**Personal Encryptor Command Line Interface (CLI)**

A basic command line utility to generate private/public key pairs and encrypt/decrypt data without having to know the inner workings of the crypto libraries.

This utility is heavily based on sample code generated by Stephen Haunts[[1]](#footnote-1) during his Practical Cryptography in .NET course[[2]](#footnote-2).

You can read more about my reasoning behind this project in my blog post[[3]](#footnote-3) as well as any [posts relating to its creation and ongoing development[[4]](#footnote-4).

# Using the Utility

## Generate Key Pair

In order to use any encryption system, you will need to generate a Key Pair consisting of a Public and Private key. The public key can be freely distributed but the private key must be protected from loss and unauthorised access.

If you lose your private key then you will not be able to decrypt messages sent to you that were encrypted using the matching private key.

If someone else gains access to your private key then they will be able to read any data you have encrypted with it or data someone has encrypted with your public key (providing they also have access to the corresponding public keys that is).

### Options

|  |  |  |
| --- | --- | --- |
| **Action** | **Options** | **Notes** |
| generatekeys |  | Signals CLI to generate a key pair |
|  | name | The name prefix for the key pair |
|  | keylength | The bit length of the keys to generate, defaults to 2048 |
|  | output | The output path for the keys, if the folder does not exist it will be created |

### Usage

To generate a new Key Pair from the command line:

C:\> PersonalEncryptorCLI generatekeys --name Alice --output C:\Users\Alice\MyKeys

This command will result in a 2048 bit Private/Public Key Pair called AlicePrivateKey.xml and AlicePublicKey.xml being created in C:\Users\Alice\MyKeys

Note that omitting the name option will generate files named PrivateKey.xml and PublicKey.xml

It is highly recommended that the private key be moved to a secure location, separate from the public key.

## Encrypt File

Files are encrypted using the senders PUBLIC key and the recipients PRIVATE key to produce an 'encrypted packet’, which is a text file containing the encrypted data. The file also contains a Digital Signature for validating the files contents during decryption. While this file can be opened in any text editor the contents can only be decrypted using the appropriate keys.

### Options

|  |  |  |
| --- | --- | --- |
| **Action** | **Option** | **Notes** |
| encryptfile |  | Signals CLI to encrypt specified file |
|  | filepath | The full path to the file to be encrypted |
|  | keylength | The bit length of the keys to generate, defaults to 2048 |
|  | senderkeypath | The full path to the sender’s PRIVATE key |
|  | recipientkeypath | The full path to the recipient’s PUBLIC key |
|  | output | The output path (and filename) where the encrypted file will be written to, if the folder does not exist it will be created |

### Usage

To encrypt a file, use the following command (replacing the appropriate paths)

C:\> PersonalEncryptorCLI encryptfile --filepath C:\Users\Alice\MyData\InputFile.pdf --senderkeypath C:\Users\Alice\MyKeys\AlicePrivateKey.xml --recipientkeypath C:\Users\Alice\MyKeys\BobPublicKey.xml --output C:\Users\Alice\MyData\TextFile.json

## Decrypt File

Files are decrypted in the same manner as used for encryption but where the sender’s PRIVATE and recipient’s PUBLIC keys were used to perform the encryption the other key in each pair is now required, i.e. the sender’s PUBLIC and recipient’s PRIVATE keys.

### Options

|  |  |  |
| --- | --- | --- |
| **Action** | **Option** | **Notes** |
| decryptfile |  | Signals CLI to decrypt specified file |
|  | pathtopacket | The full path to the file to be decrypted |
|  | keylength | The bit length of the keys to generate, defaults to 2048 |
|  | senderkeypath | The full path to the sender’s PUBLIC key |
|  | recipientkeypath | The full path to the recipient’s PRIVATE key |
|  | output |  |

### Usage

To decyrpt an 'encrypted packet' JSON file the senders PUBLIC key and recipients PRIVATE key

C:\> PersonalEncryptorCLI decryptfile --pathtopacket C:\Users\Bob\MyData\TextFile.json --senderkeypath C:\Users\Bob\MyKeys\AlicePublicKey.xml --recipientkeypath C:\Users\Bob\MyKeys\BobPrivateKey.xml --output C:\Users\Bob\MyData\OutputFile.pdf

1. <https://stephenhaunts.com> [↑](#footnote-ref-1)
2. <https://app.pluralsight.com/library/courses/practical-cryptography-dotnet/table-of-contents> [↑](#footnote-ref-2)
3. <https://www.onthefencedevelopment.com/whatsapp-a-haven-for-paedophiles-and-terrorists> [↑](#footnote-ref-3)
4. <https://www.onthefencedevelopment.com/tag/personalencryptorcli> [↑](#footnote-ref-4)