NAME

m209 – simulate the M-209 Converter

SYNOPSIS

m209 [**–v**] [**–q**] **–c|–d** [**–k** *KeyFile*] [**–i** *i1 i2 i3 i4 i5 i6*]
< *InFile* **>** *OutFile*

m209 [**–v**] [**–q**] **–c|–d –a** [**–k** *KeyFile*] [**–l** *KeyListIndicator*]
[**–t** *KeyFileDir*] **<** *InFile* **>** *OutFile*

m209 [**–v**] [**–q**] **–g –p** [**–l** *KeyListIndicator*] **>** *KeyFile*

DESCRIPTION

m209 simulates the operation of the M–209 Converter, a cipher machine used during World War 2 and the Korean War by U.S. military forces for encryption of low-level traffic. The Army versions included the M–209, M–209–A and M–209–B, while the Navy called this machine the CSP–1500. This machine was designed by Swedish cryptographer Boris Hagelin, and shares its operating principles with various other cipher machines which are collectively referred to as "pin and lug" machines.

In addition to simulating the operation of the M–209 Converter, **m209** can also generate random key settings and automate certain tedious operating procedures.

The M-209 Converter only enciphers and deciphers the letters 'A' through 'Z'. Numbers or punctuation must be spelled out. When enciphering, the operator substitutes the letter 'Z' where a space is desired. When deciphering, the machine prints a space instead of the letter 'Z', and the operator must infer any actual 'Z' letters from context.

OPTIONS

–a Automatically generate or extract message indicators in cipher (**–c**) or decipher (**–d**) modes, respectively.

In cipher mode, if a Key List Indicator (a two-letter string) is specified with the **–l** option, **m209** will automatically try to load a key list file named *KeyListIndicator*.m209key in the directory specified with the **–t** option. Message indicators will be included in the ciphertext using the protocol specified in the Signal Corps training film TF 11–1400 *M-209 Converter*, and initial key wheel settings will be randomly generated.

In decipher mode, **m209** expects to find valid message indicators in the ciphertext, and will automatically extract the initial key wheel settings. The key list indicator is automatically extracted from the ciphertext, and **m209** will automatically try to load a key list file named *KeyListIndicator*.m209key in the directory specified with the **–t** option.

In either case, a default key setting may be specified with the **–k** option, and it will be used if a key file cannot be loaded automatically.

–c Cipher mode: Read plaintext from stdin, encipher it, and write ciphertext to stdout.

–d Decipher mode: Read ciphertext from stdin, decipher it, and write plaintext to stdout.

–g Generate random key setting. Use the **–p** option to write the resulting key setting to stdout.

–i *i1 i2 i3 i4 i5 i6*
Set initial wheel positions based on the following six arguments, which must each be a single alphabetic character.

–l *KeyListIndicator*
Use the specified key list indicator, which must be a two-character alphabetic string.

–p Print key setting to stdout. The resulting output may be redirected to a file, and is suitable for loading into **m209** using either the **–a** or **–k** options.

−t *KeyDir*
: Specify the directory in which to search for key files when using the **−a** option. Defaults to current directory.

−v
: Print verbose debugging messages to stderr.

−q
: Suppress information messages which are normally printed to stderr.

FILES

Key setting files generated by **m209** using the **−p** option include both a human-readable portion using one of the formats commonly used for M-209 keys, and a machine-readable portion which is understood by the **m209** program. When loading a key file, **m209** only parses the machine-readable portion, and ignores any other text (including the human-readable text output by the **−p** option). The machine-readable format is a compromise which allows easy parsing, yet is also easy to type by hand when it is desired to use a key setting table which was not generated by **m209**.

The machine-readable portion of the key setting file consists of a series of lines each starting with the '>' character. The first six of these lines specify the pin settings for each key wheel, and the seventh line specifies the lug settings.

Each of the six lines specifying pin settings consists of the '>' character followed by a series of '0' and '1' characters, which specify the pin settings for one wheel in sequence, starting with position 'A' on the wheel. Active pins are represented by '1', and inactive pins are represented by '0'. Each line must include the correct number of characters for the corresponding wheel, and the first line represents the pin settings for the leftmost wheel. The six wheels have 26, 25, 23, 21, 19 and 17 pins, respectively.

The line which specifies the lug settings begins with the '>' character, followed by 27 two-digit numbers separated by spaces. Each number specifies the lug settings for one lug bar. Each digit specifies the setting of one of the two lugs on that bar, and may be between 0 and 6.

Here is a sample key setting, including both human-readable and machine-readable portions:

```
M-209 KEY LIST: XY
--------------------------------
NR LUGS  1 2 3 4 5 6
--------------------------------
01 0-1   A A - A - A
02 0-1   B B B B - -
03 0-1   - C C C - -
04 0-1   - - D D - D
05 0-2   E - - - - -
06 0-3   F - - - F -
07 0-3   - - - G - G
08 0-3   - H - - H -
09 0-3   - - I - - I
10 0-3   - - J J J -
11 0-3   K - K K K -
12 0-3   L L L - L L
13 0-4   - M - - M M
14 0-6   N N N N N N
15 0-6   O O O - - -
16 0-6   - - - P P P
17 0-6   Q - - Q - -
18 0-6   R - R - R
19 0-6   - S - S S
20 1-4   T - - -
21 1-6   U - U U
22 2-4   - - -
23 3-5   - X X
```

24 3-6 - Y
25 3-6 Y Z
26 3-6 Z
27 3-6
---
26 LETTER CHECK

NZQNU PDSDU SUUUZ SFAWV SRSNA J

>11001100001101101101100011
>11100001000111100001000111
>01110000111101100100101
>111100100110010110101
>0000010101111101011
>10010010100111010
>01 01 01 01 02 03 03 03 03 03 03 03 04 06 06 06 06 06 06 14 16 24 35 36 36 36 36

EXAMPLES

m209 -g -l AB -p >AB.m209key

m209 -a -c -l AB <plain.txt >cipher.txt

m209 -a -d <cipher.txt >deciphered.txt

m209 -c -k sample.m209key -i a b c d e f <plain.txt >cipher.txt

SEE ALSO

http://en.wikipedia.org/wiki/M-209

COPYRIGHT

AUTHOR

Mark J. Blair, NF6X <nf6x@nf6x.net>
http://www.nf6x.net