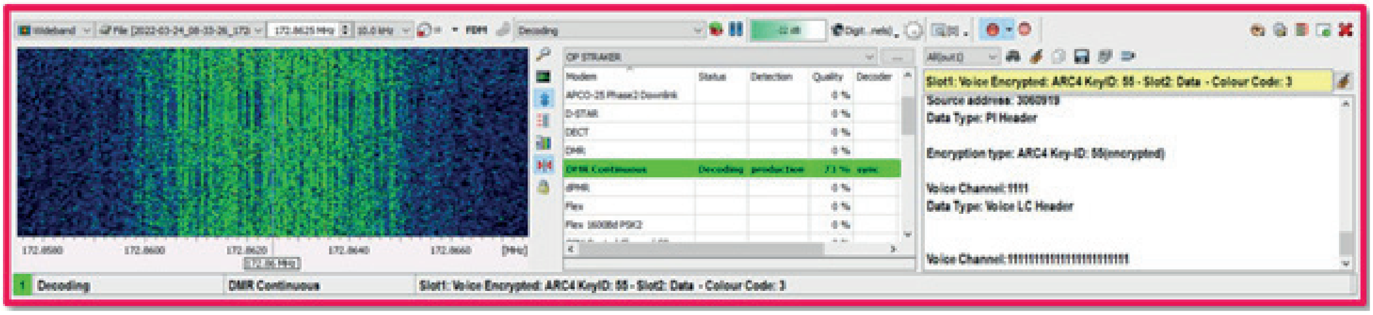
Digital Mobile Radio ‘Enhanced Privacy’ mode - ARC4 Decryption with go2key



Modem	Status	Detection	Quality	Decoder
APCO-25 Phase2 Downlink			0 %	
D-STAR			0 %	
DECT			0 %	
DMR			0 %	
DMR Continuous	Decoding	production	73 %	sync
dPMR			0 %	
Flex			0 %	
Flex 1600Bd PSK2			0 %	

Slot1: Voice Encrypted: ARC4 KeyID: 55 - Slot2: Data - Colour Code: 3

Source address: 3060919
Data Type: PI Header

Encryption type: ARC4 Key-ID: 55(encrypted)

Voice Channel: 1111
Data Type: Voice LC Header

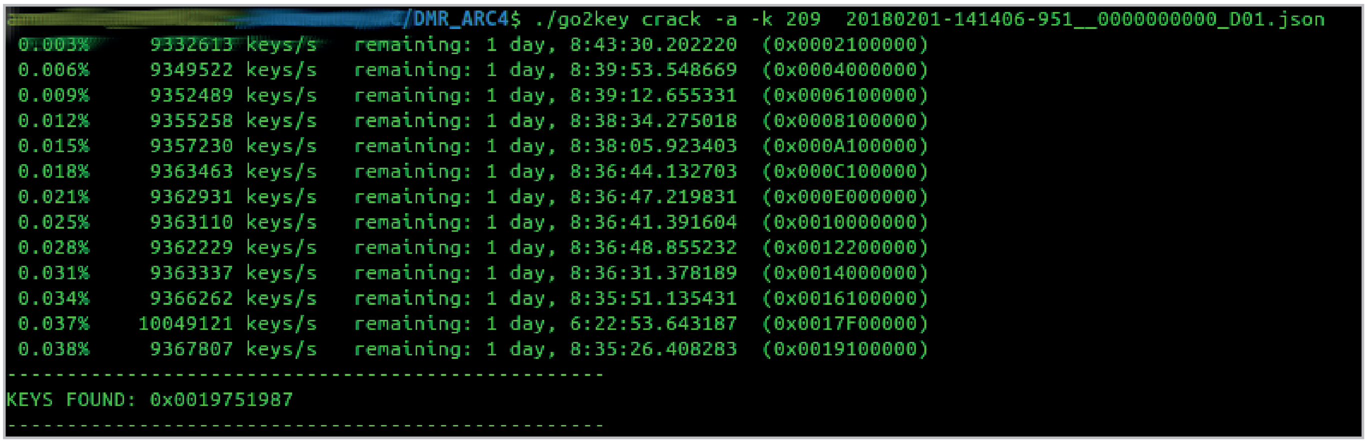
Voice Channel: 11111111111111111111111

1 Decoding | DMR Continuous | Slot1: Voice Encrypted: ARC4 KeyID: 55 - Slot2: Data - Colour Code: 3

Our R&D Team has recently developed & successfully field-tested a decryption engine for the ARC4 stream cipher. Our end-user groups are already aware that go2signals can auto-decrypt/descramble DMR networks‘ ‚Basic Privacy‘ modes such as ‘Motorola Basic’, ‘Hytera Basic’ & ‘Alinco Normal’. Using a proprietary ‚brute-force attack‘ technique, our go2signals user-communities can now decrypt the DMR Association‘s ‚Enhanced Privacy‘ mode, which employs the ARC4 cipher to encrypt its digitized speech content. This ‚Enhanced Privacy‘ mode is implemented as standard in Motorola & Hytera mid-to-high-Tier Handheld Transceivers (HTs), Mobile Units (MUs) & trunking/repeater networks, & is available as a ‘plugin’ option for other manufacturers’ DMR products & systems (e.g. Kenwood NX-series). To recover a specific DMR net‘s ARC4 encryption keys, our go2signals end-user groups can now run our ‘go2key’ ARC4 decryption engine against a DMR network’s ARC4-encrypted activations.

go2key runs with go2signals v23.2 or later. The go2key capability currently runs via command-line, but will be fully incorporated as a go2signals GUI/Remote-API plugin option during our ongoing development & implementation phases.

For further information relating to our new go2key ARC4 decryption capability, please contact sales@procitec.de.



```
[redacted]/DMR_ARC4$ ./go2key crack -a -k 209  20180201-141406-951__0000000000_D01.json
 0.003%     9332613 keys/s   remaining: 1 day, 8:43:30.202220  (0x0002100000)
 0.006%     9349522 keys/s   remaining: 1 day, 8:39:53.548669  (0x0004000000)
 0.009%     9352489 keys/s   remaining: 1 day, 8:39:12.655331  (0x0006100000)
 0.012%     9355258 keys/s   remaining: 1 day, 8:38:34.275018  (0x0008100000)
 0.015%     9357230 keys/s   remaining: 1 day, 8:38:05.923403  (0x000A100000)
 0.018%     9363463 keys/s   remaining: 1 day, 8:36:44.132703  (0x000C100000)
 0.021%     9362931 keys/s   remaining: 1 day, 8:36:47.219831  (0x000E000000)
 0.025%     9363110 keys/s   remaining: 1 day, 8:36:41.391604  (0x0010000000)
 0.028%     9362229 keys/s   remaining: 1 day, 8:36:48.855232  (0x0012200000)
 0.031%     9363337 keys/s   remaining: 1 day, 8:36:31.378189  (0x0014000000)
 0.034%     9366262 keys/s   remaining: 1 day, 8:35:51.135431  (0x0016100000)
 0.037%    10049121 keys/s   remaining: 1 day, 6:22:53.643187  (0x0017F00000)
 0.038%     9367807 keys/s   remaining: 1 day, 8:35:26.408283  (0x0019100000)
-------------------------------------------------
KEYS FOUND: 0x0019751987
-------------------------------------------------
```

Find Motorola Enhanced ARC4 encryption keys in DMR decoder output