Data Encryption
Fast & Secure

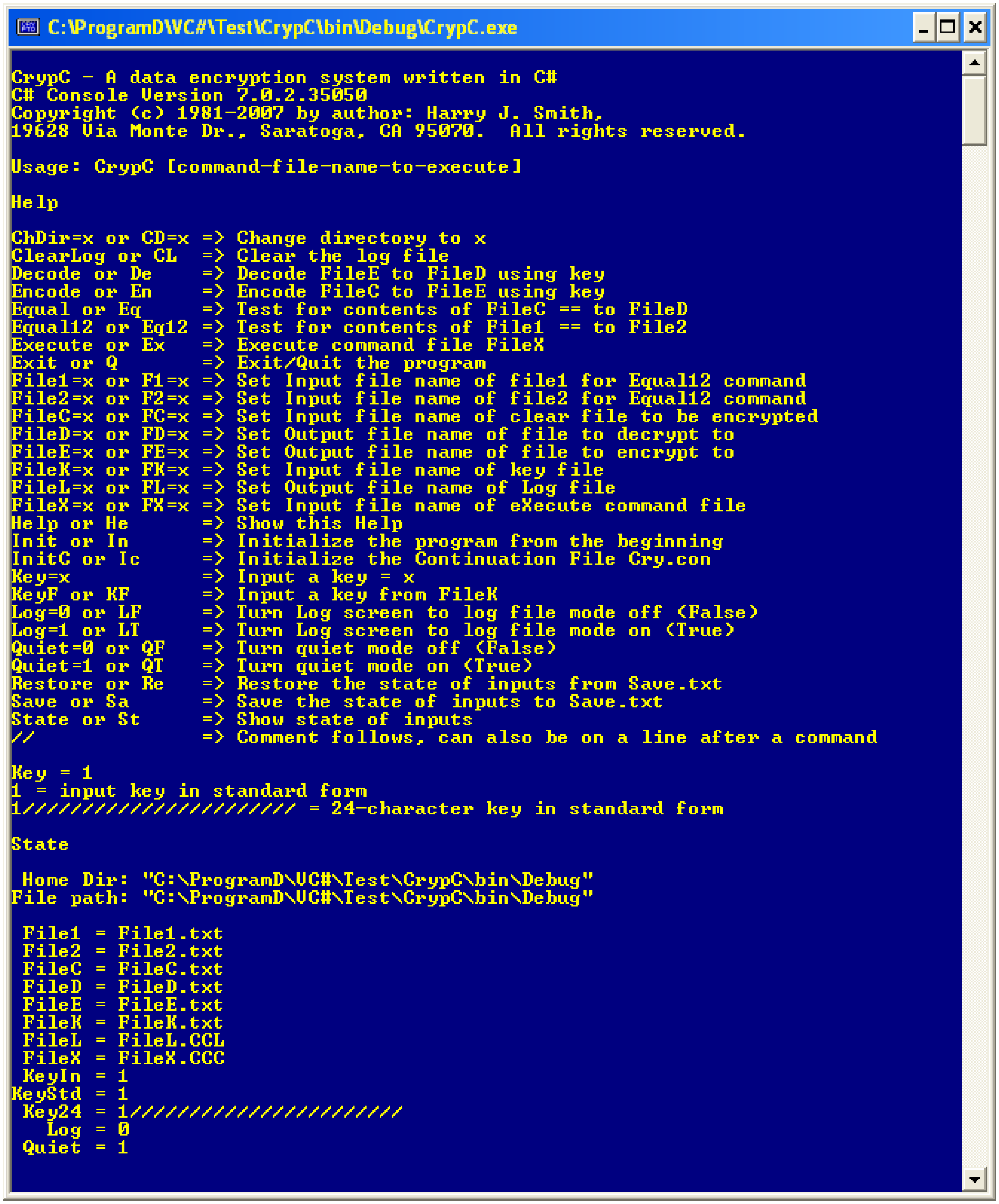
The algorithm for the Data Encryption
Standard runs too slow on most micros, but
simpler methods have not provided secure
encryption. This program solves this
problem by being both fast and secure.

By Harry J. Smith

The program CrypC is an upgrade to the programs CRYN, CRYP, and CRYU that were distributed in file CRYP60.ZIP in 1993. CrypC is compatible with the earlier programs as files encrypted in one of the programs can be decrypted in any other of the programs. The basic documentation for the earlier programs still applies to CrypC and will not be repeated in this document. The earlier documentation is distributed with this program as files CRYP.doc and CRYP.txt.

Running the program without arguments -

When the program CrypC is started with no command line arguments, a console window is displayed.



```
CrypC - A data encryption system written in C#
C# Console Version 7.0.2.35050
Copyright (c) 1981-2007 by author: Harry J. Smith,
19628 Via Monte Dr., Saratoga, CA 95070.  All rights reserved.

Usage: CrypC [command-file-name-to-execute]

Help

ChDir=x or CD=x => Change directory to x
ClearLog or CL  => Clear the log file
Decode or De    => Decode FileE to FileD using key
Encode or En    => Encode FileC to FileE using key
Equal or Eq     => Test for contents of FileC == to FileD
Equal12 or Eq12 => Test for contents of File1 == to File2
Execute or Ex   => Execute command file FileX
Exit or Q       => Exit/Quit the program
File1=x or F1=x => Set Input file name of file1 for Equal12 command
File2=x or F2=x => Set Input file name of file2 for Equal12 command
FileC=x or FC=x => Set Input file name of clear file to be encrypted
FileD=x or FD=x => Set Output file name of file to decrypt to
FileE=x or FE=x => Set Output file name of file to encrypt to
FileK=x or FK=x => Set Input file name of key file
FileL=x or FL=x => Set Output file name of Log file
FileX=x or FX=x => Set Input file name of eXecute command file
Help or He      => Show this Help
Init or In      => Initialize the program from the beginning
InitC or Ic     => Initialize the Continuation File Cry.con
Key=x           => Input a key = x
KeyF or KF      => Input a key from FileK
Log=0 or LF     => Turn Log screen to log file mode off (False)
Log=1 or LT     => Turn Log screen to log file mode on (True)
Quiet=0 or QF   => Turn quiet mode off (False)
Quiet=1 or QT   => Turn quiet mode on (True)
Restore or Re   => Restore the state of inputs from Save.txt
Save or Sa      => Save the state of inputs to Save.txt
State or St     => Show state of inputs
//              => Comment follows, can also be on a line after a command

Key = 1
1 = input key in standard form
1/////////////////////// = 24-character key in standard form

State

 Home Dir: "C:\ProgramD\VC#\Test\CrypC\bin\Debug"
File path: "C:\ProgramD\VC#\Test\CrypC\bin\Debug"

 File1 = File1.txt
 File2 = File2.txt
 FileC = FileC.txt
 FileD = FileD.txt
 FileE = FileE.txt
 FileK = FileK.txt
 FileL = FileL.CCL
 FileX = FileX.CCC
 KeyIn = 1
KeyStd = 1
 Key24 = 1///////////////////////
   Log = 0
 Quiet = 1
```

The window is scrollable and resizable. It contains a listing of the help file CrypCHelp.txt that contains the list of commands that the program can execute. It also shows that some initial commands have been executed.

CrypC - A data encryption system written in C#
C# Console Version 7.0.2.35050
Copyright (c) 1981-2007 by author: Harry J. Smith,
19628 Via Monte Dr., Saratoga, CA 95070. All rights reserved.

```
Usage: CrypC [command-file-name-to-execute]

Help

ChDir=x or CD=x => Change directory to x
ClearLog or CL  => Clear the log file
Decode or De    => Decode FileE to FileD using key
Encode or En    => Encode FileC to FileE using key
Equal or Eq     => Test for contents of FileC == to FileD
Equal12 or Eq12 => Test for contents of File1 == to File2
Execute or Ex   => Execute command file FileX
Exit or Q       => Exit/Quit the program
File1=x or F1=x => Set Input file name of file1 for Equal12 command
File2=x or F2=x => Set Input file name of file2 for Equal12 command
FileC=x or FC=x => Set Input file name of clear file to be encrypted
FileD=x or FD=x => Set Output file name of file to decrypt to
FileE=x or FE=x => Set Output file name of file to encrypt to
FileK=x or FK=x => Set Input file name of key file
FileL=x or FL=x => Set Output file name of Log file
FileX=x or FX=x => Set Input file name of eXecute command file
Help or He      => Show this Help
Init or In      => Initialize the program from the beginning
InitC or Ic     => Initialize the Continuation File Cry.con
Key=x           => Input a key = x
KeyF or KF      => Input a key from FileK
Log=0 or LF     => Turn Log screen to log file mode off (False)
Log=1 or LT     => Turn Log screen to log file mode on (True)
Quiet=0 or QF   => Turn quiet mode off (False)
Quiet=1 or QT   => Turn quiet mode on (True)
Restore or Re   => Restore the state of inputs from Save.CCC
Save or Sa      => Save the state of inputs to Save.CCC
State or St     => Show state of inputs
//              => Comment follows, can also be on a line after a command

Key = 1
1 = input key in standard form
1/////////////////////// = 24-character key in standard form

State

 Home Dir: "C:\ProgramD\VC#\Test\CrypC\bin\Debug"
File path: "C:\ProgramD\VC#\Test\CrypC\bin\Debug"

 File1 = File1.txt
 File2 = File2.txt
 FileC = FileC.txt
 FileD = FileD.txt
 FileE = FileE.txt
 FileK = FileK.txt
 FileL = FileL.CCL
 FileX = FileX.CCC
 KeyIn = 1
KeyStd = 1
 Key24 = 1///////////////////////
   Log = 0
 Quiet = 1
--------------------------------------------------------------------------------
```

In this document and program the words encipher, encrypt, and encode are used interchangeable as are the words decipher, decrypt, and decode

The commands are -

ChDir=x or CD=x => Change directory to x:

Changes the directory used for commands Decode, Encode, and Execute. The original directory when the program starts is called the Home directory and is always used for the commands ClearLog, Help, LogScreen, Restore, and Save, commands.

ClearLog or CL => Clear the log file:

If the log file is open, the file is closed and reopened. If it is currently closed, it opened and then closed. In either case it is cleared. Initially the log file name is NoName.CFL.

The cleared log file will have up to three lines of data like:

```
Log file "FileL.CCL" Cleared 10/25/2007 11:17:42 AM
CrypC - A data encryption system written in C#, C# Console Version 7.0.2.35050
Run on: Harry's Intel 3 GHz Pentium 4 - Dell DGV4T641 - Windows XP Pro SP2
```

The third line is generated by having something like:

```
SET SYSTEM=Harry's Intel 3 GHz Pentium 4 - Dell DGV4T641 - Windows XP Pro SP2
```

in your AutoExec.Bat file.

Decode or De => Decode FileE to FileD using key:

This decodes the file specified in the FileE=x command and stores the results in the file specified in the FileD=x command using the encryption key specified in the Key=x or KeyF command.

Encode or En => Encode FileC to FileE using key:

This encodes the file specified in the FileC=x command and stores the results in the file specified in the FileE=x command using the encryption key specified in the Key=x or KeyF command.

Equal or Eq => Test for contents of FileC == to FileD:

This reads in the file FileC specified by the FileC=x command and compares it byte-for-byte with the file FileD specified by the FileD=x command. It tells you if the two files are exactly the same or not. This is mainly for testing to see if the decoded file is the same as the original clear file

Equal12 or Eq12 => Test for contents of File1 == to File2:

This reads in the file File1 specified by the File1=x command and compares it byte-for-byte with the file File2 specified by the File2=x command. It tells you if the two files are exactly the same or not. This is mainly for testing.

When files are read by the Equal12 or the Equal command, the first file is read from the home directory only and the second file is read from the current directory/file path only.

Execute or Ex => Execute command file FileX:

This reads in the file specified in the FileX=x command and executes each line as a CrypC command. Blank lines are ignored.

Exit or Q => Exit/Quit the program:

This terminates the execution of the program.

File1=x or F1=x => Set Input file name of file1 for Equal12 command:

Here x specifies the name of file one that will be used by the Equal12 command. For all commands with a file name, if a file name contain embedded spaces or delimiter characters, the name need to be quoted. For example, File1=";= ()@".

File2=x or F2=x => Set Input file name of file2 for Equal12 command:

Here x specifies the name of file two that will be used by the Equal12 command.

FileC=x or FC=x => Set Input file name of clear file to be encrypted:

Here x specifies the name of the file that will be encoded by the Encode command.

FileD=x or FD=x => Set Output file name of file to decrypt to:

Here x specifies the name of the file that will be used to store the results of the Decode command.

FileE=x or FE=x => Set Output file name of file to encrypt to:

Here x specifies the name of the file that will be used to store the results of the Encode command and used as the name of the file that will be decoded by the Decode command.

FileK=x or FK=x => Set Input file name of key file:

Here x specifies the name of the file that will be read by the KeyF command.

FileX=x or FX=x => Set Input file name of eXecute command file:

Here x specifies the name of the file that will be read by the Execute command.

Help or He => Show this Help:

This reads in the file CrypCHelp.txt and displays its contents.

Init or In => Initialize the program from the beginning:

This restarts the program as if it had been terminates and restarted without command line arguments.

InitC or Ic => Initialize the Continuation File w:

This uses the current encryption key specified in the Key=x or KeyF command to initialize the contents of the Cry.con file in the home directory. The Cry.con file is always read from and written to the home directory.

Key=x => Input a key = x:

This uses x to specify the encryption key and computes the “input key in standard form” and the “24-character key in standard form”. Everything following the first = sign is taken as the Key. For example,

```
       Key = //~ as @!~;"= // "  ~//
```

Leading and trailing spaces are removed from the key. So, the / character must be used for these.

KeyF or KF => Input a key from FileK:

This uses the first line of the file specified in the FileK=x command to specify the encryption key and computes the "input key in standard form" and the "24-character key in standard form". Leading and trailing spaces are deleted.

Log=0 or LF => Turn Log screen to log file mode off (False):

When logging mode is on, all output to the screen is logged to a disk file. See the FileL=x command for specifying a file name for this purpose.

Log=1 or LT => Turn Log screen to log file mode on (True):

When logging mode is on, all output to the screen is logged to a disk file. See the FileL=x command for specifying a file name for this purpose.

Quiet=0 or QF => Turn quiet mode off (False):

When the quiet mode is off, all of the status messages all displayed.

Quiet=1 or QT => Turn quiet mode on (True):

When the quiet mode is on, some of the status messages all not displayed.

Restore or Re => Restore the state of inputs from Save.CCC:

This reads in the file Save.CCC and executes each line as a CrypC command. Normally the Save.CCC has been written by the Save command.

Save or Sa => Save the state of inputs to Save.CCC:

This writes the Save.CCC file containing the six commands needed to restore CrypC’s state to its current value. An example of Save.CCC contents is:

```
ChDir = C:\ProgramD\VC#\Test\CrypC\bin\testOutput
File1 = File1.txt
File2 = File2.txt
FileC = FileC.txt
FileD = FileD.txt
FileE = FileE.txt
FileK = FileK.txt
FileL = FileL.CCL
FileX = FileX.CCC
Key = 1
Log = 0
Quiet = 1
```

State or St => Show state of inputs:

This shows the home directory and the state of the six commands that would be saves by the Save command. For example:

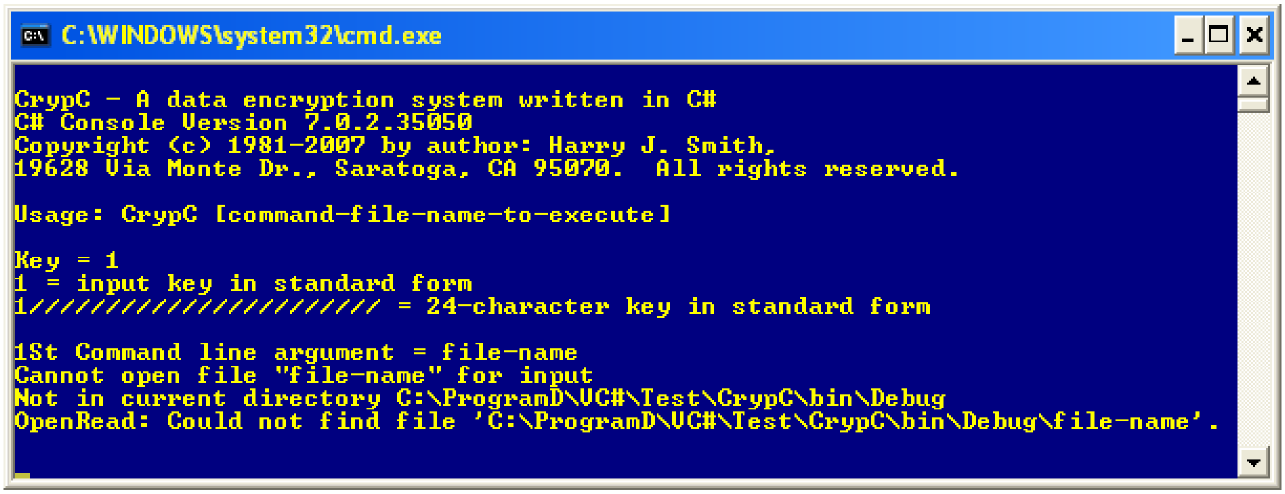
```
 Home Dir: "C:\Program Files\CrypC 7.0\run"
File path: "C:\Program Files\CrypC 7.0\testOutput"

 File1 = File1.txt
 File2 = File2.txt
 FileC = FileC.txt
 FileD = FileD.txt
 FileE = FileE.txt
 FileK = FileK.txt
 FileL = FileL.CCL
 FileX = FileX.CCC
 KeyIn = 1
KeyStd = 1
 Key24 = 1///////////////////////
   Log = 0
 Quiet = 1
```

// => Comment follows, can also be on a line after a command:

If // starts in column one or is preceded by blanks, it shows on the screen but is considered a NoOp command. If the // is preceded by a command on the same line, the command is executed.

Running the program with arguments -

When the program CrypC is started with command line arguments, only the first argument is used. This first argument is taken as the name of a file to be executed and a console window is displayed.



```
CrypC - A data encryption system written in C#
C# Console Version 7.0.2.35050
Copyright (c) 1981-2007 by author: Harry J. Smith,
19628 Via Monte Dr., Saratoga, CA 95070.  All rights reserved.

Usage: CrypC [command-file-name-to-execute]

Key = 1
1 = input key in standard form
1/////////////////////// = 24-character key in standard form

1St Command line argument = file-name
Cannot open file "file-name" for input
Not in current directory C:\ProgramD\VC#\Test\CrypC\bin\Debug
OpenRead: Could not find file 'C:\ProgramD\VC#\Test\CrypC\bin\Debug\file-name'.
```

```
CrypC - A data encryption system written in C#
C# Console Version 7.0.2.35050
Copyright (c) 1981-2007 by author: Harry J. Smith,
19628 Via Monte Dr., Saratoga, CA 95070.  All rights reserved.

Usage: CrypC [command-file-name-to-execute]

Key = 1
1 = input key in standard form
1/////////////////////// = 24-character key in standard form

1St Command line argument = file-name
Cannot open file "file-name" for input
Not in current directory C:\ProgramD\VC#\Test\CrypC\bin\Debug
OpenRead: Could not find file 'C:\ProgramD\VC#\Test\CrypC\bin\Debug\file-name'.
```

The program is initialized; FileX is set to the first command line argument and then executed by the Execute command.

Encrypting and decrypting files -

To encrypt a file, start CrypC and execute the commands

```
Key=x
FileC=x
FileE=x
Encode
```

To decrypt a file, start CrypC and execute the commands

```
Key=x
FileE=x
FileD=x
Decode
```

The x in the File commands can specify a full path like

C:\My Documents\!Private\Accounts.Doc
Or simply a file name like Accounts.Doc
In the latter case, the file must be in the same folder as the program's .exe file. This folder should also be the "Start in:" folder or home folder.

You must copy the files you are working with to the folder that contains the executable (normally C:\Program Files\CrypC 7.0\run) or copy Cry.con, CrypC.exe, and CrypCHelp.txt to the folder that has your files.

Screen messages -

Error messages are:

```
      Cannot Decode file "{filename}" to itself
      Cannot Encode file "{filename}" to itself
      Cannot open file “{filename}” for input
      Cannot open file “{filename}” for output
      Cannot read file “{filename}”
      File write error {error-message}
      I do not understand ‘{command}’
      Not in current directory “{directory}”
      Not in home directory “{directory}”
      OpenAppend: {error-message}
      OpenRead: {error-message}
      OpenWrite: {error-message}
      Path not found!
```

Other informational messages:

```
      {key} = 24-character key in standard form
      {key} = input key in standard form
      1St Command line argument = {argument}
      Continuation file “Cry.con” updated
      Directory changed to “{directory}”
      Directory name = “{directory}”
      Directory not changed “{directory}”
      False, files "{filename}" and "{filename}" are not equal
      False, files "{filename}" and "{filename}" are not the same length
      File “{filename}” opened for reading
      File “{filename}” opened for writing
      File “{filename}” verified and closed
      Full name = “{directory}\{filename}”
      Home directory is “{directory}”
      Key = {key}
      Log file "{filename}" Cleared {date} {time}
      Log file "{filename}" Closed {date} {time}
      Log file "{filename}" Opened for Append {date} {time}
      Save file “Save.CCC” updated
      True, files "{filename}" and "{filename}" are equal
      True, files "{filename}" and "{filename}" are the same file
      Usage: CrypC [command-file-name-to-execute]
```

Program distribution –

This program and the older CRYP60.ZIP are available at my website:

http://www.geocities.com/hjsmithh/

in the **Files to Download** section

http://www.geocities.com/hjsmithh/download.html#CRYP

When you install the program using the distribution file CrypC70?.exe or CrypC70?.zip, a folder is created with 4 subfolders:

```
├── CrypC 7.0
│   ├──doc
│   ├──run
│   ├──src
│   ├──test
│   ├──testOutput
│   └──testVerify
```

The main folder has two files sseexec.dat and SSEun.dat. These are needed to be able to uninstall the program

The doc subfolder has the following files:

```
!.txt      (Information on version)
CRYP.doc   (Basic documentation for the earlier programs, still applies)
CRYP.txt   (Plain ASCII text copy of the CRYP.doc file)
CrypC.doc  (This documentation in a Microsoft Word file)
CrypC.txt  (Plain ASCII text copy of the CrypC.doc file without graphics)
Fixes.txt  (A list of features and fixes added to each version)
Note.txt   (Old note written 7/10/1994)
```

The run subfolder has the following files:

```
!.txt
Cry.con
CrypC.exe
CrypCHelp.txt
```

The .exe file is executed from there.

The src subfolder has all the source files needed for development:

```
!.txt
App.ico
AssemblyInfo.cs
COPYING.txt
CrypC.cs
CrypC.csproj
CrypC.sln
CrypC.suo
CrypC.csproj.user
```

The test subfolder has the files I use for testing the program. They are:

```
!.txt
0.txt
1.txt
17.txt
18.txt
1R.txt
2R.txt
```

```
      3.txt
      Cry.con
      Cry1.con
      CrypC.exe
      CrypCHelp.txt
      FileC.txt
      FileD.txt
      FileE.txt
      FileK.txt
      FileL.CCL
      FileX.bat
      FileX.CCC
      FileX.CCL
      K.txt
      Save.CCC
      TestArgs.bat
      WhatForTst.txt
      X
      X.bat
      Z
      Z128K
      Z160K
```

The testOutput subfolder has the output files I use for testing the program. They are:

```
      !.txt
      0D.txt
      0E.txt
      17D.txt
      17E.txt
      18D.txt
      18E.txt
      1D.txt
      1E.txt
      1RD.txt
      1RE.txt
      2RD.txt
      2RE.txt
      3D.txt
      3E.txt
      Cry.con
      TestV.CCC
      TestV.CCL
      WhatForOut.txt
      Z128KD
      Z128KE
      Z160KD
      Z160KE
      Z160KED
      Z160KEE
      ZD
      ZE
```

The testVerify subfolder has old output files I use to verify that CrypF still works correctly, by using the CrypC code file TestV.CCC. These files were actually generated by:

```
      CRYP - A data encryption system written in C, with pipes
      Version 6.00, 1992-11-15, 1400 hours
      Copyright (c) 1987-1992 by author: Harry J. Smith
```

The files are:

```
      !.txt
      0D.txt
      0E.txt
      17D.txt
      17E.txt
      18D.txt
      18E.txt
      1D.txt
      1E.txt
      1RD.txt
      1RE.txt
      2RD.txt
      2RE.txt
      3D.txt
      3E.txt
      WhatForOut.txt
      Z128KD
      Z128KE
      Z160KD
      Z160KE
      Z160KED
      Z160KEE
      ZD
      ZE
```

The program can generate the following files:

```
      Cry.con
      Save.CCC
      {encrypted-file}
      {decrypted-file}
```

The end -

Report any errors by sending me a letter, an e-mail or call me at my home phone.

-Harry

Harry J. Smith
19628 Via Monte Dr.
Saratoga, CA 95070-4522, USA

Home Phone: 1 408 741-0406
E-mail: hjsmithh@sbcglobal.net
Website: http://www.geocities.com/hjsmithh/