

# **encio**

---

a program and library for data compression  
Copyright © 2004 Mario Juric  
version 0.1 of 12 December 2004

**Mario Juric**

---

Distributed under the GNU GPL. See Copying section for details.  
Copyright © 2004 Mario Juric

# 1 Overview

`libencio` is a library providing `stdio`-like interface for reading and writing of encrypted files in `MCrypt` format. Additionally, through creation of an "index", `libencio` provides full support for `fseek()`-like random read access of encrypted data. This allows one to operate on `MCrypt`-encrypted files as if they were ordinary, cleartext files.

The main motivation for this library was to create code for easy random access of encrypted data for a project I'm working on. This is a preliminary, proof-of-concept release, able to seek/encrypt/decrypt to `MCrypt` format only and with symmetric encryption algorithms only. The final goal is to implement reading, writing and seeking of data in `OpenPGP` format, with support for public key algorithms. As it's an open question how much time will I have to continue working on it, I'm putting it out in case someone finds it useful. I will, however, accept patches and bugfixes.

A library like this one can be used to provide MUAs (mail readers) with a layer to transparently handle encrypted attachments, or, more interestingly, as a backend to software such as `ffmpeg` or `mplayer` to directly play encrypted files without making temporary, decrypted copies. Another use would be to combine it with tar archives for encrypted backups, like `duplicity` does. A KDE IO-Slave can also be envisioned.

`libencio` uses `libmcrypt` and `libmhash` libraries for encryption and hashing algorithms, respectively. I've chosen these two mostly for their simple API. In the future, a transition to `libgcrypt` is likely, due to its wider userbase.

## 2 Requirements

libmcrypt

libmhash

### 3 Caveats and Warnings

This code has been poorly tested. Would I (the author) encrypt my most confidential files with it? No. I think it needs a more thorough checks before that, especially the random number generation routines. You have been warned.

However, it's great to use for reading files encrypted with other code!

## 4 TODO List

- Read/write OpenPGP file format
- Switch to `libgcrypt`
- Implement a seekable file format. The easiest way to do this is to encrypt the file in equal sized blocks, each with it's own IV. This keeps the encryption strong, but effectively interleaves the ENCINDEX into the file itself.

## 5 Writing Encrypted Files

`libencio` conceptually follows `stdio` in the naming and function of its function calls. This short example program demonstrates how to write an encrypted file with default encryption settings (rijndael-128/cfb mode/sha1 checksum).

```
#include <stdio.h>
#include "encio.h"

int main(int argc, char **argv)
{
    ENCFILE *ef;
    char buf[1000];
    char *passphrase = "acompliatedpassphrase";

    /* open an file encrypted with passphrase */
    ef = enc_fopen("test.txt.nc", "wb", passphrase);

    while(!feof(stdio))
    {
        int nread = fread(stdio, 1, buf, 1000)
        enc_fwrite(ef, 1, buf, nread);
    }

    enc_fclose(ef);
}
```

This short example program encrypts anything given to it from `stdio` into a file named `test.txt.nc`. All `enc_*` calls function are equivalent to their `stdio` counterparts, except they transparently encrypt the data written to the output file. There is an additional third parameter to `enc_fopen()`, compared to `fopen()`, through which you supply the passphrase to use to encrypt the data.

Note that `enc_fseek()` is not available when a file is opened in write mode – i.e., you cannot write 10 kb, then seek back to the beginning and rewrite 1 kb. This is due to the properties of the encryption mode, where each subsequent byte written depends on all of the preceding bytes - changing them would require reencryption of the whole file.

## 6 Reading and Seeking Encrypted Files

This short sample program should give you an idea what is and how to use `libencio`.

```
#include <stdio.h>
#include "encio.h"

int main(int argc, char **argv)
{
    ENCFILE *ef;
    char buf[100];

    char *passphrase = "acompllicatedpassphrase";

    /* open an file encrypted with passphrase */
    ef = enc_fopen("test.txt.nc", "rb", passphrase);
    enc_add_index(ef, "test.txt.ix", passphrase,
        INDEX_LOAD | INDEX_CREATE | INDEX_SAVE);

    /* read first 100 bytes of the encrypted data*/
    enc_fread(ef, 1, buf, 100);
    printf("First 100 bytes of the file: %s", ef);

    /* read last 100 bytes of the encrypted data */
    enc_fseek(ef, -100, SEEK_SET);
    enc_fread(ef, 1, buf, 100);
    printf("Last 100 bytes of the file: %s", ef);

    enc_fclose(ef);
}
```

In the sample, we assume that we have a file named `test.txt.nc` which has been symmetrically encrypted with passphrase `"acompllicatedpassphrase"`.

`enc_fopen()` opens the file for reading, just as `fopen()` would open a non-encrypted counterpart. The difference, compared to `stdio fopen()` call, is a third parameter through which you supply the passphrase for decryption. All other `libencio` functions in the example function as their `stdio` counterparts.

## 7 Random access (seeking)

The other difference from `stdio` is that a call to `enc_add_index()` is required in order to support random seeking of the file. This is needed because in most encryption modes considered secure (eg, feedback modes - CFB), in order to decrypt `n`-th byte of a file, one must decrypt all preceding bytes as well. In the worst case scenario – a seek to the last byte in the file – the complete file must be decrypted. Such an implementation of seeking would be unacceptably timeconsuming for large files.

`libencio` handles this by creating an "encryption state index" (ENCINDEX) on the file - a snapshot of decryption engine state (usually, the feedback register, `FR`), at predefined locations ("bookmarks") in the file (usually, every `blocksize` bytes, where by default `blocksize = 1024`). This allows `libencio` to quickly resume decryption starting from the bookmark nearest to the requested seek location. The worst case scenario in seeking with an index is a required decryption of `blocksize-1` bytes, which is usually acceptable.

Memory required for an index is proportional to  $(fsize/blocksize)*FR\_size$  where `fsize` is the encrypted file size and `FR_size` is the size of the feedback register for the cipher mode. For example, using 256 bit AES cipher requires 32 bytes per bookmark, which for a 500MB file and one bookmark per kb (`blocksize = 1024`), will generate a 16MB encryption state index. Increasing the `blocksize` will reduce the ENCINDEX footprint, but will degrade the seek performance.

ENCINDEX can (and should, for frequently accessed files) be saved to speed up construction on subsequent openings of the file. When an ENCINDEX is saved, it is encrypted with the same passphrase as the file which it indexes. The index is saved by adding an `INDEX_SAVE` flag as the fourth parameter of the `enc_add_index()` call. It can be subsequently loaded by specifying the `INDEX_LOAD` flag.

## 8 Encryption and File Format Details

Default settings for encryption are to encrypt using rijndael-128 (AES) algorithm, in cfb mode (with an IV), and attach a sha1 checksum to the encrypted file to check for errors in transmission. There is a number of global `enc_*` variables defined in `seekcrypt_internal.h` which control this behavior. CAVEAT: THESE VARIABLES ARE INTERNAL TO THE IMPLEMENTATION, AND WILL LIKELY CHANGE IN THE FUTURE, THUS BREAKING YOUR CODE. So don't touch them unless you really need to change the encryption details.

Any cipher from `libmcrypto` and any hash algorithm from `libmhash` can be used. However, for now you can only use stream modes (such as `cfb`) for encryption/decryption. Also, note the caveat from the previous paragraph.

The files produced by `encio` will be readable by MCrypt, version 2.6. Similarly, `encio` can read files produced by MCrypt, version 2.6, if they're in stream mode (eg., `cfb`).

## 9 API Reference

### 9.1 ENCFEILE

```
typedef struct ENCFEILE_t ENCFEILE;
```

ENCFEILE is an opaque handle to an encrypted file, equivalent to `stdio`'s `FILE`.

### 9.2 `enc_fopen()`

```
ENCFEILE *enc_fopen(const char *filename, const char *rwmode, const char
*passphrase);
```

`enc_fopen()` opens an encrypted file `filename`, encrypted with `passphrase`, for reading or writing depending on `rwmode`. Other than the `passphrase` parameter, it is equivalent to `fopen()`.

### 9.3 `enc_add_index`

```
int enc_add_index(ENCFEILE *ef, const char *indexfile, const char
*passphrase, int index_mode);
```

Adds an "encryption state index" (ENCINDEX) to a file `ef` which has been opened for reading. After the successful completion of this call, you can randomly access any location in the file using `enc_fseek()`.

Parameter `index_mode` determines the source of the encryption state index. If it contains the `INDEX_LOAD` flag, an attempt will be made to load it from file `indexfile`, which is assumed to be encrypted with `passphrase`. If successful, the `enc_add_index` will return 0. If `index_mode` has the `INDEX_CREATE` bit set, index will be constructed by internally decrypting the whole file `ef`. Finally, if `index_mode` has the `INDEX_SAVE` bit set, the index will be encrypted with `passphrase` and saved to `indexfile` file.

`INDEX_*` flags can be OR-ed, in which case first the `INDEX_LOAD` flag will be tested, then `INDEX_CREATE` and finally `INDEX_SAVE`. A typical use would be:

```
enc_add_index(ef, "test.txt.ix", passphrase, INDEX_LOAD | INDEX_CREATE | INDEX_SAVE);
```

where `encio` will first attempt to load the index from `test.txt.ix` and if that fails it will create the index, and store it to `test.txt.ix`.

### 9.4 `stdio`-like functions

```
int enc_fread(void *out, int size, int count, ENCFEILE *ef);          int enc_
fwrite(void *data, int size, int count, ENCFEILE *ef);
int enc_fseek(ENCFEILE *ef, long at, int dir); int enc_ftell(ENCFEILE *ef);
void enc_fflush(ENCFEILE *ef);          int enc_feof(ENCFEILE *ef);          int enc_
fclose(ENCFEILE *ef);
void enc_info(ENCFEILE *ef);
```

All these functions function exactly like their `stdio` counterparts.

## 10 Copying

# GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright © 1989, 1991 Free Software Foundation, Inc.  
59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

## Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software—to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

## TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The “Program,” below, refers to any such program or work, and a “work based on the Program” means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term “modification.”) Each licensee is addressed as “you.”

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program’s source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:
  - a. You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
  - b. You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
  - c. If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions

for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:
  - a. Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
  - b. Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
  - c. Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.
5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you

indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.
7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.
9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version," you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

## **NO WARRANTY**

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.
12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

## **END OF TERMS AND CONDITIONS**

## How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the “copyright” line and a pointer to where the full notice is found.

```
one line to give the program's name and an idea of what it does.
Copyright (C) 19yy name of author
```

```
This program is free software; you can redistribute it and/or
modify it under the terms of the GNU General Public License
as published by the Free Software Foundation; either version 2
of the License, or (at your option) any later version.
```

```
This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU General Public License for more details.
```

```
You should have received a copy of the GNU General Public License along
with this program; if not, write to the Free Software Foundation, Inc.,
59 Temple Place, Suite 330, Boston, MA 02111-1307, USA.
```

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

```
Gnomovision version 69, Copyright (C) 20yy name of author
Gnomovision comes with ABSOLUTELY NO WARRANTY; for details
type 'show w'. This is free software, and you are welcome
to redistribute it under certain conditions; type 'show c'
for details.
```

The hypothetical commands ‘show w’ and ‘show c’ should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than ‘show w’ and ‘show c’; they could even be mouse-clicks or menu items—whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a “copyright disclaimer” for the program, if necessary. Here is a sample; alter the names:

```
Yoyodyne, Inc., hereby disclaims all copyright
interest in the program 'Gnomovision'
(which makes passes at compilers) written
by James Hacker.
```

```
signature of Ty Coon, 1 April 1989
Ty Coon, President of Vice
```

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General Public License instead of this License.

# Index

introduction ..... 1

## Short Contents

1	Overview . . . . .	1
2	Requirements . . . . .	2
3	Caveats and Warnings . . . . .	3
4	TODO List . . . . .	4
5	Writing Encrypted Files . . . . .	5
6	Reading and Seeking Encrypted Files . . . . .	6
7	Random access (seeking) . . . . .	7
8	Encryption and File Format Details . . . . .	8
9	API Reference . . . . .	9
10	Copying . . . . .	10
	GNU GENERAL PUBLIC LICENSE . . . . .	11
	Index . . . . .	17

## Table of Contents

<b>1</b>	<b>Overview</b> .....	<b>1</b>
<b>2</b>	<b>Requirements</b> .....	<b>2</b>
<b>3</b>	<b>Caveats and Warnings</b> .....	<b>3</b>
<b>4</b>	<b>TODO List</b> .....	<b>4</b>
<b>5</b>	<b>Writing Encrypted Files</b> .....	<b>5</b>
<b>6</b>	<b>Reading and Seeking Encrypted Files</b> .....	<b>6</b>
<b>7</b>	<b>Random access (seeking)</b> .....	<b>7</b>
<b>8</b>	<b>Encryption and File Format Details</b> .....	<b>8</b>
<b>9</b>	<b>API Reference</b> .....	<b>9</b>
	9.1 ENCFILE .....	9
	9.2 enc_fopen() .....	9
	9.3 enc_add_index .....	9
	9.4 stdio-like functions .....	9
<b>10</b>	<b>Copying</b> .....	<b>10</b>
	<b>GNU GENERAL PUBLIC LICENSE</b> .....	<b>11</b>
	Preamble .....	11
	TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION .....	11
	How to Apply These Terms to Your New Programs .....	16
	<b>Index</b> .....	<b>17</b>