CLEAR CRYPTOSYSTEM

SDK Installation guide – Java Edition

Abstract

Start securing content to quantum-safe levels of encryption in less than two minutes. Easy to follow install installation guide provides steps to get you up and running fast.

Cipher IP
info@cipherip.com

Table of Contents

Section 1 – The CLEAR Cryptosystem SDK

Overview

Since the year 2001, the state of the art for symmetric encryption ciphers has remained essentially stagnant at a cipher strength level of 256-bits. The Advanced Encryption Standard (AES) with a 256-bit key remains the strongest commercially available algorithm. AES-256 was first announced in 1997, then adopted by the US National Institute of Standards and Technology (NIST) and published in 2001.

Do you remember what your mobile phone looked like in 1997?

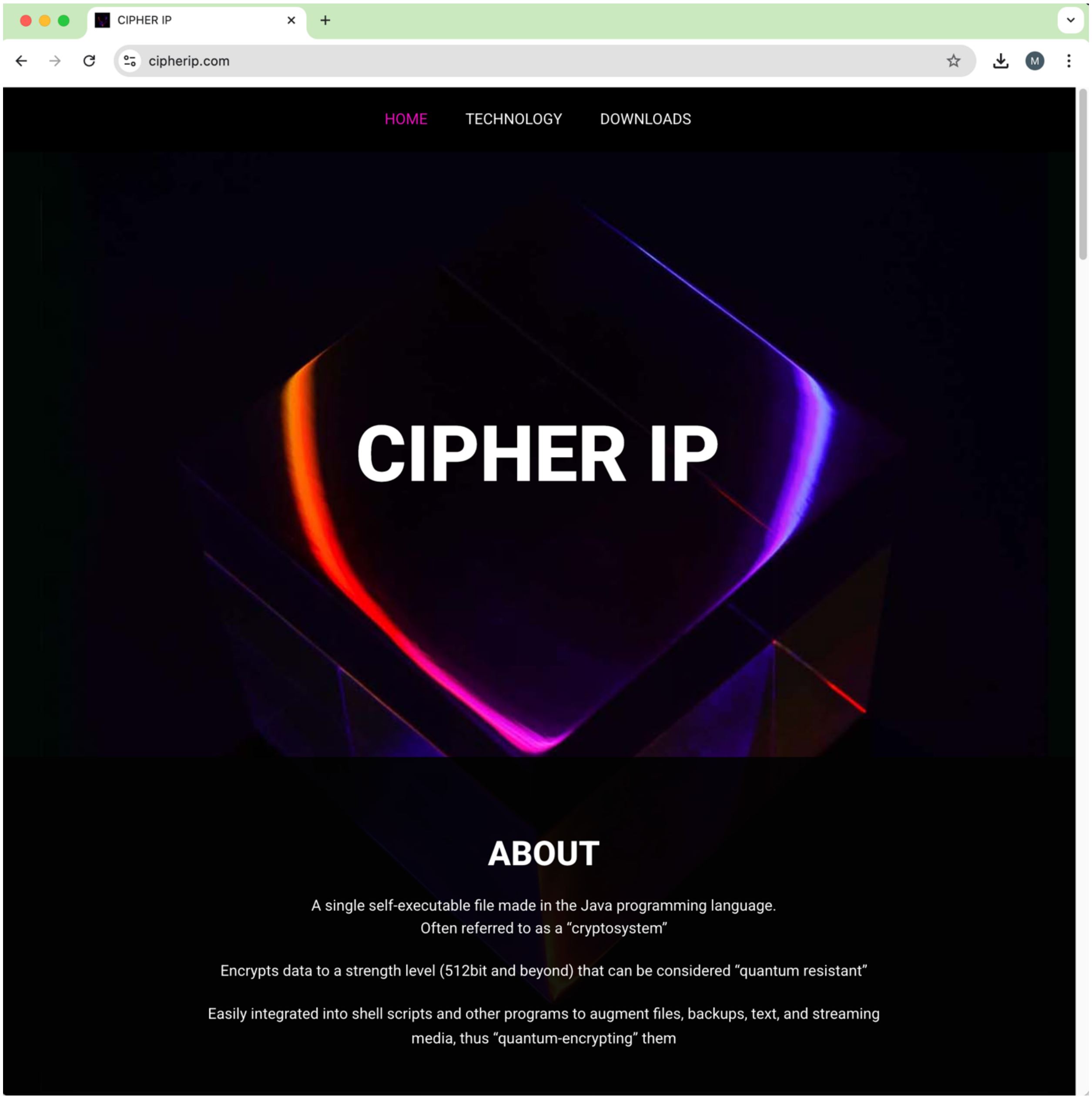
In March 2008, Daniel J. Bernstein created the CHACHA-20 stream cipher as a more efficient alternative to block ciphers like AES. Although many Intel CPUs now incorporate AES-NI (AES New-Instructions) and (AVX instruction sets) designed to improve the speed of the AES encryption / decryption functions, AES remains challenging for some smart phones and IIOT devices that do not include hardware performance boost. In 2013, the internet Engineering Task Force (IETF) standardized CHACHA-20 into the Transport Layer Security (TLS) protocol as a replacement for the aging RC4 cipher. Today, CHACHA-20 is widely used in the Linux kernel, OpenSSH, OpenSSL, and various Google projects. CHACHA-20 is typically implemented in a 128-bit strength mode of operation.

Quantum computers, once built, will be able to perform certain types of computations much faster than classical computers. This includes breaking many of the encryption algorithms currently in use, such as RSA and elliptic curve cryptography (ECC). To address this threat, NIST introduced a post-quantum competition beginning in 2017 to encourage innovation for the next generation of “quantum resistant” algorithms. To be “quantum safe”, it is suggested that ciphers should have 512-bit strength or above. NIST’s competition for next-generation cryptographic ciphers has yet to be concluded.

Download the CLEAR SDK

1.1 Download Outlets

The CLEAR Cryptosystem SDK (“CLEAR”) can be downloaded from our website at www.cipherip.com.



ABOUT

A single self-executable file made in the Java programming language.
Often referred to as a “cryptosystem”

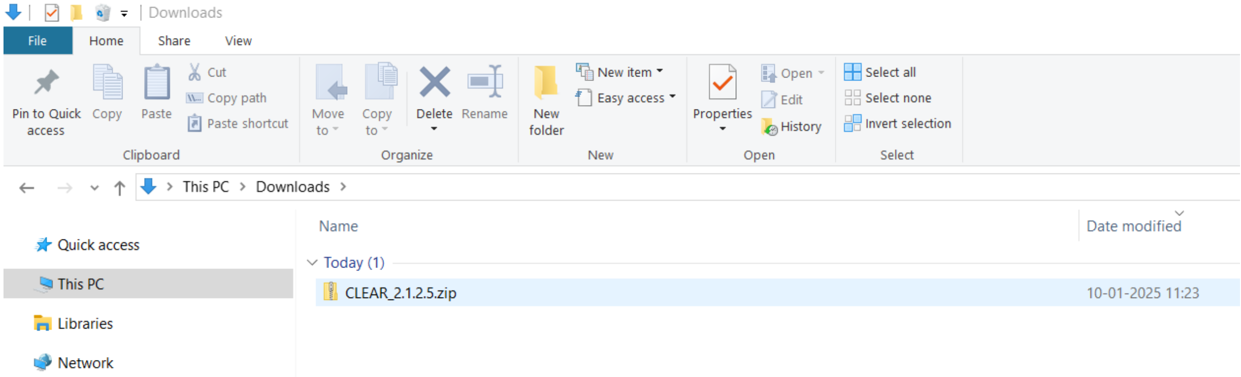
Encrypts data to a strength level (512bit and beyond) that can be considered “quantum resistant”

Easily integrated into shell scripts and other programs to augment files, backups, text, and streaming media, thus “quantum-encrypting” them

1.2 Receiving the Download

Your copy of CLEAR is "cross platform" and will work with Windows, Mac, and Linux. The download consists of a single .ZIP file containing the SDK, documentation, as well as information and accessories. CLEAR **does not require** any install routines, MSI, or executable to be deployed. Simply unzip your copy of CLEAR anywhere you like to keep and store files. As a developer SDK tool, most likely you will keep CLEAR in the "classpath" of your Java applications along with other commonly used Java JAR file libraries.

Note: You may have downloaded a *version* of CLEAR that is different to the one pictured in the examples.



CLEAR_2.1.2.5.zip 10-01-2025 11:23

Figure 1 - Download of CLEAR to the Downloads Folder - as shown on a PC

1.3 Unzip & Verify the Package

Unzipping the CLEAR download (payload) reveals the following content:

FILENAME	**PURPOSE**
clear_n.n.n.n.jar	This is CLEAR. Nothing else is required to run the program.
ccj-3.0.1.jar	Optional FIPS 140-3 compliance module. Use w/ CLEAR for FIPS.
API DOCUMENTATION	**PURPOSE**
install_guide.pdf	This document – explains how to install and license CLEAR.
API-strings.pdf	API document. Best place to begin! Learn how to encrypt text.
UNIT TESTS	**PURPOSE**
Unit_Tests.zip	Functional code examples – illustrates how to use CLEAR.

Note: For extra security, please check the SHA-512 Hash validation of your download on our website.

Pre-Requisites

1.4 The Java Runtime Environment (JRE) or (JDK)

The CLEAR Cryptosystem (Java Edition) is a single streamlined JAR file with no external dependencies. CLEAR is optimized to run on the latest (current) Java Virtual Machine (JVM) and is backward compatible to the 2006-era of Java, JDK 1.6.X.   You will need a copy of the Java Runtime installed on your system to proceed with CLEAR.

The following are popular options for downloading Java:

Oracle's Java Development Kit (JDK):
https://www.oracle.com/java/technologies/javase-downloads.html

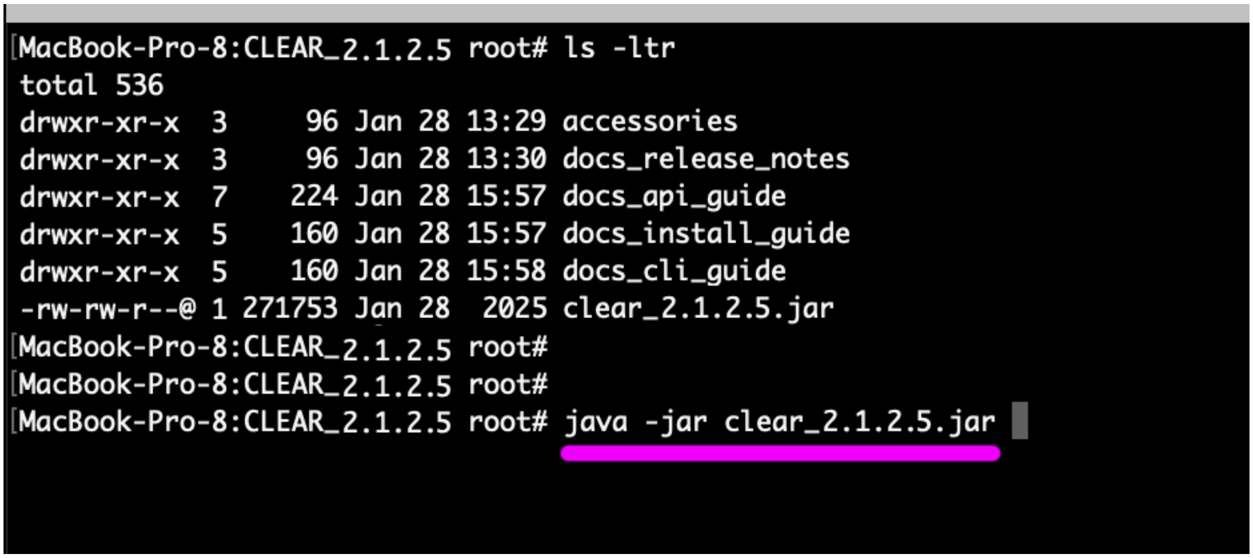
OpenJDK – (A free and open-source implementation of the JDK):
https://adoptopenjdk.net

Amazon Corretto – (Amazon's own JDK distribution that is based on OpenJDK):
https://aws.amazon.com/corretto

1.5 Testing CLEAR with JVM

Test that your version of CLEAR is working with your installed version of the Java Runtime Environment by typing the following at the command prompt or terminal window:

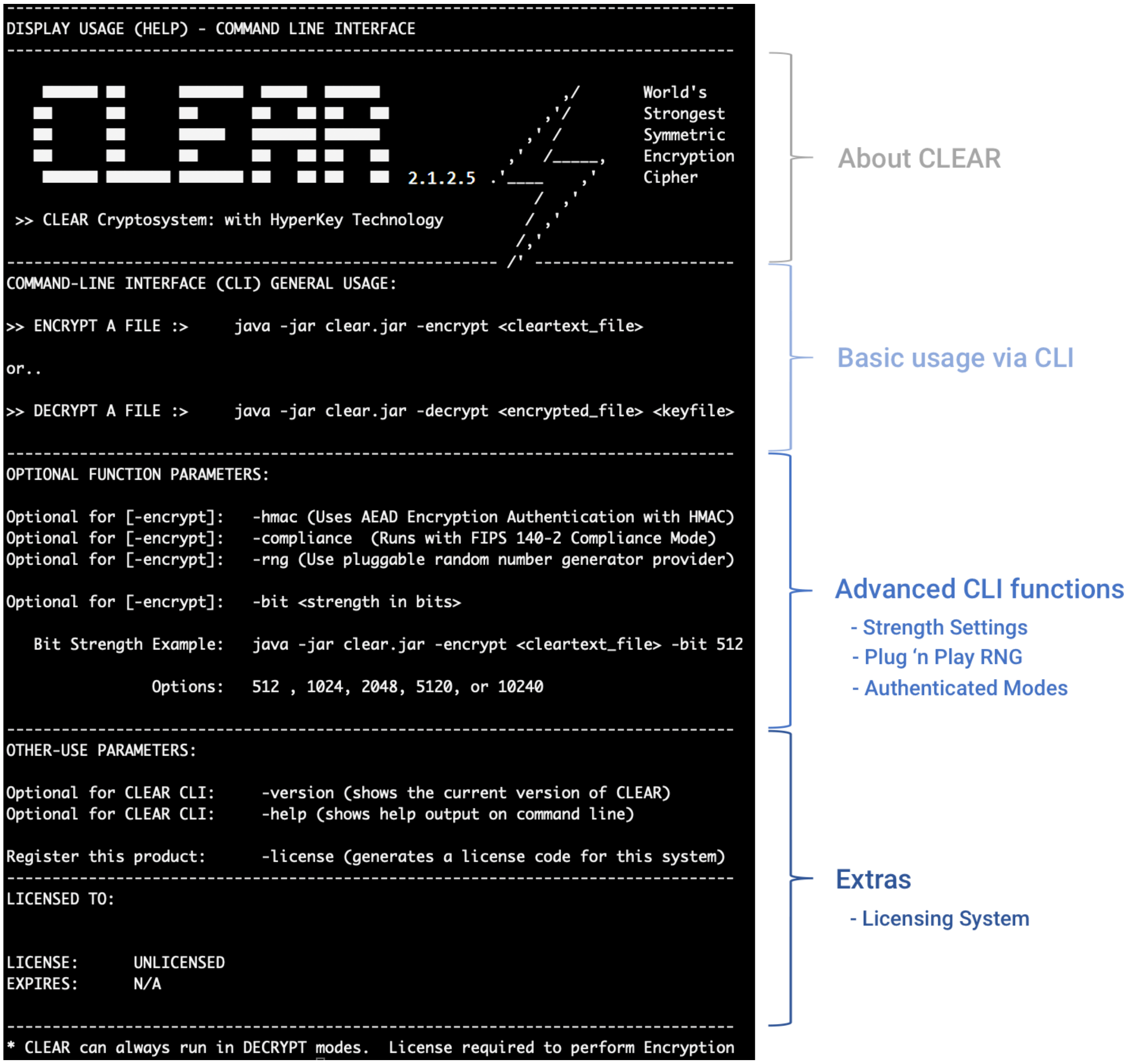
```
java -jar clear_2.1.2.5.jar
```



```
[MacBook-Pro-8:CLEAR_2.1.2.5 root# ls -ltr
total 536
drwxr-xr-x  3     96 Jan 28 13:29 accessories
drwxr-xr-x  3     96 Jan 28 13:30 docs_release_notes
drwxr-xr-x  7    224 Jan 28 15:57 docs_api_guide
drwxr-xr-x  5    160 Jan 28 15:57 docs_install_guide
drwxr-xr-x  5    160 Jan 28 15:58 docs_cli_guide
-rw-rw-r--@ 1 271753 Jan 28  2025 clear_2.1.2.5.jar
[MacBook-Pro-8:CLEAR_2.1.2.5 root#
[MacBook-Pro-8:CLEAR_2.1.2.5 root#
[MacBook-Pro-8:CLEAR_2.1.2.5 root# java -jar clear_2.1.2.5.jar
```

Figure 3 - Test the CLEAR JAR file from command-line interface

Once the Java environment has been installed correctly, a test run of CLEAR from the command prompt or terminal window will display the CLEAR CLI "help splash-screen" as shown below:



```
-------------------------------------------------------------------------------
DISPLAY USAGE (HELP) - COMMAND LINE INTERFACE
-------------------------------------------------------------------------------

    ██████ ██      ███████  █████  ██████                   ,/        World's
   ██      ██      ██      ██   ██ ██   ██                ,'/         Strongest
   ██      ██      █████   ███████ ██████                ,' /         Symmetric
   ██      ██      ██      ██   ██ ██   ██             ,'  /_____,    Encryption
    ██████ ███████ ███████ ██   ██ ██   ██ 2.1.2.5 .'____     ,'      Cipher
                                                         /  ,'
 >> CLEAR Cryptosystem: with HyperKey Technology        / ,'
                                                       /,'
------------------------------------------------------ /' --------------------
COMMAND-LINE INTERFACE (CLI) GENERAL USAGE:

>> ENCRYPT A FILE :>     java -jar clear.jar -encrypt <cleartext_file>

or..

>> DECRYPT A FILE :>     java -jar clear.jar -decrypt <encrypted_file> <keyfile>

-------------------------------------------------------------------------------
OPTIONAL FUNCTION PARAMETERS:

Optional for [-encrypt]:   -hmac (Uses AEAD Encryption Authentication with HMAC)
Optional for [-encrypt]:   -compliance  (Runs with FIPS 140-2 Compliance Mode)
Optional for [-encrypt]:   -rng (Use pluggable random number generator provider)

Optional for [-encrypt]:   -bit <strength in bits>

   Bit Strength Example:   java -jar clear.jar -encrypt <cleartext_file> -bit 512

                Options:   512 , 1024, 2048, 5120, or 10240

-------------------------------------------------------------------------------
OTHER-USE PARAMETERS:

Optional for CLEAR CLI:     -version (shows the current version of CLEAR)
Optional for CLEAR CLI:     -help (shows help output on command line)

Register this product:      -license (generates a license code for this system)
-------------------------------------------------------------------------------
LICENSED TO:


LICENSE:      UNLICENSED
EXPIRES:      N/A

-------------------------------------------------------------------------------
* CLEAR can always run in DECRYPT modes.  License required to perform Encryption
```

Figure 4 - CLEAR Help Splash Screen (Un-licensed)

Additional license information will be displayed in the bottom section of CLEAR help splash-screen once the product has been licensed. At this point CLEAR can be used to decrypt data; however, it will not be able to encrypt new data until a license key is associated with the CLEAR JAR file.

Section 2 – Licensing & Activation

CLEAR requires a localized license file to run encryption functions. It is this local license that enables CLEAR to run entirely offline and without access to the internet. CLEAR Licenses are delineated by strength and feature.

CLEAR Licenses are available in any of the following combinations:

STRENGTH	INDIV-FEATURE	RENEWAL PERIOD	LICENSE TYPE	EXTENSIBILITY
512-bit	HMAC / AEAD	Monthly	Individual	Single Machine
1,024-bit	MFA Mode	Annually	Enterprise	Three Machine
2,048-bit	Hyper Key Mode	Three Year	Embedded	Five Machine
5,120-bit	CLEAR Key Tool			Unlimited
10,240-bit	Airgap Mode			

Note: The CLEAR **30-DAY FREE TRIAL** license includes strengths up to 2,048-bit with most of the optional individual features except for Airgap and Hyper Key Mode.

Licensing CLEAR

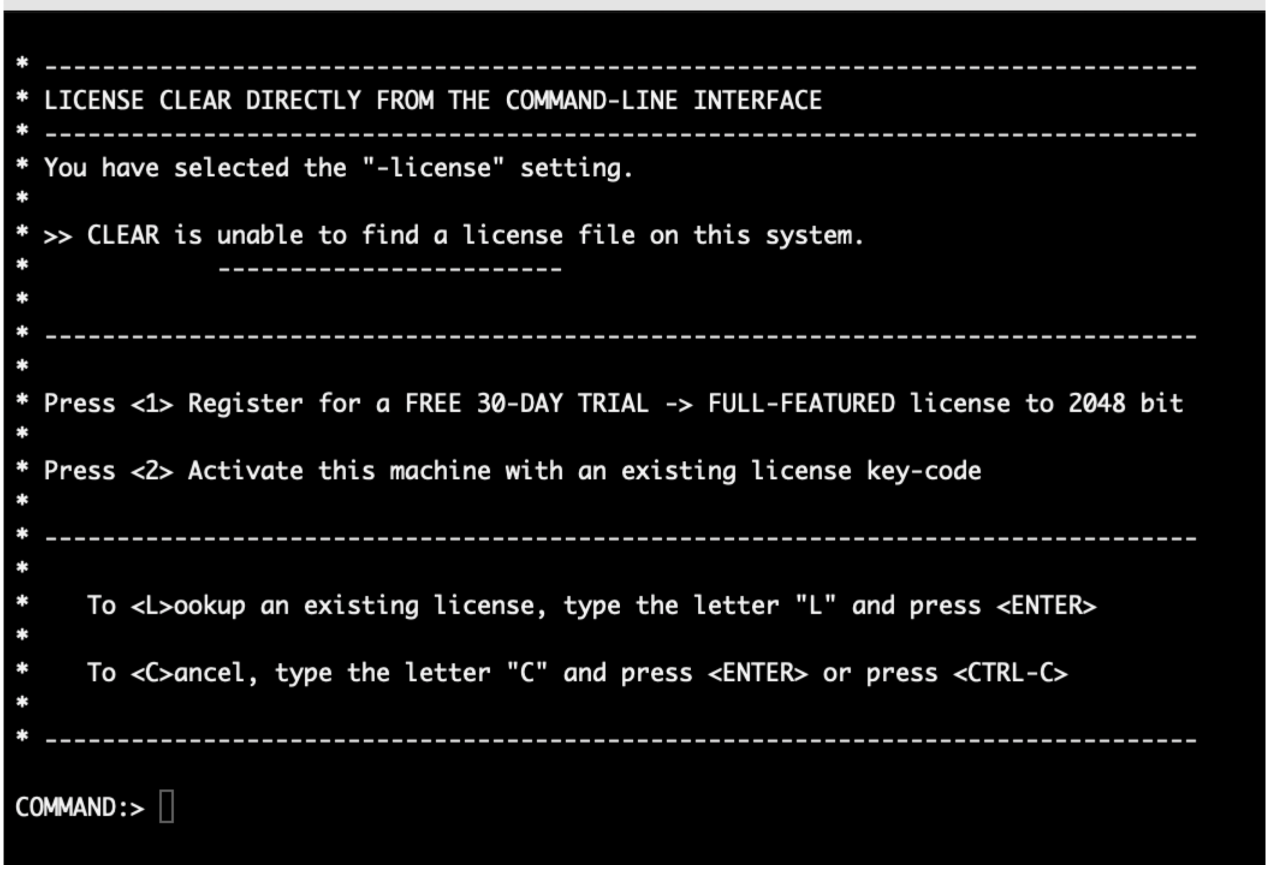
2.1 Free Trial License – Command-Line Interface

CLEAR licenses may be obtained online at our website at www.cipherip.com. From there, you can choose a **30-DAY FREE TRIAL** license, or shop online for a commercial license to purchase. Different licenses will enable different features of the CLEAR Cryptosystem.

In addition to purchasing a license online, CLEAR may also be licensed directly from the command prompt or terminal. Note, licensing from the Command Line Interface (CLI) requires an internet connection. This section describes how to activate a **30-DAY FREE TRIAL** license of clear directly from the CLI.

From a folder with the CLEAR JAR, type the following at the CLI:

```
java -jar clear_2.1.2.5.jar -license
```



```
* -------------------------------------------------------------------------------
* LICENSE CLEAR DIRECTLY FROM THE COMMAND-LINE INTERFACE
* -------------------------------------------------------------------------------
* You have selected the "-license" setting.
*
* >> CLEAR is unable to find a license file on this system.
*           -------------------------
*
* -------------------------------------------------------------------------------
*
* Press <1> Register for a FREE 30-DAY TRIAL -> FULL-FEATURED license to 2048 bit
*
* Press <2> Activate this machine with an existing license key-code
*
* -------------------------------------------------------------------------------
*
*    To <L>ookup an existing license, type the letter "L" and press <ENTER>
*
*    To <C>ancel, type the letter "C" and press <ENTER> or press <CTRL-C>
*
* -------------------------------------------------------------------------------

COMMAND:>
```

Figure 5 - Begin the CLI licensing workflow

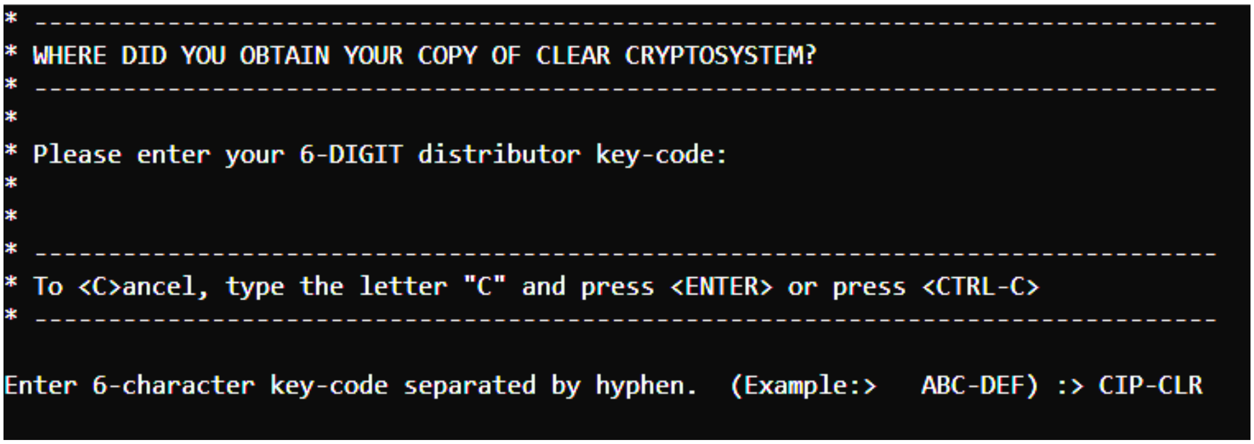
Running the CLEAR JAR File from the CLI with the "-license" parameter starts a brief interactive CLI workflow with several options. To activate a **30-DAY FREE TRIAL** license, select the first option by typing the **number 1** into the terminal, then press enter key. Other licensing options will be covered a bit later in this document.

2.2 Distributor Key-Code

Quantum Knight works with channel partners and various resellers that may white-label CLEAR or use different branding. For this reason, CLEAR requires a distributor code to identify the licensor of this system.

At the prompt, use the distributor code:

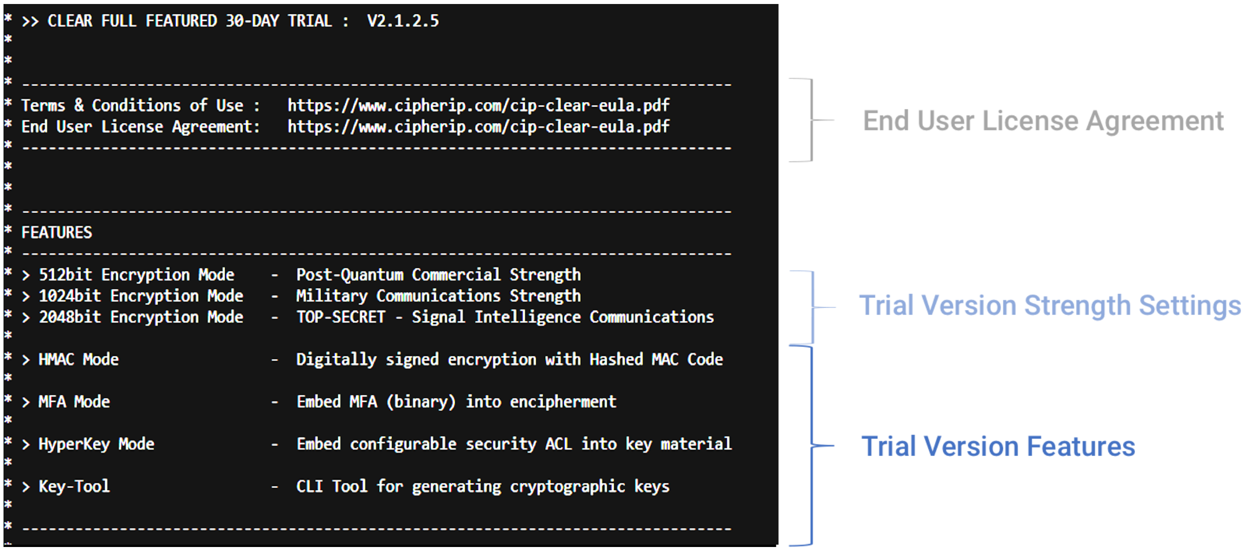
CIP-CLR



```
* --------------------------------------------------------------------------------
* WHERE DID YOU OBTAIN YOUR COPY OF CLEAR CRYPTOSYSTEM?
* --------------------------------------------------------------------------------
*
* Please enter your 6-DIGIT distributor key-code:
*
*
* --------------------------------------------------------------------------------
* To <C>ancel, type the letter "C" and press <ENTER> or press <CTRL-C>
* --------------------------------------------------------------------------------

Enter 6-character key-code separated by hyphen.  (Example:>   ABC-DEF) :> CIP-CLR
```

Figure 6 - Enter the Distributor Code "QKI-CLR"

After selecting the distributor, a list of available features for this license type will be displayed, as well as links to the End User License Agreement (EULA). The trial version of CLEAR does not necessarily include 100% of available features and may also differ by distributor.

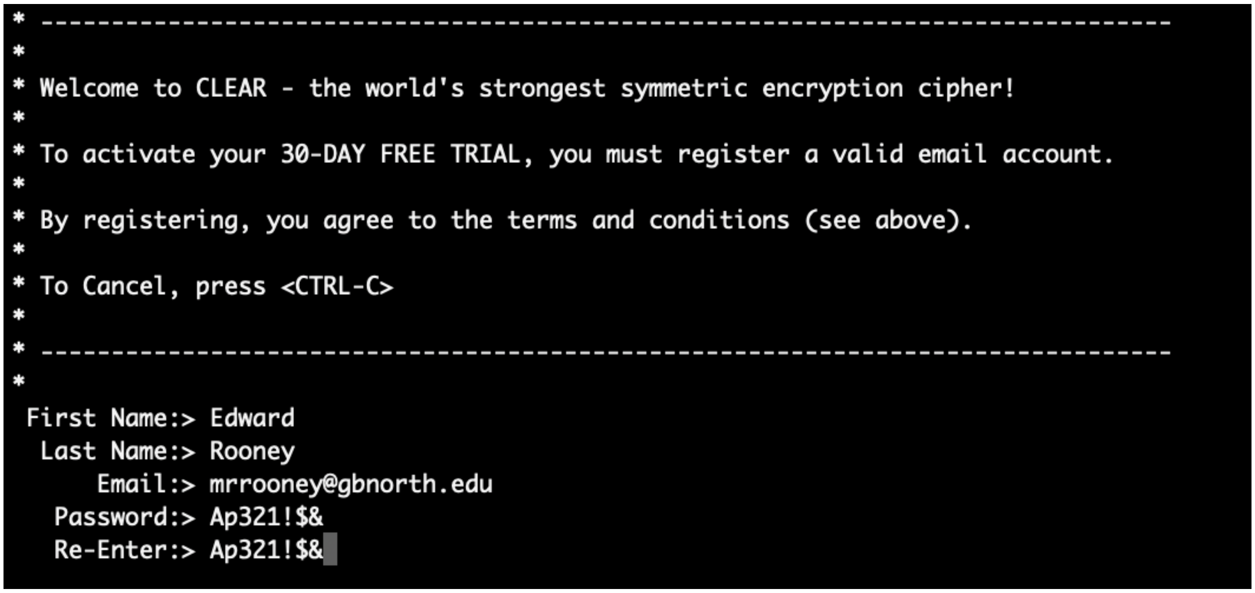


```
* >> CLEAR FULL FEATURED 30-DAY TRIAL :  V2.1.2.5
*
*
* ---------------------------------------------------------------------------------
* Terms & Conditions of Use :   https://www.cipherip.com/cip-clear-eula.pdf
* End User License Agreement:   https://www.cipherip.com/cip-clear-eula.pdf
* ---------------------------------------------------------------------------------
*
*
* ---------------------------------------------------------------------------------
* FEATURES
* ---------------------------------------------------------------------------------
* > 512bit Encryption Mode    -  Post-Quantum Commercial Strength
* > 1024bit Encryption Mode   -  Military Communications Strength
* > 2048bit Encryption Mode   -  TOP-SECRET - Signal Intelligence Communications
*
* > HMAC Mode                 -  Digitally signed encryption with Hashed MAC Code
*
* > MFA Mode                  -  Embed MFA (binary) into encipherment
*
* > HyperKey Mode             -  Embed configurable security ACL into key material
*
* > Key-Tool                  -  CLI Tool for generating cryptographic keys
*
* ---------------------------------------------------------------------------------
```

Figure 7 - Features of Trial License Displayed

2.3 Minimal Signup

CLEAR **30-DAY FREE TRIAL** licenses may be extended on up to **3 MACHINES** for a single user account. Valid email address is required to establish a trial license. Trial licenses may not be renewed for a given email address. Additional MFA security protections and more detailed account setup with various purchasing options for full licenses may found online at https://cipherip.com.

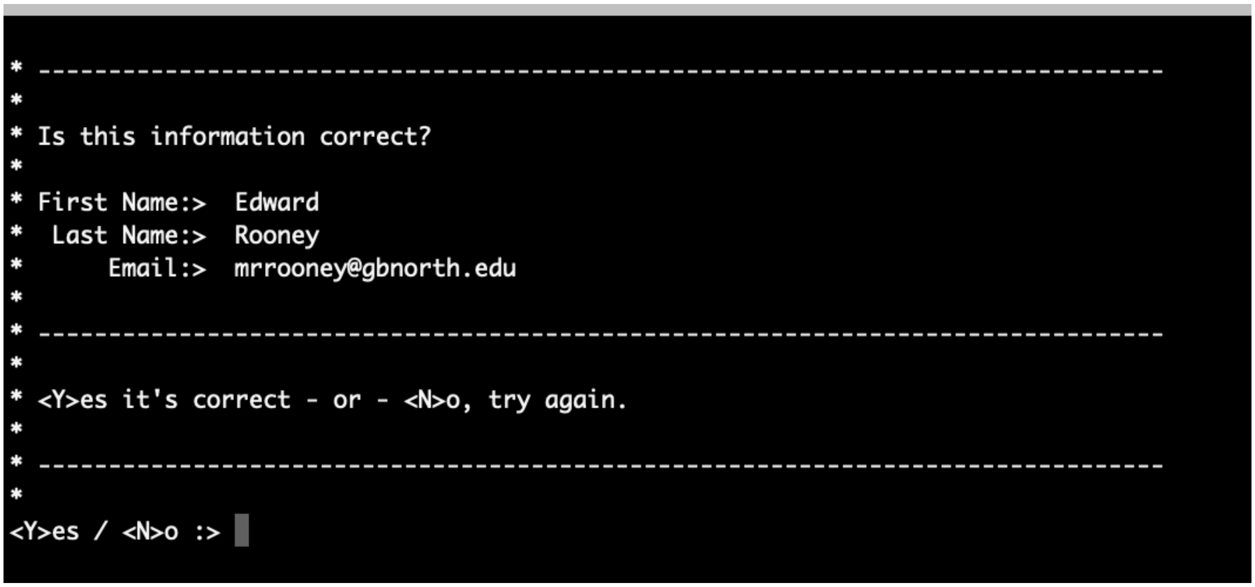


```
* ---------------------------------------------------------------------------------
*
* Welcome to CLEAR - the world's strongest symmetric encryption cipher!
*
* To activate your 30-DAY FREE TRIAL, you must register a valid email account.
*
* By registering, you agree to the terms and conditions (see above).
*
* To Cancel, press <CTRL-C>
*
* ---------------------------------------------------------------------------------
*
 First Name:> Edward
  Last Name:> Rooney
      Email:> mrrooney@gbnorth.edu
   Password:> Ap321!$&
   Re-Enter:> Ap321!$&
```

Figure 8- License Screen 3 with User Signup

Data entry requirements for user signup are as follows:

- **First Name & Last Name**: May not contain any special characters
- **Email Address**: Must be a valid email address. Trial licenses only sent 1X per unique email.
- **Password**: Minimum 8-characters with upper, lower, number, and special character required.



```
* ---------------------------------------------------------------------------------
*
* Is this information correct?
*
* First Name:>  Edward
*  Last Name:>  Rooney
*      Email:>  mrrooney@gbnorth.edu
*
* ---------------------------------------------------------------------------------
*
* <Y>es it's correct - or - <N>o, try again.
*
* ---------------------------------------------------------------------------------
*
<Y>es / <N>o :>
```

Figure 9- License Screen 3 with User Signup

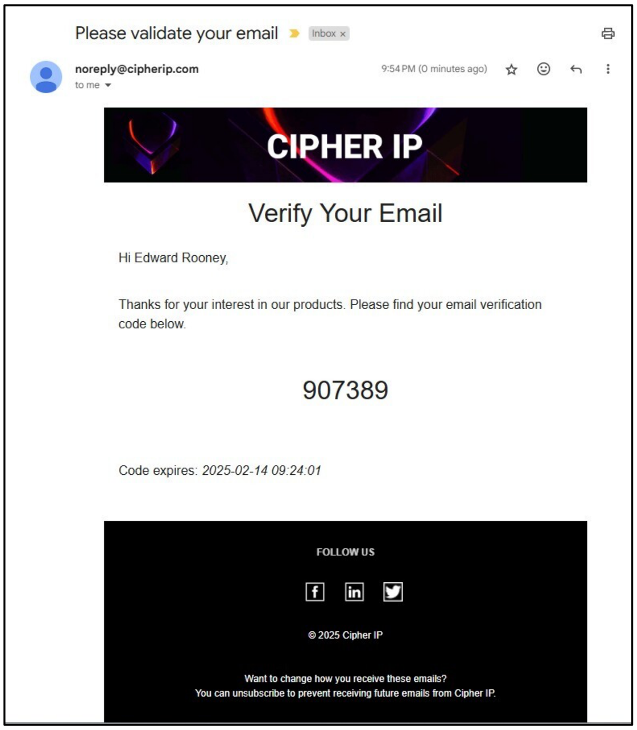
2.4 Email Verification

Within a few moments, you should receive a verification email from noreply@cipherip.com. Please be sure to check your spam or junk folder. If you do not receive a verification email, contact our support group at support@cipherip.com.

Your verification email contains a **six-digit** code that will remain valid for up to **1 hour**.

If you do not receive an email or you have waited longer than **1 hour**, restart the process to try again.

Quantum Knight support team is available during US business hours and can be reached via email at: support@cipherip.com



Please validate your email

noreply@cipherip.com 9:54 PM (0 minutes ago)

Verify Your Email

Hi Edward Rooney,

Thanks for your interest in our products. Please find your email verification code below.

907389

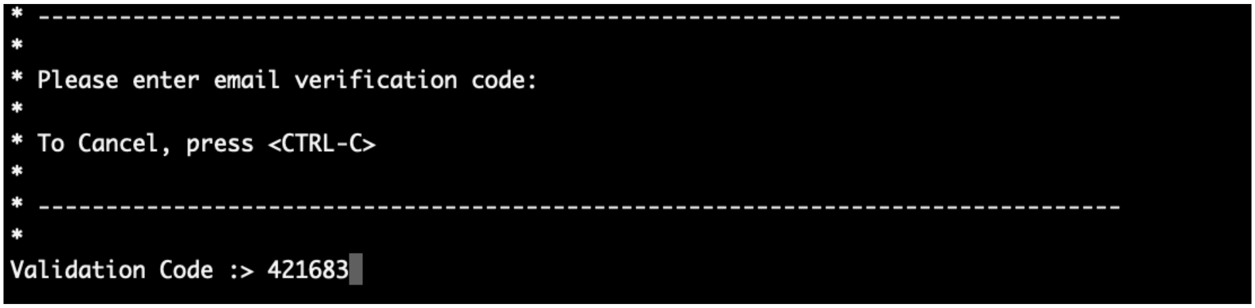
Code expires: *2025-02-14 09:24:01*

© 2025 Cipher IP

Want to change how you receive these emails?
You can unsubscribe to prevent receiving future emails from Cipher IP.

Figure 1 - Verification Email with Code

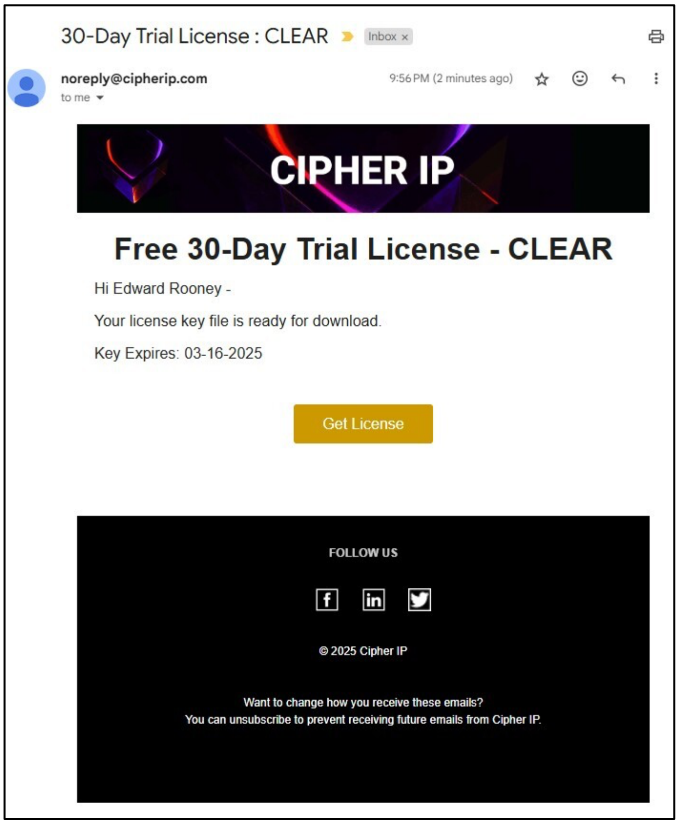
Once you have received your verification email, enter the 6-digit code at the prompt:



```
* ---------------------------------------------------------------------------
*
* Please enter email verification code:
*
* To Cancel, press <CTRL-C>
*
* ---------------------------------------------------------------------------
*
Validation Code :> 421683
```

2.5 License Issuance

If this is your first time requesting a trial license, you will see a message informing you that your trial license has been created and a reminder to check your email. If you have already used a trial license but would like to request another one, kindly please send us email at support@cipherip.com.



30-Day Trial License : CLEAR

noreply@cipherip.com

to me

9:56 PM (2 minutes ago)

CIPHER IP

Free 30-Day Trial License - CLEAR

Hi Edward Rooney -

Your license key file is ready for download.

Key Expires: 03-16-2025

© 2025 Cipher IP

Want to change how you receive these emails?
You can unsubscribe to prevent receiving future emails from Cipher IP.

Figure 2- License Key Download Email

Your **30-DAY FREE TRIAL** license can be directly downloaded from email. Click "**Get License**" button.

If you do not receive an email or you have waited longer than 1 hour, you may "**Lookup**" your license code via the first screen in CLI license process by selecting option "L". Detailed examples for license recovery via "Lookup" are available in the sections below.

This license email is valid for:

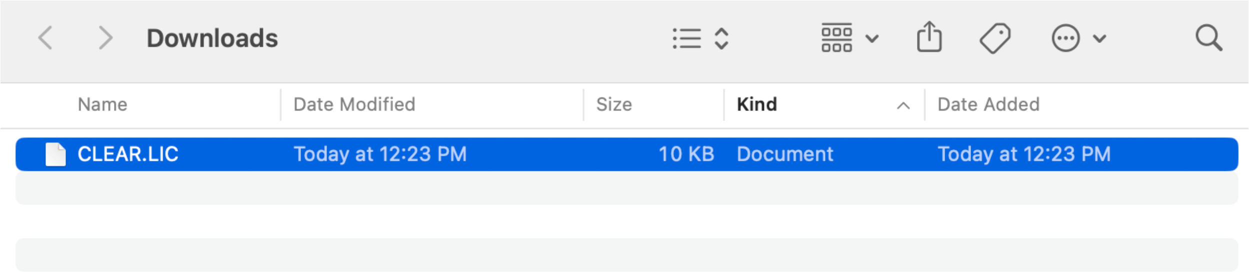
- **24 HOURS**

The license link may be used:

- **3 TIMES**

Quantum Knight support team is available during US business hours and can be reached via email at: support@cipherip.com

Successful license recovery will result in the immediate download of your unique "**CLEAR.LIC**" license file.



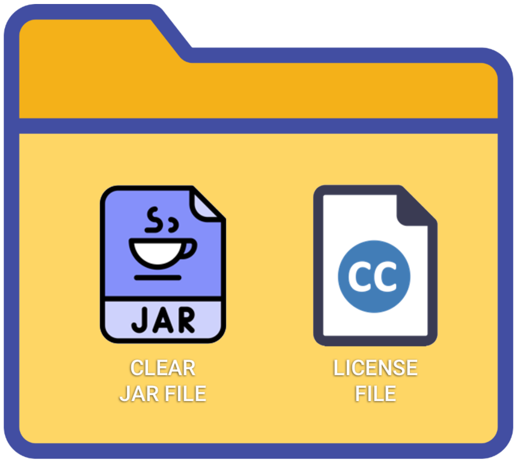
Downloads

Name	Date Modified	Size	Kind	Date Added
CLEAR.LIC	Today at 12:23 PM	10 KB	Document	Today at 12:23 PM

2.6 Associate License with CLEAR

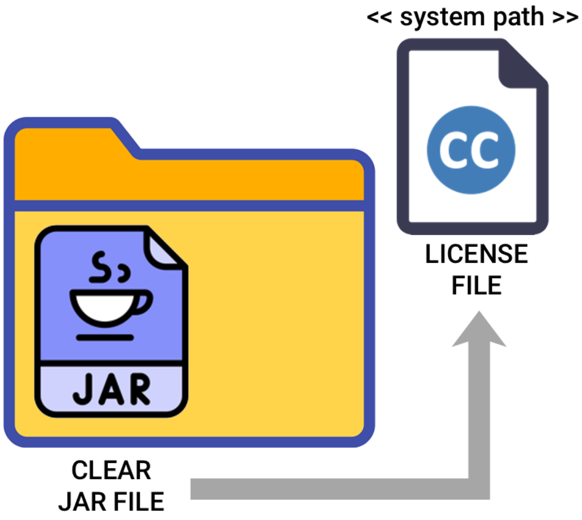
There are **two [2] methods** for CLEAR to associate with a corresponding license file. The simplest arrangement is to keep the license file together in the same local folder or directory as the CLEAR JAR file. Recognizing that such an arrangement may be undesirable or infeasible in certain cases, you may also set a “System Variable” that the CLEAR JAR will recognize to maintain these two artifacts separately.

Once you have acquired a license file, deploy in either of these arrangements:



Method 1: License file in same folder as JAR File

Simply copy the **CLEAR.LIC** file into the same folder or directory as **clear_n.n.n.n.jar**.



Method 2: Reference license file via System Path

Establish a system variable with the name CLEAR_LIC and a value with the absolute path to the location of the **CLEAR.LIC** file.

Example Windows:

```
set CLEAR_LIC=c:\temp\CLEAR.LIC
```

Example Mac / Linux:

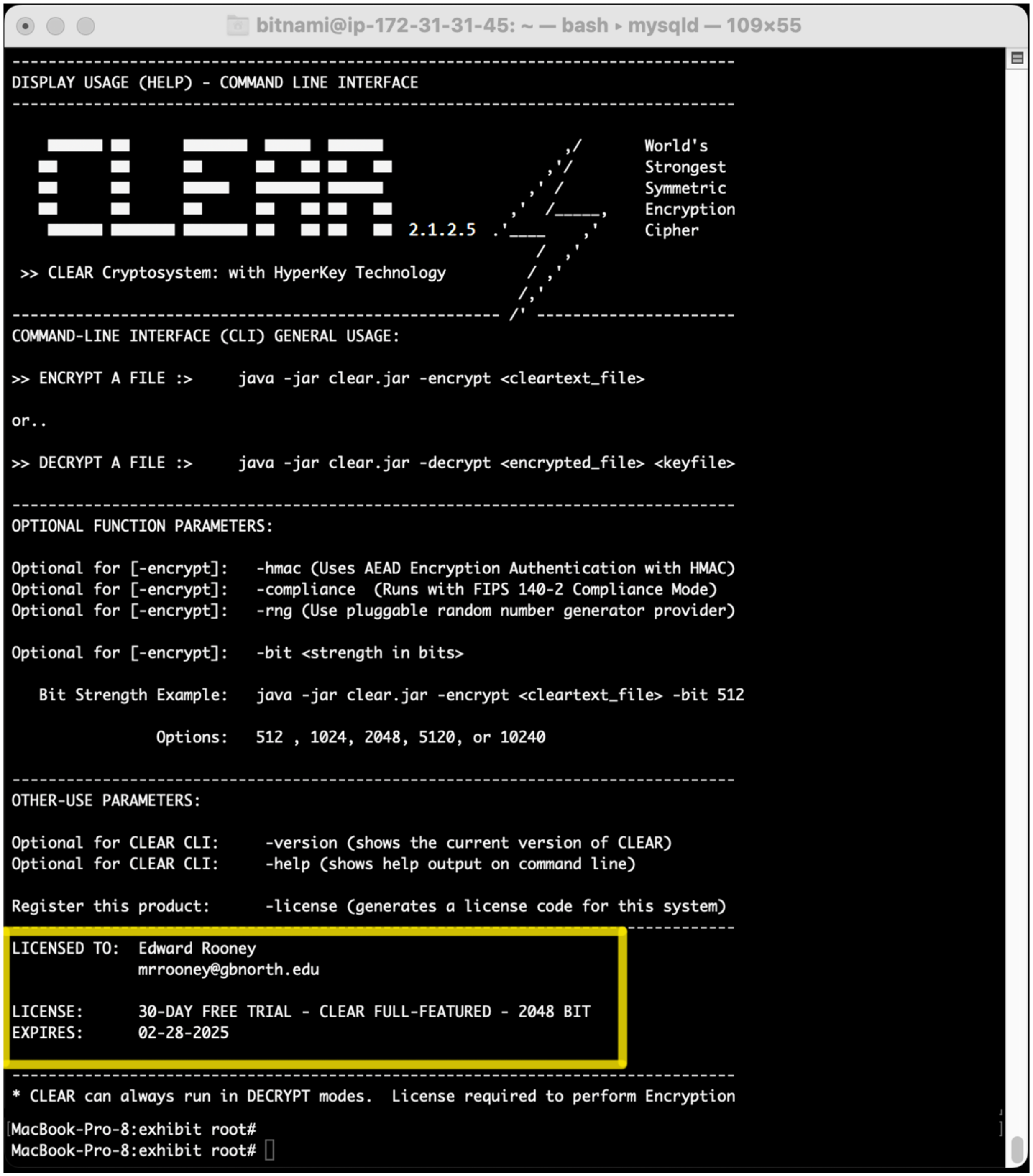
```
export CLEAR_LIC=/temp/CLEAR.LIC
```

Note: You may use any folder you like. “temp” is only meant as an example here.

2.7 Test License Association

To test the activation status of a CLEAR license with the CLEAR JAR, type the following at the CLI:

```
java -jar clear_2.1.2.5.jar
```



```
--------------------------------------------------------------------------------
DISPLAY USAGE (HELP) - COMMAND LINE INTERFACE
--------------------------------------------------------------------------------

                                                            ,/      World's
                                                          ,'/       Strongest
                                                        ,' /        Symmetric
                                                      ,'  /_____,   Encryption
                                        2.1.2.5     .'____    ,'    Cipher
                                                         /  ,'
 >> CLEAR Cryptosystem: with HyperKey Technology        / ,'
                                                       /,'
------------------------------------------------------ /' ----------------------
COMMAND-LINE INTERFACE (CLI) GENERAL USAGE:

>> ENCRYPT A FILE :>     java -jar clear.jar -encrypt <cleartext_file>

or..

>> DECRYPT A FILE :>     java -jar clear.jar -decrypt <encrypted_file> <keyfile>

--------------------------------------------------------------------------------
OPTIONAL FUNCTION PARAMETERS:

Optional for [-encrypt]:   -hmac (Uses AEAD Encryption Authentication with HMAC)
Optional for [-encrypt]:   -compliance  (Runs with FIPS 140-2 Compliance Mode)
Optional for [-encrypt]:   -rng (Use pluggable random number generator provider)

Optional for [-encrypt]:   -bit <strength in bits>

   Bit Strength Example:   java -jar clear.jar -encrypt <cleartext_file> -bit 512

                Options:   512 , 1024, 2048, 5120, or 10240

--------------------------------------------------------------------------------
OTHER-USE PARAMETERS:

Optional for CLEAR CLI:     -version (shows the current version of CLEAR)
Optional for CLEAR CLI:     -help (shows help output on command line)

Register this product:      -license (generates a license code for this system)
--------------------------------------------------------------------------------
LICENSED TO:  Edward Rooney
              mrrooney@gbnorth.edu

LICENSE:      30-DAY FREE TRIAL - CLEAR FULL-FEATURED - 2048 BIT
EXPIRES:      02-28-2025

--------------------------------------------------------------------------------
* CLEAR can always run in DECRYPT modes.  License required to perform Encryption

MacBook-Pro-8:exhibit root#
MacBook-Pro-8:exhibit root#
```

Figure 3 - Activated 30-Day Trial License

Your license activation status will be displayed in the area shown lighted in figure 12.

Using CLEAR

Ready to grind your data through the most powerful commercial shredding mechanism ever created? Wait no longer. CLEAR Cryptosystem enciphers data to a level not reversable by Quantum Computers.

CLEAR encryption produces encipherment ranging from **512-bit** to **10,240-bit** strength. The probability of guessing a 512-bit key is approximately **1 in 3.4 x 10^154**. At maximum operating strength, CLEAR can encipher data to a key space that would require **2^10,240** possible combinations to reverse / brute force.

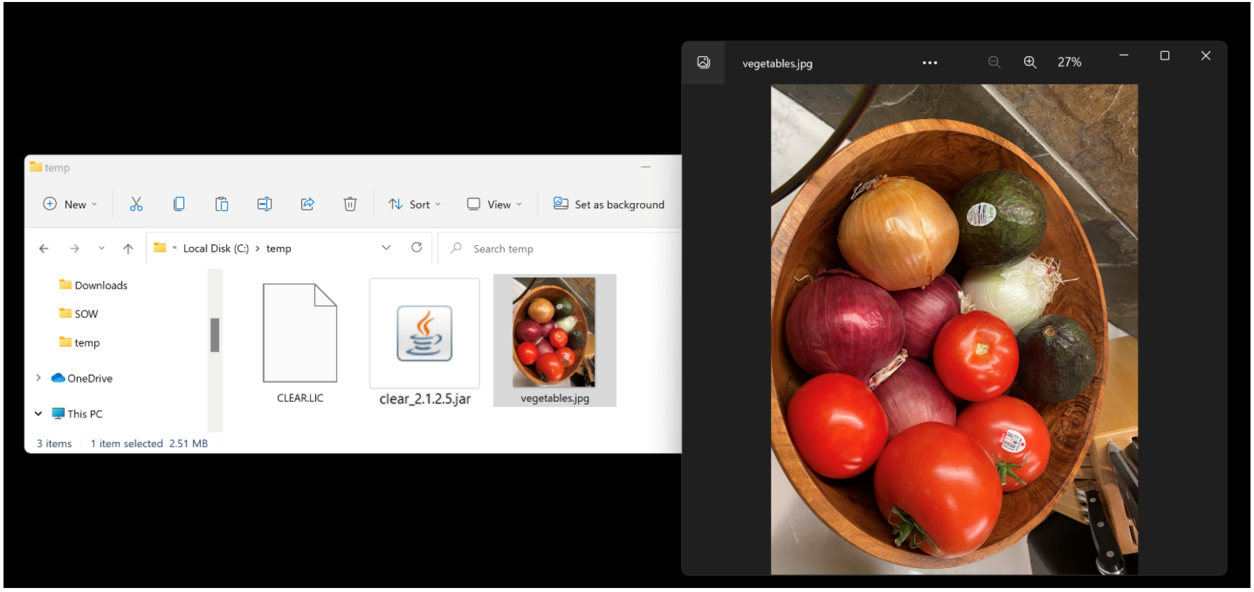
According to **Chat-GPT**; "*… The probability of guessing a 10240-bit key space is extremely low, effectively zero for all practical purposes. A 10240-bit key space provides 2^10240 possible combinations, which is an astronomically large number. To put it into perspective, the estimated number of atoms in the observable universe is around 10^80.*"

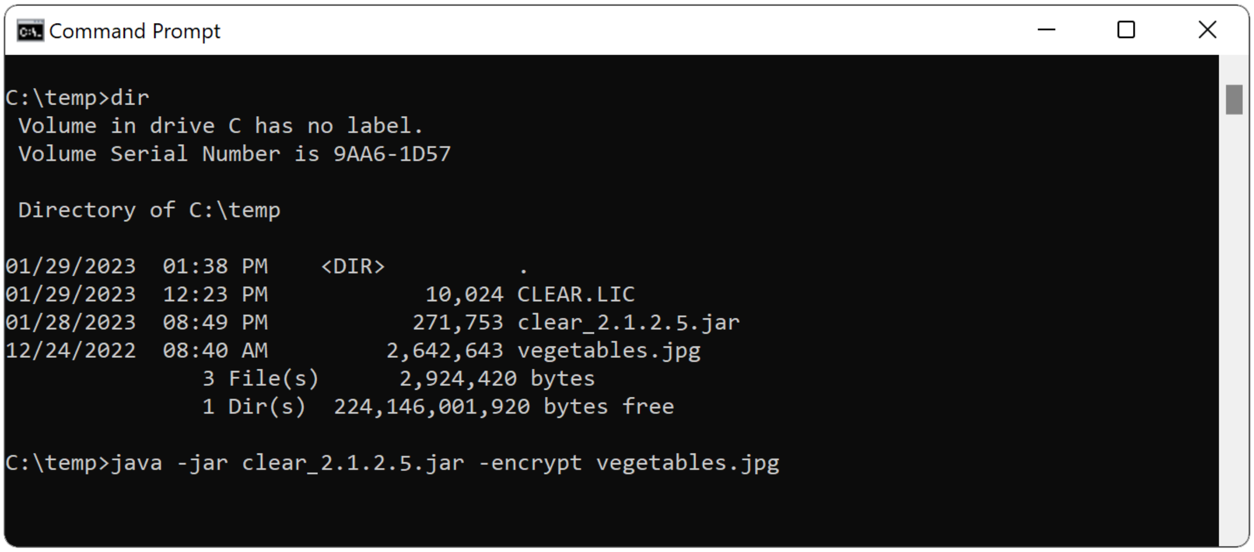
3.1 First Run

The CLEAR JAR File is intended for inclusion into Java source-code libraries; however, it can also be run with local files directly from the Command Line Interface (CLI). As a first test-run, we will begin by staging a test file that we wish to encrypt. Please find a file or data that you would like to test.

Original files are never modified (or harmed) in the process of encryption! Original data / files are treated as **READ-ONLY** by the CLEAR Cryptosystem in 100% of use-cases.

For our example, we are placing the 2.51-megabyte file "**vegetables.jpg**" in the "**c:\temp**" folder on our Windows-11 PC workstation. In the same folder, we have copied the **CLEAR.LIC** and **clear_2.1.2.5.jar** file that were produced on a Mac in the previous session in this document.





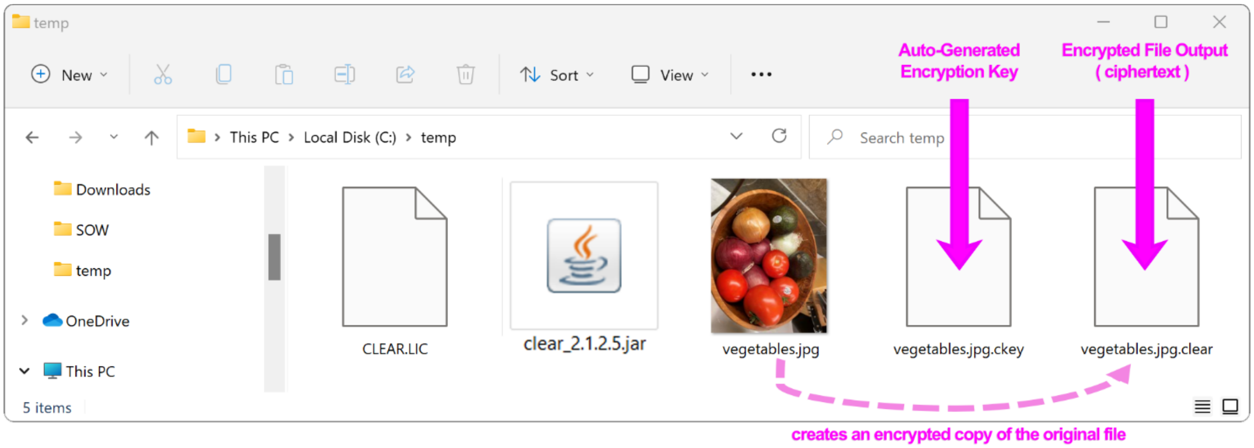
```
C:\temp>dir
 Volume in drive C has no label.
 Volume Serial Number is 9AA6-1D57

 Directory of C:\temp

01/29/2023  01:38 PM    <DIR>          .
01/29/2023  12:23 PM            10,024 CLEAR.LIC
01/28/2023  08:49 PM           271,753 clear_2.1.2.5.jar
12/24/2022  08:40 AM         2,642,643 vegetables.jpg
               3 File(s)      2,924,420 bytes
               1 Dir(s)  224,146,001,920 bytes free

C:\temp>java -jar clear_2.1.2.5.jar -encrypt vegetables.jpg
```

From the c:\temp folder with the CLEAR JAR, we type the following at the CLI:

```
java -jar clear_2.1.2.5.jar -encrypt vegetables.jpg
```

3.2 Examine the Output

Done! We have our first ciphertext. Basic encryption generates two [2] new files in the same folder:—



The first output is the encrypted (ciphertext) of the original file. The ciphertext file is generated automatically with the same filename as the original. The suffix ".clear" is appended to the file type. CLEAR encrypted files can be easily identified as those with the ".clear" files data type.

The second output is the auto-generated encryption key. By default, the CLI encryption job is run at 512-bit strength. Therefore, this key file contains 512 bits of cryptographically secure key-space entropy. The key file can be considered as a "private key" and should be stored carefully. This key file is the only thing that can possibly reverse the ciphertext back into cleartext.

To reverse the operation, move the original file elsewhere and type following command at the CLI:

```
java -jar clear_2.1.2.5.jar -decrypt
  vegetables.jpg.clear vegetables.jpg.ckey
```

The decryption operation requires the following (minimum) three parameters:

- 1. **-decrypt** : The decryption mode of operation
- 2. **vegetables.jpg.clear** : The ciphertext file to be decrypted
- 3. **vegetables.jpg.ckey** : The key file to be used to decrypt the ciphertext

The CLEAR Cryptosystem will always function to decrypt data, even without a license key. For additional information on how to encrypt and decrypt data from the Command Line Interface (CLI), please refer to our "CLI-GUIDE" documentation with further instructions and examples.

3.3 FIPS 140-2/3 Compliance Modes

CLEAR Cryptosystem is pleased to offer FIPS 140-2/3 Compliance modes of operation for special use in the government, financial, and healthcare sectors.

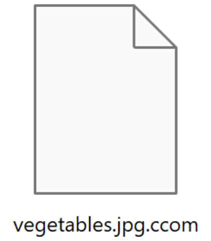
From the Command Line Interface (CLI), CLEAR can be run in FIPS Compliance mode simply by adding the keyword "**-compliance**" to the list of input parameters. For a list of all keywords, parameters, and modes of operation, please see our "CLI-GUIDE" documentation.

```
java -jar clear_2.1.2.5.jar -encrypt ip.jpg -compliance
```

3.3 FIPS Mode – Basic

At this point, we have not installed any other JAR files, modules, or external dependencies to the CLEAR Cryptosystem. Executing the earlier operation with "**-compliance**" causes the generated KEY FILE to be "**post-processed**" after the encipherment step takes place. A "compliant" key is subsequently encrypted (wrapped) with an AES-256 encryption step.

AES-256 wrapped encryption keys implies that decryption cannot take place without first "un-wrapping" the keys via AES-256 decryption. This feature is strong enough to meet FIPS validation standards for many organizations.



(FIPS-Mode Key)

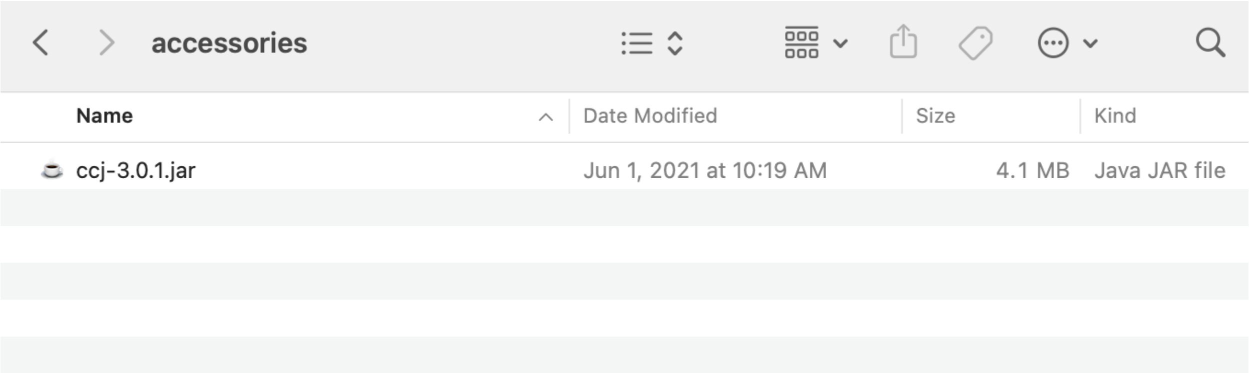
3.4 FIPS Mode - Advanced

Certain use-cases (frequently in government operations) demand ultra-strict adherence to FIPS data exposure. In such circumstances, a bit of data could benefit from the encryption security advantages of 512-bit and greater encryption strength; however, it may be required that the data *also* be encrypted with a recognized FIPS validated algorithm such as AES-256.

A solution to this could be to encrypt data (first with CLEAR for the strength), then subsequently again (re-encrypt) with AES-256 for the compliance. Double-encrypting data can have many disadvantages in terms of data size, encryption performance, and data volume, etc.

CLEAR Cryptosystem addresses the advanced FIPS Compliance use-cases with the inclusion of the US National Institute of Standards and Technology (NIST) recognized Crypto-Compliance (**ccj-3.0.1.jar**) JAR File Accessory, produced and distributed by Safe Logic, Inc, Palo Alto, California, USA.

The CCJ JAR File is included with all distributions of CLEAR in the **/accessories** folder as shown:



Name	Date Modified	Size	Kind
ccj-3.0.1.jar	Jun 1, 2021 at 10:19 AM	4.1 MB	Java JAR file

Figure 4 - NIST Recognized Crypto Compliance "CCJ" JAR – @ see: www.safelogic.com

3.5 Installing Crypto Compliance JAR

Crypto-Compliance CCJ JAR file can be installed in **two [2] ways**, just the same as the CLEAR.LIC file referenced above. Copy the "**ccj-3.0.1.jar**" file into the same folder or classpath as the **clear_n.n.n.n.jar** Java SDK distribution and it will automatically be recognized by CLEAR.

Alternatively, the CCJ JAR file can be referenced by creating a system variable, "CLEAR_COMPLIANCE".

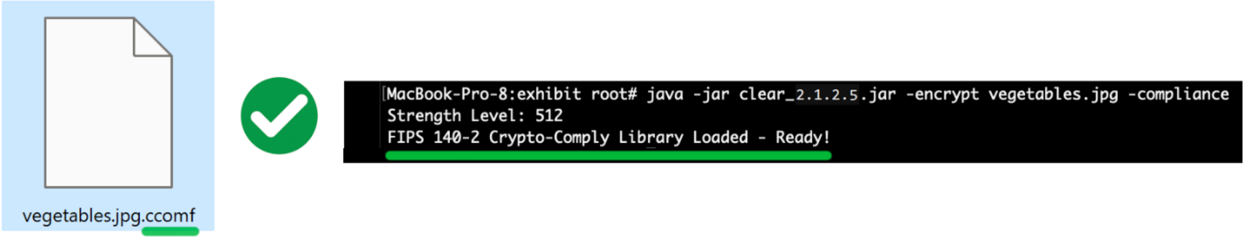
Example Windows:

```
set CLEAR_COMPLIANCE=c:\temp\ccj-3.0.1.jar
```

Example Mac / Linux:

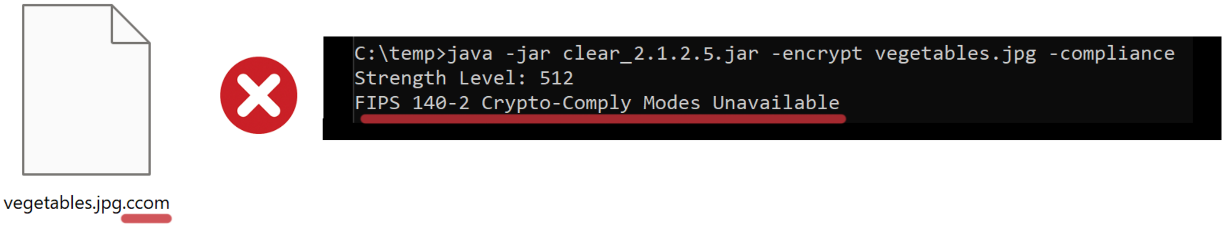
```
export CLEAR_COMPLIANCE=/temp/ccj-3.0.1.jar
```

When the CCJ JAR is successfully recognized, and encryption run in compliance mode of operation, the ciphertext will be AES-256 comingled and the encryption key output files will end with "**.ccomf**".



```
[MacBook-Pro-8:exhibit root# java -jar clear_2.1.2.5.jar -encrypt vegetables.jpg -compliance
Strength Level: 512
FIPS 140-2 Crypto-Comply Library Loaded - Ready!
```

When the CCJ JAR is not found or unavailable, and encryption run in compliance mode of operation, the ciphertext will be naturally CLEAR encrypted and the encryption key output files will end with "**.ccom**".



```
C:\temp>java -jar clear_2.1.2.5.jar -encrypt vegetables.jpg -compliance
Strength Level: 512
FIPS 140-2 Crypto-Comply Modes Unavailable
```

For more information on the mechanics of encryption and CCJ FIPS Compliance comingling of data, please see the white-papers and peer-reviewed Crypt Analysis for CLEAR Cryptosystem.

References

[1] CLEAR Cryptosystem

[2] AES-256

[3] CHACHA-20

[4] One-Time Pad Encryption

[5] Safe Logic, Inc.

[6] Chat GPT

[7] US National Institute of Standards and Technology (NIST)

[8] Quantum Knight, Inc.

[9] Oracle, Inc.

[10] Amazon Corretto

[11] The Open JDK Foundation

[12] The Java Virtual Machine

[13] Edward Rooney

[14] Microsoft Corporation