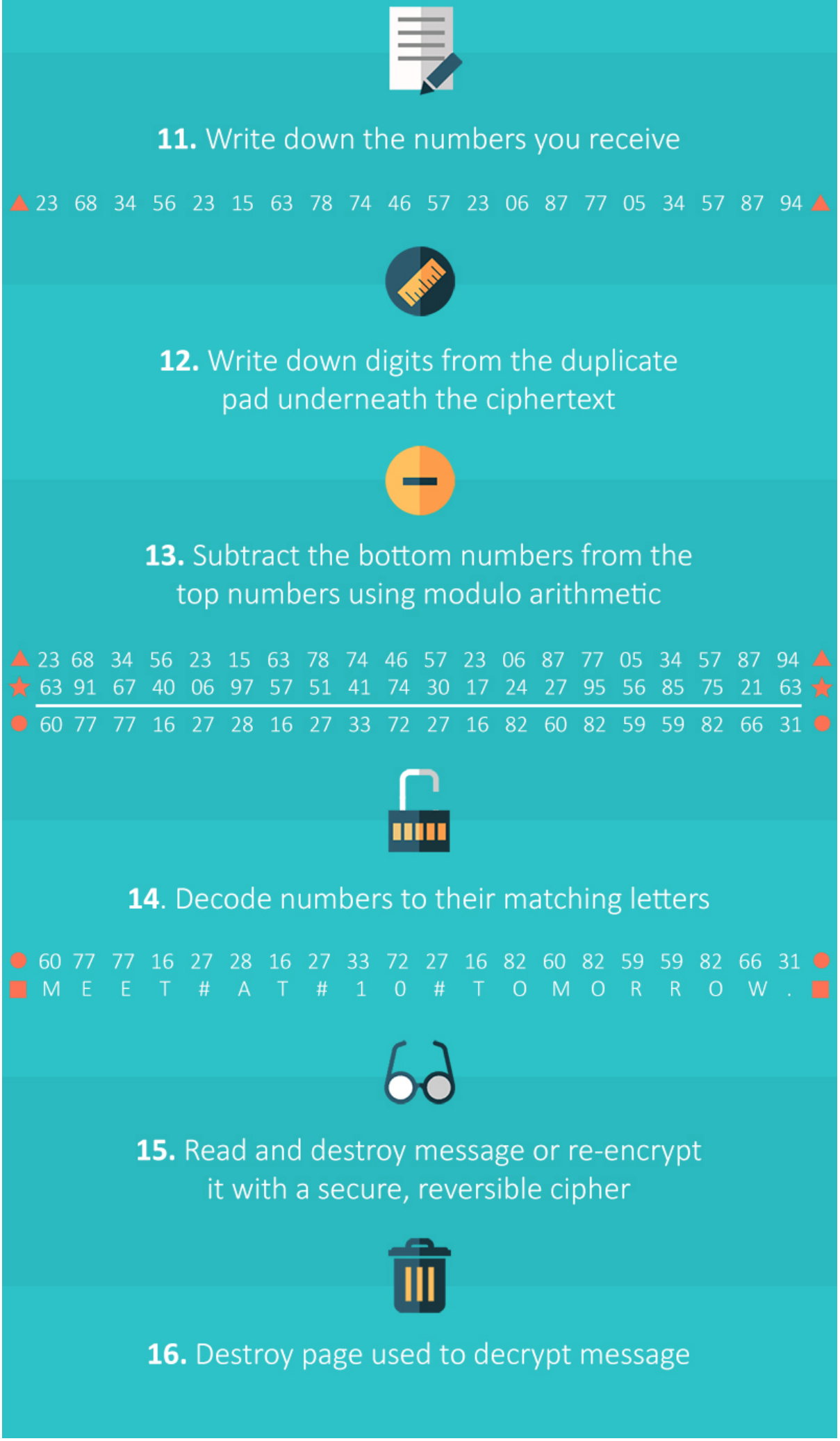
9. Transmit the ciphertext

▲ 23683 45623 15637 87446 57230 68777 05345 78794 ▲

10. Destroy the page you used to encrypt the message, and the message

Receiver executes steps 5-8 in reverse:

Receiver



OTP is a theoretically uncrackable cipher which requires that the sender and receiver each have identical copies of a secret numeric

“key”.

For the message to remain secure, the key used to encrypt or decrypt a message must be destroyed immediately after being used.

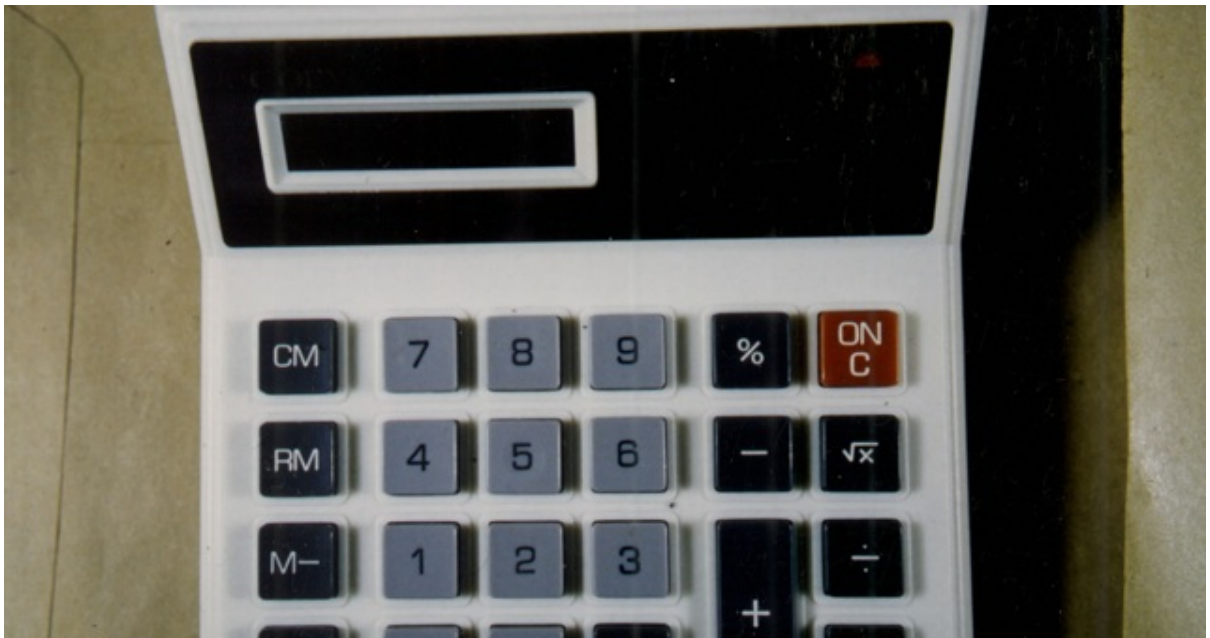
The “plaintext” or decrypted message itself must also either be re-encrypted with a reversible cipher, or destroyed.

Tim Jenkin, who was a communications officer for the ANC from around 1979, helped develop the one-time pad system the organisation used – along with a way to send messages electronically:

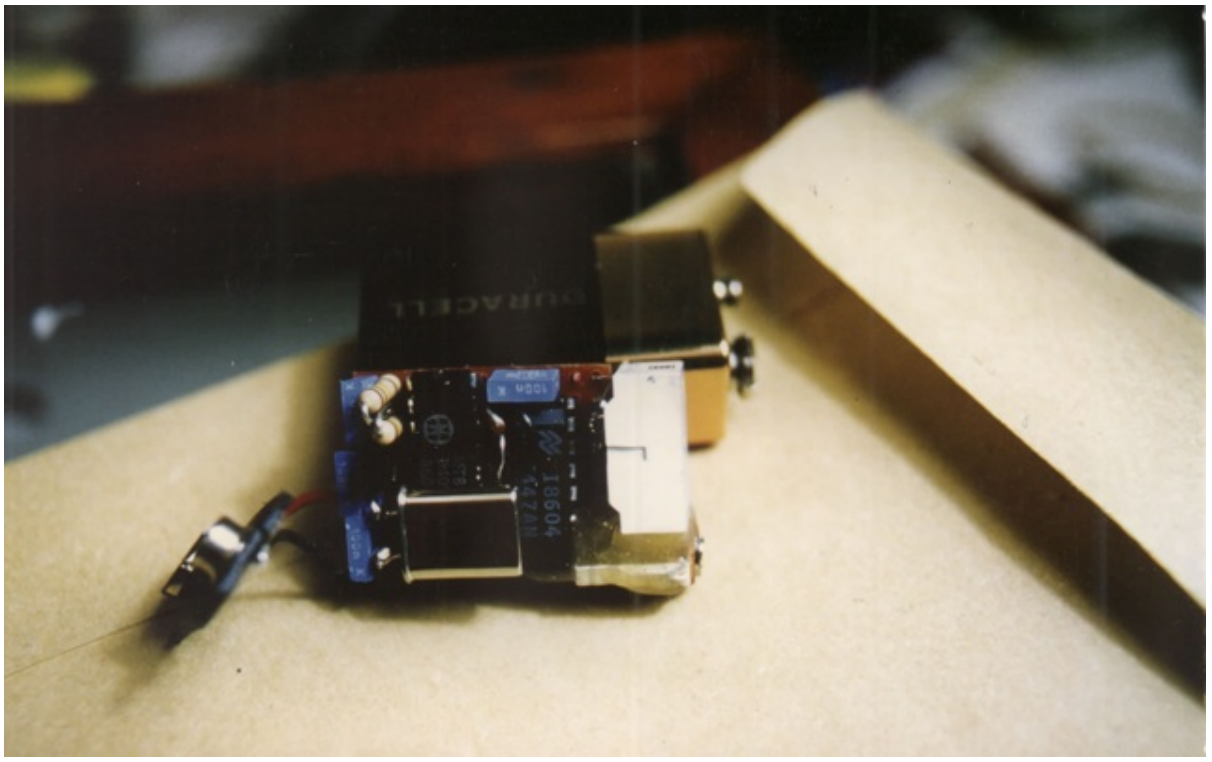
- Encrypted messages were encoded into a series dual-tone multi-frequency (DTMF) sounds, which are used by normal telephones.
- These DTMF tones were recorded onto a cassette tape.
- Operatives would call a “message drop” answering machine from a payphone.
- The recorded DTMF tones were played back from the cassette into the phone’s receiver.

  To create these tones, a DTMF generator disguised as a calculator was used.

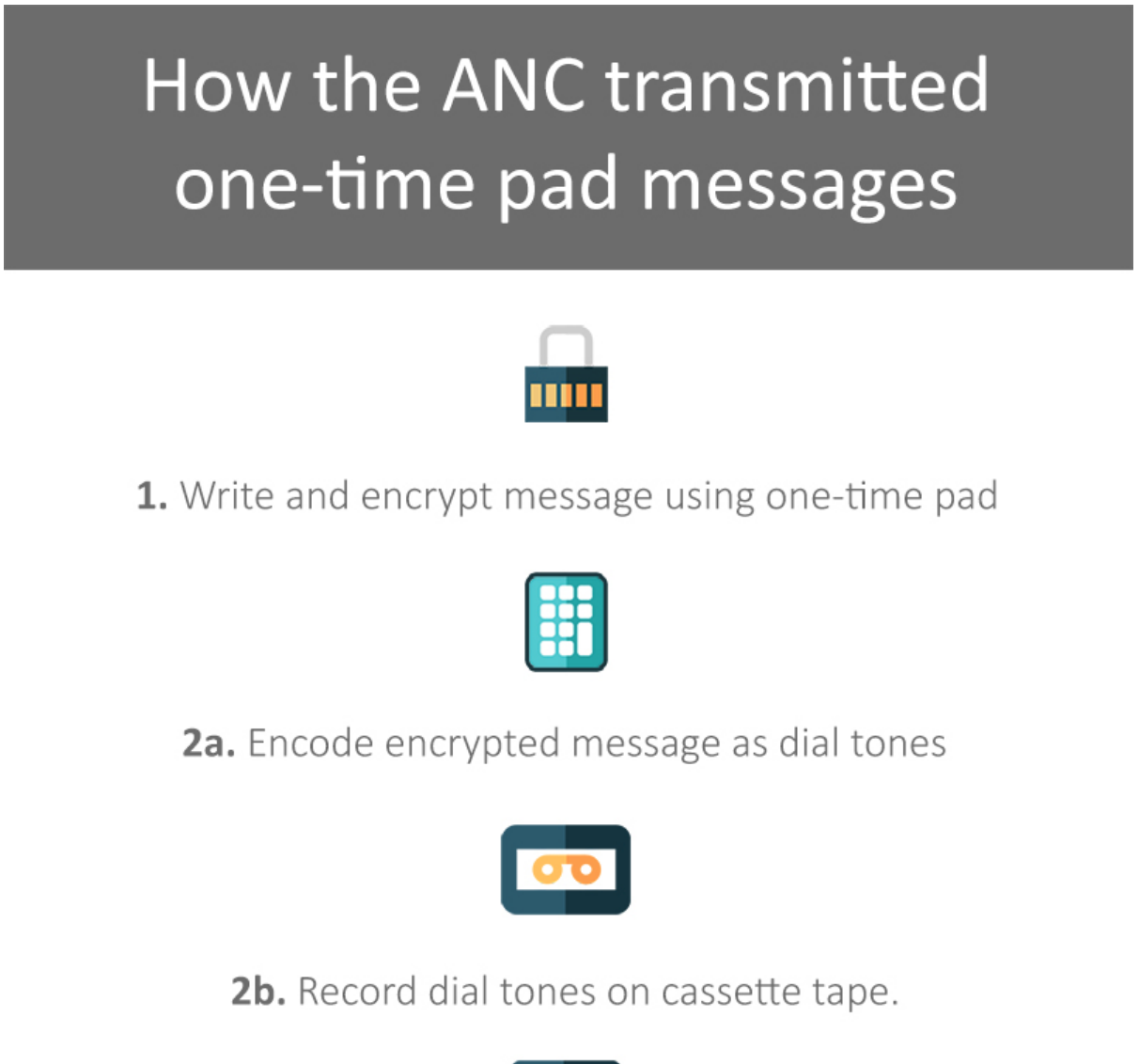
  The “calculator” could also be used to decode DTMF tones into digits, which then had to be manually decrypted with a one-time pad.



Modified dial tone calculators



Miniaturised DTMF decoder atop a 9V battery. It displayed the numbers of DTMF tones fed into it.



3. Phone message drop
(answering machine)

4. Play recorded dial tones into phone receiver

Computerised encryption for Operation Vula

For Operation Vula to succeed, the ANC leaders who infiltrated South Africa needed a way to send more detailed messages back to Lusaka.

Between 1984 and 1987 Jenkin and a colleague, Ronnie Press, worked on a computer program to automate the OTP encryption and decryption the ANC used.

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

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

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

Characters were assigned random values from 0 to 127 (7-bit ASCII), and later from 0 to 255 (8-bit ASCII). Normal modulo arithmetic was applied to encrypt the message once, followed by bitwise encryption (using exclusive-or, or XOR).

Jenkin provided the following snippet of code which shows an early version of the encryption subroutine, written in PowerBASIC.

```
 SUB EncVerFD(MSG$,SNUM$,SALF())
    LOCAL BM,CP
    LENMSG=LEN(MSG$)
    $EVENT OFF
    FOR ENC=1 TO LENMSG
        RL=ASC(MID$(SNUM$,CP+1,1))
        CH=SALF(ASC(MID$(MSG$,ENC,1)))
        CD=(RL XOR CH) MOD 128
        MOUT$=CHR$(CD+32)
        IF (ENC+2) MOD 10=0 THEN
MOUT$=MOUT$+CHR$(160+BM):INCR BM
        PUT$ #1,MOUT$
        CP=ENC MOD 3000:BM=BM MOD 15
    NEXT ENC
    $EVENT ON
    EM$=STRING$(5,175)
    PUT$ #1,EM$
END SUB
```

Trying to use the same DTMF-based system to transmit encrypted messages proved problematic, but Jenkin said they had a breakthrough when they tried acoustic couplers for the first time.

Instead of recording tones, operatives recorded the output from an acoustic modem.

An example of what one of these messages sounded like is embedded below.

Distributing digital one-time pads

While the ANC's new secure electronic communications system was ready for prime time, the technical challenges were only half the battle.

The next hurdle was distributing cryptographic keys to everyone who would use the system.

For this they used 1.44MB floppy disks (stiffies), which were filled

with random data that could be used to encrypt and decrypt messages.

When a message was encrypted or decrypted, used key data was scrubbed by repeatedly writing zeros over those areas of the disk.

Since “keys” from these data disks could not be re-used, the ANC needed to find someone who could bring replacement disks to operatives at regular intervals.

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

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

As Jenkin notes, Vogelsang’s role was key if the encryption was going to work.

If she had provided copies of the disks to the South African authorities at the time, the system could have been compromised.

3. Perform one-time pad encryption on compressed message

4. Delete used key data from disk

5. Perform one-time key encryption

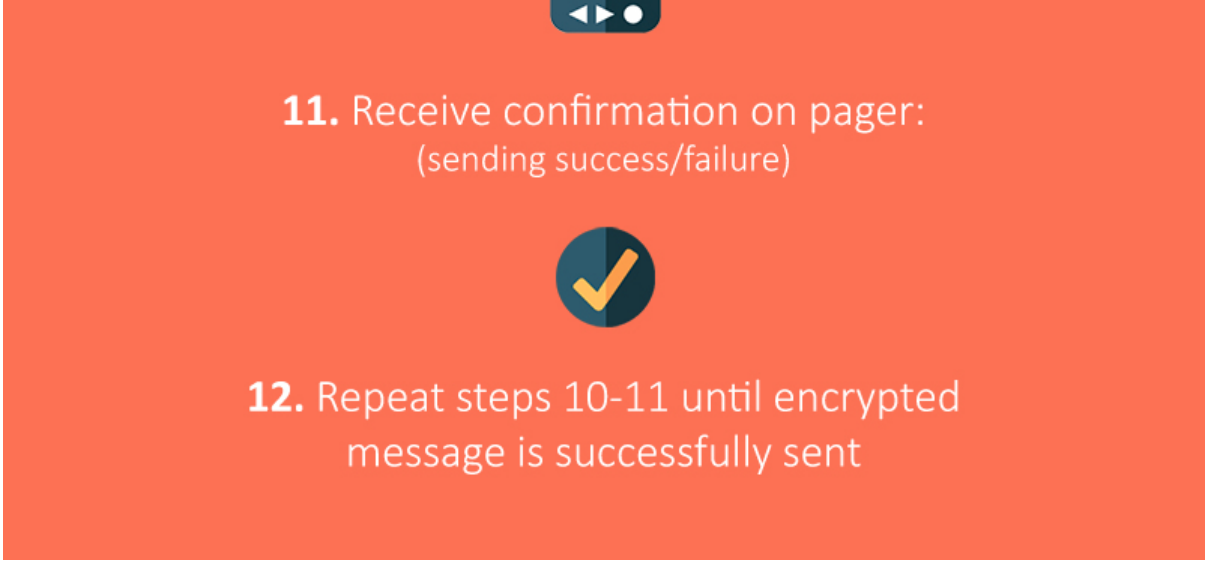
6. Delete used key data from disk

7. Repeat steps 5-6 as many times as desired

8. Record encrypted message to cassette tape over acoustic modem

9. Use payphone to call answering machine in London

10. Play cassette tape into telephone



The power of secure communications

The ANC's encryption system evolved over the course of Operation Vula, eventually incorporating e-mail as a way to transmit encrypted messages.

At the request of field operatives, Jenkin also developed a way to re-encrypt messages so that they could be stored without compromising security.

Its ultimate triumph came when Mac Maharaj managed to set up a communications channel to Nelson Mandela, who was then able to get messages out to the rest of the ANC via the central communications office in London.

Mandela was in talks with the NP regime at the time, and according to Jenkin they wanted to create the impression Mandela was negotiating with them as an individual. Little did the NP know that Mandela was in constant contact with his comrades.

"Messages from Mandela became a regular feature and in response there were long memos from Oliver Tambo in Lusaka," said Jenkin. "The two were now talking in confidence for the first time since the early 60s."

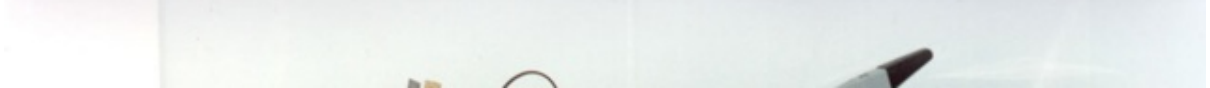
Tim Jenkin at his workstation in London

Tim Jenkin – then and now

Ronnie Press (right) and Conny Braam (centre) in Amsterdam

Operation Vula headquarters, nicknamed GCHQ after the UK's own Government Communications Headquarters

Operation Vula control centre at Ronnie Press' place. In the middle is the main Toshiba T3100 computer. Mounted on the wall are a pair of the incoming and outgoing answering machines. The acoustic modem is the white box under the bottom shelf behind the computer. On the first shelf at left are various radios used to communicate in London. In front, just to the right of the chair, is a home-made acoustic coupler attached to a mobile phone handpiece.



Close up view of the equipment

Toshiba T1000, personal computer of the revolution

Toshiba T3100, personal computer of the revolution

Another view of “GCHQ”. Not visible in the scale image are various antennas sprouting from the roof. One of these was for a high-powered cellphone, used for sending and receiving messages via an electronic answering service (“voice bank”) instead of answering machines. There were three phone lines in the flat: one for personal use, one for incoming Vula messages, and one for outgoing Vula messages. Adding more phone lines would have looked suspicious, so additional phone lines were installed at sympathisers’ homes nearby. These were connected by (illegal) high-powered cordless phones. Aerials on the roof had line-of-sight with those at the other peoples’ homes, so the reception was really good. Sophisticated commercial answering machines were installed that could be controlled remotely via the handsets in “GCHQ”.

Operation Vula workshop

Operation Vula workshop

MyBroadband would like to thank Tim Jenkin for his assistance in compiling this article.

Further reading: Talking to Vula**, by Tim Jenkin.**

Here are the leaked e-mails from SARS spy unit to Hacking Team

Signal jamming not Parliament's fault

'Big Brother' spying in South Africa exposed