CryptoAlgo Documentation

Version 0.8.9

CryptoAlgro
Email: support@cryptoalgo.cf

5/13/20

About CryptoAlgo

Commonly asked questions:

Q1: What is CryptoAlgo?

Answer: CryptoAlgo is an encryption and decryption program that allows you to quickly and easily encrypt and decrypt private text and files.

Q2: What encryption algorithms are used in CryptoAlgo?

Answer: CryptoAlgo uses the US Military Grade **AES encryption algorithm** to encrypt your data (text or files) then uses the secure **RSA encryption algorithm** to encrypt the AES key files.

Q3: How do I encrypt my files?

Answer: To communicate with the other party, simply encrypt the AES keyfiles with your receiver's RSA Public key, then send the encrypted AES key files along with the encrypted data itself to your receiver. The receiver then uses its RSA Private key to decrypt the AES key files and then decrypts the data with them.

Q4: What encryption/decryption module does CryptoAlgo use?

Answer: CryptoAlgo uses the Node.js inbuilt Crypto library, which uses OpenSSL for its core functions, to encrypt/decrypt data. OpenSSL is extremely secure, and the version used has been verified to have no security flaws.

Questions? Problems? Suggestions?

Feel free to contact me anytime at support@cryptoalgo.cf should you encounter any problems while using CryptoAlgo.

A quick note from the developer:

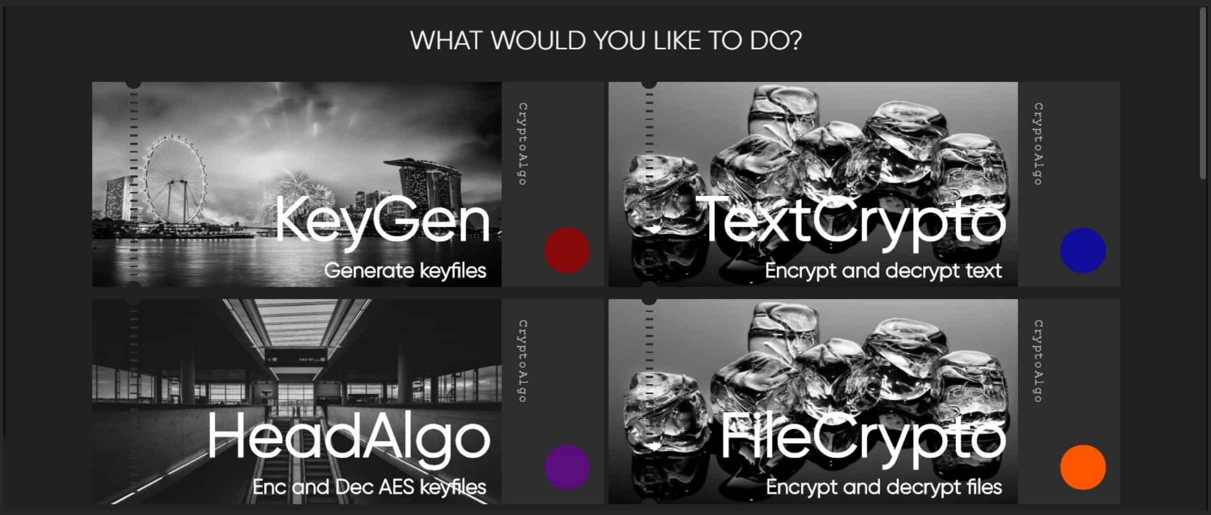
Please ensure that CryptoAlgo is up to date as older versions, especially beta/alpha releases, may have security vulnerabilities.

~ CryptoAlgo Inc.

13 May 2020
Developer contact: support@cryptoalgo.cf

CryptoAlgo Documentation

CryptoAlgo Selection Menu



Summary:

This program uses RSA to encrypt the AES key files (Key and IV) with the receiver's public key. Before the AES key files are encrypted, they are used to encrypt your data with AES256. The encrypted data can be sent with the encrypted key files to the other party and can be decrypted with the RSA private key of the receiver. These decrypted keys can then be used to decrypt the encrypted data with CryptoAlgo.

Detailed Explanation of Functions

CryptoAlgo has 5 options:

1. KeyGen – Generate RSA or AES Keyfiles
2. TextCrypto – Encrypt or Decrypt Text With AES
3. HeadAlgo – Encrypt or Decrypt AES Keyfiles with RSA
4. FileCrypto – Encrypt or Decrypt Files with AES
5. Settings (Not shown in screenshot) – Change CryptoAlgo Settings

The first option is straightforward, generating AES or RSA keyfiles. The RSA keypair generation wizard would generate an RSA keypair and store it in your Documents folder. The length of the generated keypair can be changed in CryptoAlgo Settings (option 5). Larger keypair length values gives a higher level of security but takes a longer time to encrypt or decrypt. As a rule of the thumb, with every 1000-byte increase of key modulus length, the generation time doubles. With every 5000-byte increase of key length, the decryption and encryption time doubles. Thus, the recommended value for key length is 9999 as it allows reasonable encryption, keypair generation and decryption durations while providing a good to strong amount of security.

13 May 2020
Developer contact: support@cryptoalgo.cf

Option 2 is where the actual encryption and decryption of text data happens. The function prompts for an input text, then tries to encrypt or decrypt it. For these functions to work, the decrypted AES key files must be present. If they are not found or corrupt, these functions would exit with errors. If the text input data for decryption is corrupt, the decrypt function would exit with an error.

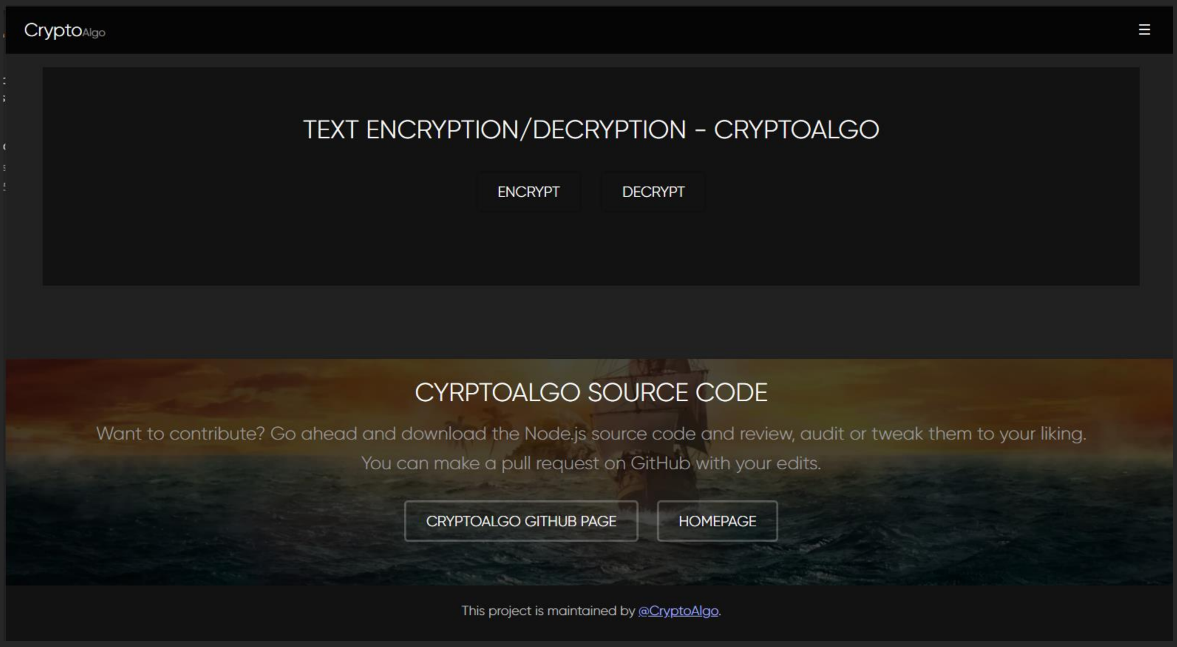
The next option encrypts and decrypts the AES header (AES key files), which can be done both before and after the data is encrypted, as this function does not override the encrypted or decrypted AES key files. The encrypt function produces two encrypted files named “enc_key.txt” and “enc_iv.txt” in your Documents directory. The decrypt function first looks for the encrypted AES key files, “enc_key.txt” and “enc_iv.txt” then continues to decrypt them. If the encrypted AES key files are not present, this function checks for the decrypted AES key files, “key.txt” and “iv.txt”. If the decrypted AES key files are present, the function exits successfully.

Option 4 is an experimental feature that allows you to encrypt or decrypt files. This function prompts for the file name relative to the location of the program. If the program is installed, the working directory would be C:\Program Files (x86)\CryptoAlgo\ as the main executable (CryptoAlgo-GUI.exe) is installed there. If CryptoAlgo is run in portable mode (not possible in version 2.8 Stable), the working directory is the location at which the program resides.

Relative paths are relative to the location of the main executable. An example of a relative path would be My Stuff\what I want to encrypt.txt where the location of the CryptoAlgo install is C:\Program Files(x86)\CryptoAlgo and the location of the file to be encrypted is C:\Program Files(x86)\CryptoAlgo\My Stuff\what I want to encrypt.txt . Notice how the path is added on to the installation directory of the program.

Absolute paths, on the other hand, are paths that not added on to the working directory of the program. For example, an absolute path would be C:\Some directory\Another one\An Important File.js . This is the absolute path of your file and is not relative to the path of the program.

Figure 2 – File encryption & decryption with AES



TEXT ENCRYPTION/DECRYPTION - CRYPTOALGO

CYRPTOALGO SOURCE CODE

Want to contribute? Go ahead and download the Node.js source code and review, audit or tweak them to your liking. You can make a pull request on GitHub with your edits.

This project is maintained by @CryptoAlgo.

CryptoAlgo Documentation V1.0.0

13 May 2020
Developer contact: support@cryptoalgo.cf