Cryptx 4.1
Documentation

CryptX 4.1

Contents

1 Introduction

This is the documentation for CryptX 4.1. It is fundamentally easy to use encryption/decryption software. The first versions were very simple but did not offer many features, the most prominent of which was the lack of a password protection. To cover all that we bring you the next milestone development from the R & D team at Centrum Inc Software Solutions, Cryptx 4.1. The core functional part of this project is a 32-bit application written in C and compiled using the 32-bit Borland C++ Compiler 5.0.5.

The UI that you see is an HTA file which has been made to simplify the working of the program. We have done this program for an educational purpose. It is a JavaScript code that produces the correct parameters for the application. It was developed by our R & D team, after long and hard research has been made open source. So you can learn and adapt these in your own projects. Read this documentation for further details.

1.1 About HTA

HTA is a Microsoft® technology that allows a developer to deploy an HTML page consisting of scripts as a desktop application on Windows. The advantage is the efforts and know how required for developing the UI of the application, which is the same as that for any HTML page. The functionality or processing is imparted through scripting. For more information on the HTA technology, refer to http://msdn.microsoft.com/library/default.asp?url=/workshop/author/hta/overview/htaoverview.asp. We used this technology because the interface design is very easy. All we have to do is design an HTML page for the UI. You should know the level of interface that a 32 - bit C program can provided. This HTA program is run by an interpreter called MSHTA.EXE located in your WINDOWS/SYSTEM32 folder in Windows NT installations and with the same name in WINDOWS/SYSTEM folder in Windows 95/98 installations.

1.2 RSA s MD5 Encryption Algorithm

In this program, we use RSA's MD5 encryption algorithm to protect passwords. This program uses "**RSA Data Security, Inc. MD5 Message-Digest Algorithm**" under licence from RSA by mentioning this project is derived from their algorithm.

2 How To Use

This section tells you how to use the program.

2.1 The Interface

Fig : CryptX 4.0 GUI

1. Use the Browse button to browse for the file that you would like to encrypt or decrypt. Then select it.
2. Type your password here.
3. Press this button when you are satisfied with the chosen file & password. When you press this button, your file would be encrypted or decrypted.
4. Press this button to see the log of the program. The last entry would show the result of the last operation.
5. Shows the help bundled with the software installation.
6. Shows the information about the program.
7. The demo interface for Cryptx 4.0. It shows you a quick demonstration on how to encrypt or decrypt a file using this utility. To view the demo you will need Macromedia Flash Player 6 or above.
8. The controls for the demo of Cryptx 4.0. Press play to play the demo. Stop to stop it & help to bring up the help bundled with the installation.

2.2 Encryption

This program has an easy to use interface. There are two input fields. The first one is used to get the name of the file to be encrypted or decrypted. You can easily browse for the specific file by clicking on the 'Browse...' button. The next field is for the password. Again, this is a great advancement in the history of the development of this program.

When you have entered the password, press Crypt. You may see a black splash screen. That is Cryptx4 in action. You can press 'Show Log' to see the result of the operation. Please remember that since we are using RSA's MD5 encryption algorithm to protect the password, there is no way to recover it since, the settings file is protected.

Before you start encrypting files, take a note these limitations.

- The filenames or directory names can be of any lengths as long as they do not contain more that 1 space with in the first 6 characters. For example '**My Documents**' is acceptable whereas '**in cd three**' is not allowed.
- The supported file formats are given in detail in the following part of this documentation.
- The password can be of any length, have spaces and any type of characters.
- The file to encrypt or decrypt cannot be on a CD/DVD or other read only devices.

2.3 Decryption

When you encrypt a file with CryptX 4.0, two files are created in that directory. For example, if your file is '**my_file_name**'.ext. Assuming that ext is the file's extension. Then the two files created will be '**my_file_name**'.rap and '**my_file_name**'.set. The *.rap is called a Reminiscent Alternative Protection (RAP file). It is the encrypted file. But it does not stand by itself. The *.set is the settings file. It holds information that regards to the encrypted file. You can only decrypt a rap file with its corresponding settings file. To decrypt a file encrypted with CryptX 4.0 all you need are the rap file, settings file and of course the password.

Decryption is more or less like encryption. Here you select the rap file. Make sure that its settings file is there with it. Type your password and press '**Crypt**'. If you check the program log, you can find if the process was successful or not. If it isn't, the error will be reported along with an error code. You can lookup the detailed reason of the error in the error codes page in this help. If the process is successful, the decrypted file will be in that directory with its original extension.

3. Supported File Formats

There are only two types of file. Files that are written in '**text**' mode and those in '**binary**' mode. They have been classified as under TEXT and BINARY mode. Files written in one mode should only be processed only in that mode. So the extensions supported by this utility are given below.

Note that we have only added the most commonly used file formats and avoided system files like dlls etc alone. Also note that we currently donot support filenames whose extensions are larger than three characters like html, jpeg, mpeg etc. If you want you can rename the files to their three character extensions as htm, jpg or jpe, mpg or mpe etc.

3.1 TEXT Mode

ASP, BAT, C, CPP, CSS, DEF, DIC, H, HTM, INI, INC, INF, JS, LOG, PHP, TXT, XML.

3.2 BINARY Mode

Archive files: 7Z, ARC, RAR, ZIP, CAB, GZ, LZH, TAR, PAK.

Document formats: DOC, RTF, PDF, XLS, DB, PPS, PPT.

Executable Files: EXE.

Image files: BMP, JPG, JPE, PNG, GIF, PSD, TGA.

Media formats: AIF, AU, ASF, ASX, AVI, MP2, MP3, MP4, MPE, MPG, WMV, WAV, WMA.

Standard Binary Format: BIN.

4.0 Error codes

Whenever you crypt / decrypt a file, it is resourceful to check the program's log and look at the last entry to see what happened. If it says Success, the program did its job without any errors. If any errors occur, it will report an error code with a simple description. If you want to know more about the error, just refer to this documentation which has been written by running through each step of the source code of the programs. If you have any further doubts or additional information on the error codes, you are always welcome to take part in contributing your information for the improvement of this program and its documentation.

Most of these errors do not occur if you use the GUI of the Cryptx 4.0. We are only mentioning these here for completion. These errors may come up if you try to use the program from command line which is not advised.

Error RB MN43

The reason is that the program was passed invalid no of arguments. The program is expecting 7 arguments if you are encrypting a file and 6 if you are decrypting a rap file. This error code should not normally come up if you use the Cryptx 4.0 GUI.

Error RB TX109, RB BI163

An error occurred when the program was trying to open the specified file.
If the filename or a folder name in the path of the specified file has more than one space within the first 6 characters, this could happen.
This may be because the file may not exist or the file may be opened by another application.
Other likely reasons may be that your disk space might be insufficient to open a file or that the disk might be damaged.

Error RB TX128, RB BI182

An error happened when the program had done the first part of the encryption/decryption process and then it tried to copy the file to the final path.
When you try to decrypt a rap file which is in a read only device, the first part of the process goes on if the passwords match. Then when the program tries to copy the file to the destination, the new file cannot be created.
If the file to encrypt is on a read only device. So when the program tries to write the settings file, the process fails. So this error is not reported.

ErrorSE WS36

The program could not create the settings file. This may happen if the file that you selected to encrypt is on a read-only device like CD or DVD.

ErrorSE GM62

When you are decrypting a file, the password that the user specified and the one with which the original file was encrypted do not match. Please note that since we are using RSA's MD5 algorithm to protect the password, there is no way to retrieve the password.

ErrorSE GM66

The settings file has gone through many revisions until it was standardized. So Cryptx 4.0 cannot read the settings file of a rap file encrypted with a previous version of CryptX. Also since CryptX 4.0 is the standard release with a settings file & rap file combination, the previous versions were all Betas.

Error SE GM68

As an extra method of protection, we store the file size of the original file. When the rap file is decrypted, its size is checked against the original file size. If these two do not match, this error is flagged.
Note that this checking is only performed for binary files, because when encrypted the text mode files seem to reduce sizes! The reason for this phenomenon is still unknown. It works for the files that are in Binary mode.
The user may have used the settings file of another rap file and tried to decode this rap file; perhaps assuming that they have the same passwords.

Error SE GM91

This is a fatal error. The program could not open the settings file, or it was not found. The settings file is the key to opening a rap file with the correct password of course. Please note that both the rap file and the settings file should have the same names and reside in the same directory. If the settings file is missing, there is no way to decrypt the file even if you have the correct password.

Further Queries

For further information on errors or any issues, just log onto our website for updated documentation details, or you can mail us your queries. http://www.geocities.com/mhkonline2/

5 Program Versions

Cryptx 1.1:
Released on 23rd January 2006. Only had capability to encrypt or decrypt files in text mode. There was no way to make sure that the filename that was entered was text based and can be crypted. No error reporting for HTA version.

Cryptx 1.2:
Not a release version, but acted as an intermediate, internal development version. This version created a log file in which the details of the process were logged. The development process for this version was completed on 24th January 2006. A button to show the log file was added.

Cryptx 1.3.2:
Released on 25th January 2006. Because there was much more than logging, we had to release this version as a new one. That's why V1.2 was not released externally. In this version, we added a new version of Cryptx that can successfully crypt files that have been written in Binary mode. This is a real jump forward as far as we are concerned.
- Updated the help provided with the program and documentation on the website.
- Also some bugs in the programs were fixed.
- The code was optimized to work more efficiently when errors occur.
- We were able to place code to check the format of the filename and use the appropriate crypting program. This also helped us to prevent crypting of system files and files which are generally not used.
- The log writing was also modified to give error codes from the crypting programs. We also added a new help file just for handling info on the error codes. The error codes are placed in the program's log file with a basic description of the error.
- Certain bugs in the installer were corrected.
- New file formats were added to the script to recognize.
- Updated help file.

Cryptx 2.0.78b:
This version works on the same principle as its predecessors but its core working part changed considerably. So version 2 was born. The improvements in this version are:
- Installed a file browser to browse for the file to encrypt/decrypt.
- Optimized the core program working in the background.
- Size optimized the installation.
- Fixed folder name limitation of 8.3 DOS format.
- Updated Help.
- Optimized the Demo interface.

Cryptx 2.1:
- Some bug fixes were made to the scripts.
- Optimized the entire working of the program.

Cryptx 3.0:
- The program now uses a combination of rap file & settings file when encrypting. Thus ridding the original file of any changes.
- Was only released as internal Beta.

Cryptx 3.1:
- Optimized & revised the settings file.

Cryptx 3.2:
- 32-bit version of CryptX was released!

Cryptx 3.3:
- Up until now the filename was always shortened to the 8.3 dos format in all cases. Now if the filename does not contain any spaces, the modified script makes the output filename the real name of the specified file.

Cryptx 3.4:
- This version uses password to protect the file with a Simple encryption technology, which is not consistent.
- The maximum length of the password was 10 characters.
- The output filenames were all in caps. We took care of that by modifying the JavaScript code to workaround that. Now they are as same as the original files.
- Modified the structure of the settings files and minor bug fixes were made.
- Added standard extension for binary files, '**bin**'.

Cryptx 4.0:
- We now use RSA Data Security's MD5 Encryption algorithm to encrypt the password.
- The filenames can now be of any length, the MD5 would be a constant 32 bytes.
- New Icon & Color Scheme. Graphical renovation by artistik expressionz.
- The help system was updated considerably.
- '**The potential Unleashed**'! Marketed by M-Dezigns.
- A new, simple and secure method for protecting the settings file.
- Added the about button.
- Updated and size optimized the demo interface.

Cryptx 4.1:

- Released on 20th June 2006. This is a big development as far as we are concerned. We finally understood and fixed a bug that has been baffling us since 'CryptX Version 1'. The file size of the rap file seemed to be less than the original file if the file was written in 'Text Mode'. This is because when a '\n' character is written to the file, it is actually converted into a '\r\n' combination; i.e. a carriage return and linefeed or one extra character per new line. But when the CryptX program reads this file, the C library files convert the '\r\n' combination to '\n'.

- So we now can now calculate the file size of the rap file using the equation.

$$rapFileSize = sourceTXTFileSize - \left(\frac{sourceTXTFileSize - numCharsTXTFile}{2}\right)$$

- This means improved security for 'Text Mode' files. Until now we had relaxed the restriction of checking the original file size and the rap filesize in case of 'Text Mode' files. This version is fully compatible with the rap files generated by CryptX 4.0. We haven't changed the structure of the settings file.

- Developer's Note: This discrepancy does not happen to files written in 'Binary Mode'.

- Another minor development was also done. Now the Cryptx4 core expects 8 items as the command line parameters. Previous versions expected one number for encrypting and another for decrypting. This move was done to standardize the system and also for future developmental purposes.

6.0 License Information

6.1 CryptX License

This software is provided 'as-is', without any express or implied warranty. In no event will the author or the publishers be held liable for any consequences/damages arising from the use of this software.

The JavaScript code used in this program are Open Source and can be used by anyone at any time. But the author's rights must be acknowledged. This program and the accompanied files/artwork are FREEWARE. You can use it for personal, business, educational or any other need of yours, subject to the following restrictions:

1. You may not re-distribute this program by modifying its contents
2. You may not charge any fee or re-distribution fee for it.
3. Respect the efforts made by the author.

6.2 MD5 Licence

Copyright (C) 1991-2, RSA Data Security, Inc. Created 1991. All rights reserved.

License to copy and use this software is granted provided that it is identified as the "RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing this software or this function.

License is also granted to make and use derivative works provided that such works are identified as "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing the derived work.

RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind.

These notices must be retained in any copies of any part of this documentation and/or software.

7.0 Support

You can check out our website for latest updates, versions, information and documentation on the support page of Cryptx utility at http://www.geocities.com/mhkonline2/downloads/cryptx.html.The latest news on our products are given here. The latest news relating to all kinds of works that we provide is made available at http://www.geocities.com/mhkonline2/solutions/. Feel free to visit our website at http://www.geocities.com/mhkonline2/. If you are a developer and want to know into the technology that we used to make this site, just mail us and we will provide you with the required details.

7.1 Disclaimer

We, Centrum Inc Software Solutions & VM Enterprises are not responsible for any data loss due to the use and or misuse of this program. It is entirely the responsibility of the end user to make sure he / she follows the instructions given by us.

7.2 Credits

Centrum Inc Software Solutions for doing the Research & Development required for making this program. The advanced scripting end was done by Centrum Inc Software Solutions.

VM Enterprises for marketing this program.

Artistik Expressionz for providing the graphical elements for this program. Also for the design and layout of the interface of the HTA.

Mhkonline2 for providing the web support and making available the documentation and updates on the web

---

Documentation for CryptX 4.1
June 2006

Centrum Inc Software Solutions
http://www.geocities.com/mhkonline2/
midhunhk@gmail.com