CryptoAlgo Documentation

CryptoAlgro
Email: cryptoalgro@gmail.com
Version 0.5:

CryptoAlgo Documentation

FIGURE 1 – CRYPTOALGO MENU

Simplified version:

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.

Full version:

This program has 9 options,

1. Generation of RSA keypair
2. Generation of AES key files
3. Encryption of AES key files
4. Decryption of AES key files
5. Encryption of data with AES
6. Decryption of data with AES
7. Continuous encryption and decryption of data with AES
8. File encryption with AES [Alpha]
9. File decryption with AES [Alpha]

The first two options are straightforward, generating AES or RSA keys. The RSA keypair generation wizard would prompt you for the keypair length. Larger keypair length values gives a higher level of security but takes a longer time to encrypt and decrypt the header. 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.

The next two options encrypt and decrypt the AES header or 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". 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.

Option 5 and 6 are where the actual encryption and decryption of text data happens. These functions prompt for an input text, then tries to encrypt or decrypt them. For these functions to work, the decrypted AES key files must be present. If they are not found or corrupt, these

Developer contact: cryptoalgro@gmail.com

functions would exit with errors. If the text input data for decryption is corrupt, the decrypt function would exit with an error.

Option 7 is a new function that allows you to continuously encrypt and decrypt text data. This function is actually a wrapper for option 5, 6 and 4. First, it runs option 4 to decrypt the AES key file and then runs option 5 and 6 continuously until “exit” is input.

Option 8 is an experimental feature in the alpha stage. Currently, it is the most automated function. This function shows the user a list of files in the current directory, then prompts for the number corresponding to the file they wish to encrypt or decrypt. Filenames of encrypted files are colored in purple for decryption and filenames of unencrypted files are colored purple for encryption. After encryption, the output file would have an added “encrypted_” to the filename. After decryption, the “encrypted_” tag would be removed from the file and instead “decrypted_” would be added. As this feature is still in the alpha stage, it is not yet available in the stable builds.

FIGURE 2 – FILE ENCRYPTION & DECRYPTION WITH AES