

COMP 7402 - Assignment 3

Tehrani Parsa, Peyman - A00922386

February 14, 2019

Usage	2
Design	2
Pseudocode	2
Encrpytion	2
Decrpytion	2
Testing	3

Usage

For dependencies: npm install

Usage: index [options]

Options:

- V, --version output the version number
- f, --file <file> File location is relative to JS file
- k, --key <key> Required only when mode is set to decrypting
- c, --cypher <cypher> Required only when mode is set to decrypting
- e, --encrypt [encrypt] encryption mode
- d, --decrypt [decrypt] decrypt mode
- h, --help output usage information

Design

Pseudocode

Encryption

Load input as plain text

Create randomized string of size plain text for key value

XOR plain text and key value to get cypher text

Write key value and cypher text to files

Decryption

Load key value and cypher text

XOR cypher text and key value to get plain text

Write plain text to file

Testing

Test	Print usage
Desired output	./index.js or ./index.js -h
Result	<pre> peymon@CM-Desktop /run/media/peymon/Slow/Code/BTech/7402/asn3 master • ./index.js -h Usage: index [options] Options: -V, --version output the version number -f, --file <file> File location is relative to JS file -k, --key <key> Required only when mode is set to decrypting -c, --cypher <cypher> Required only when mode is set to decrypting -e, --encrypt [encrypt] encryption mode -d, --decrypt [decrypt] decrypt mode -h, --help output usage information </pre>
PASS	

Test	Input file doesn't exist
Desired output	Error with detailed description
Result	<pre> peymon@CM-Desktop /run/media/peymon/Slow/Code/BTech/7402/asn3 master • ./index.js -f na -e Error: Error: ENOENT: no such file or directory, open 'na' at Object.openSync (fs.js:449:3) at Object.readFileSync (fs.js:349:35) at OTP.readFile (/run/media/peymon/Slow/Code/BTech/7402/asn3/OTP.js:58:35) at new OTP (/run/media/peymon/Slow/Code/BTech/7402/asn3/OTP.js:11:29) at Object.<anonymous> (/run/media/peymon/Slow/Code/BTech/7402/asn3/index.js:18:13) at Module._compile (internal/modules/cjs/loader.js:736:30) at Object.Module._extensions..js (internal/modules/cjs/loader.js:747:10) at Module.load (internal/modules/cjs/loader.js:628:32) at tryModuleLoad (internal/modules/cjs/loader.js:568:12) at Function.Module._load (internal/modules/cjs/loader.js:560:3) at /run/media/peymon/Slow/Code/BTech/7402/asn3/OTP.js:14 this.key = this.generateKey(this.msg.length); </pre>
PASS	

Test	Encrypting File
Desired output	Create a file for key and encrypted text
Result	<pre> peymon@CM-Desktop /run/media/peymon/Slow/Code/BTech/7402/asn3 master • head --lines=2 cypher ZchPKmf\EsGS}\%N + EY%30/JK T2{<ID K^^&[\@DTP^YRF2F60VU Z/L-UWsr!\w.0%=P-XHg#+jm;A5x9.Mm4J\$^x22fGR!BF "MIJK m(Y@i7T- BZ@{35B peymon@CM-Desktop /run/media/peymon/Slow/Code/BTech/7402/asn3 master • head --bytes=256 key ->yG^QNg5b2Max. H*. V/l]sFgLyUAY). &];<r&X**v=-j.2#kt3hI(06%9,Gsq!P.;<LkzJ7{Lo4cu85RU4f}lEJss `_,:lI bR_(0b<LHG:o!T_dajeRwExzyd Grb:(0a_oP!1,/x&EJ*Dk10 WdLS)GMVWq peymon@CM-Desktop /run/media/peymon/Slow/Code/BTech/7402/asn3 master • </pre>
PASS	

Test	Decrypt file
Desired output	String matching original file
Result	<pre>peymon@CM-Desktop /run/media/peymon/Slow/Code/BTech/7402/asn3 master • head --lines=2 plain [0#5%&*()_+==] / [;,:]</pre>
PASS	

Test	Unique Encrypting
Desired output	Different sha256sum for the same file
Result	<pre>peymon@CM-Desktop /run/media/peymon/Slow/Code/BTech/7402/asn3 master • sha256sum cypher daaa2c203ea51051af2cfee533b18f5e1b4e0d46503e038b3ca4afbe54233411 cypher peymon@CM-Desktop /run/media/peymon/Slow/Code/BTech/7402/asn3 master • ./index.js -f wap -e cypher saved! key saved! peymon@CM-Desktop /run/media/peymon/Slow/Code/BTech/7402/asn3 master • sha256sum cypher 13763db9e162876111fcade262d91d3b3c920add89c8fe4fbfa54c7b031258e3 cypher peymon@CM-Desktop /run/media/peymon/Slow/Code/BTech/7402/asn3 master • █</pre>
PASS	