InkDeck

Justin Thomas

Version 1.1

Updated March 14, 2018

Table of Contents

Section 1: What is InkDeck?

InkDeck is a program written in Java by Justin Thomas. It was created to implement the features of RSA Encryption learned in a class that semester (Advanced Data Structures and Algorithms). RSA Encryption was discovered by Ron Rivest, Adi Shamir, and Leonard Adleman (the first letters of their surnames make up the RSA name). It is a very secure encryption method.

In order to understand InkDeck, it's important to understand how RSA Encryption works (or at least the basics). I won't go into detail, because it's a difficult to explain, even if you're studying Computer Science (In fact, one could argue that the difficulty to understand RSA is one of the reasons it's secure!). In RSA, you generate a set of keys: public and private. The private key, as you may have guessed, is the one you keep to yourself. The public key, by contrast, is meant to be published. You can give it out to anyone without compromising the security of your encryption. **Remember these principles, you'll be using them!**

It's likely you're not a spy, so why use InkDeck? Well, even if you're not transmitting confidential information, I'm sure you like your privacy. Every free service you use today marks **you** as their product. Data about you is collected every second, from your music tastes, to places you've been, to, you guessed it, the contents of any messages you send. Now, not all companies do this (most do), but if you're transmitting text data to someone, odds are it's been stored somewhere for "unspecified" reasons.

Now consider the many recent cases of tech companies being hacked. Consider the information that's been stolen. Don't think that just because you don't deal "that one" that you're safe. If that company has any connection to the Internet, it's at risk. If you're a high profile individual, you could also be targeted specifically. The tactics would then shift from breaking into a server to breaking into your account.

In short, your data can easily fall into the wrong hands.

That's in large part why InkDeck was created: to provide a backup level of security if your data is compromised. This software may only encrypt textual messages (for now), but that's one more barrier a hacker needs to get through to retrieve information about you.

And in a world like today's, you can't be too safe.

To all who wish to use this software, whether they be a high profile official, a common civilian, or somewhere in between, I offer a word of advice:

"Use it well." – *Harry Potter and the Sorcerer's Stone*

Thank you for choosing this software.

Section 2: How to use InkDeck

This section is broken up into two main parts: a guide to the GUI and how to use the software itself. The GUI guide will show what every button in the software does, while the latter part will explain in detail how to use it. You'll be a master of InkDeck in no time!

A Guide to the GUI

When you first open InkDeck, you'll be greeted with a dialog box asking you to enter in a "codename"
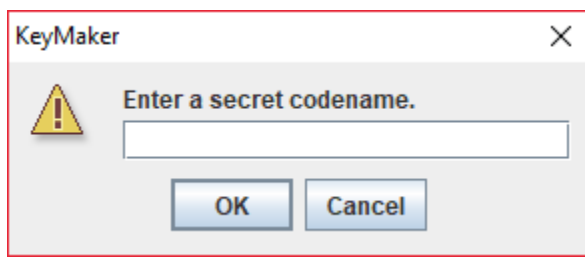

Figure 1 A dialog box instructing you to enter in a "codename".

Enter one in to continue (this will generate a private and public key for you).

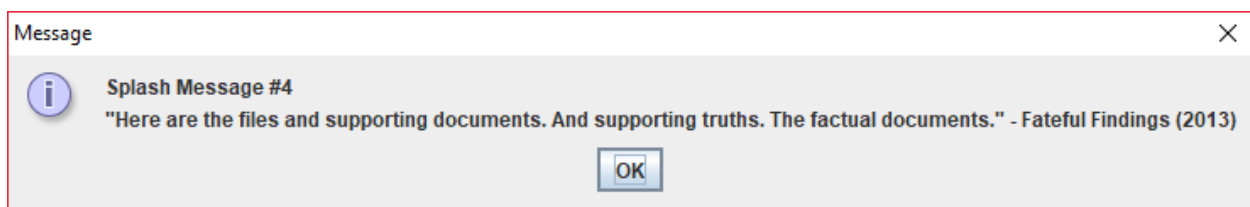Afterwards, you'll be greeted with a random splash message displayed in a dialog box.

Figure 2 A message is displayed when the software is opened.
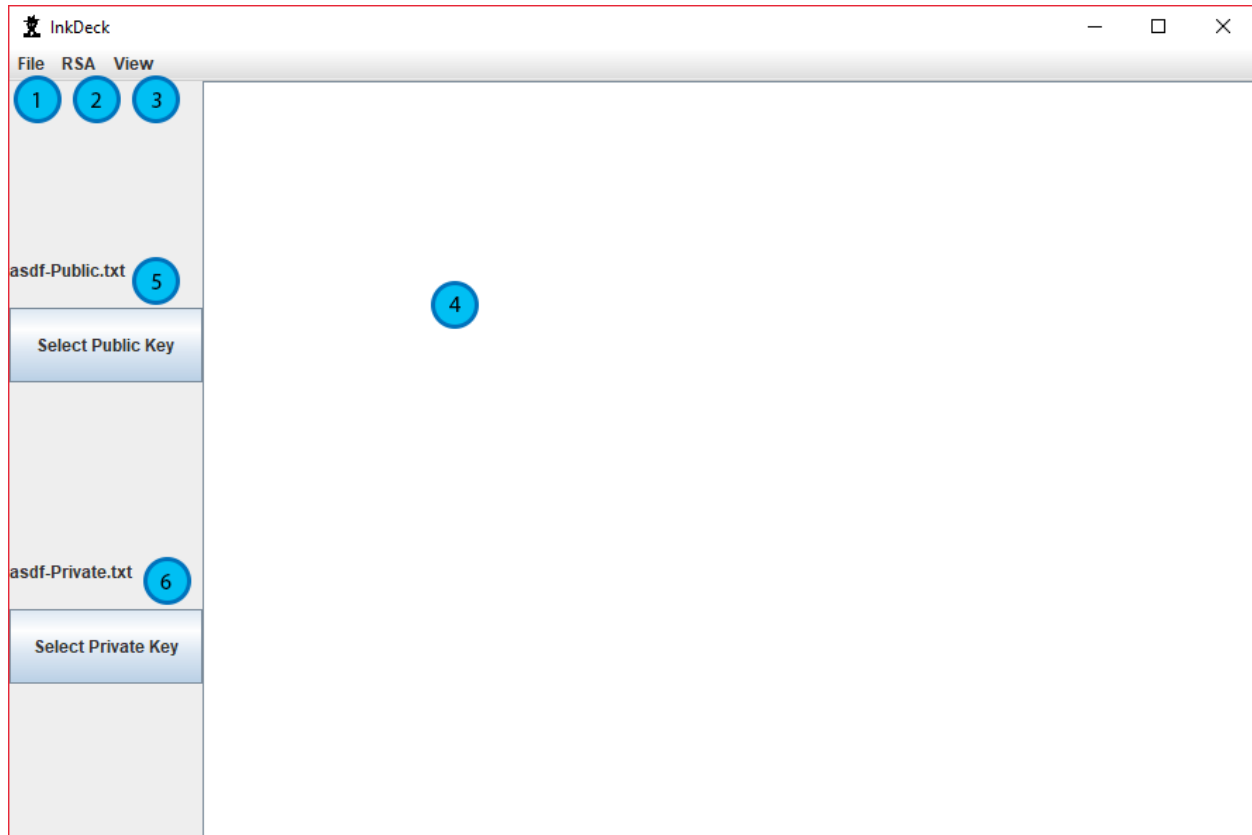
Click OK or the red X in the corner to continue.

Figure 3 The main screen of InkDeck

1) The "File" tab of the menu bar. Explained below.
2) The "RSA" tab of the menu bar. Explained below.
3) The "View" tab of the menu bar. Explained below.
4) The textbox where you enter your message.
5) The "Select Public Key" button with the current Public Key displayed above it. Clicking this button will open a dialog box prompting you to select a Public Key.
6) The "Select Private Key" button with the current Private Key displayed above it. Clicking this button will open a dialog box prompting you to select a Private Key.
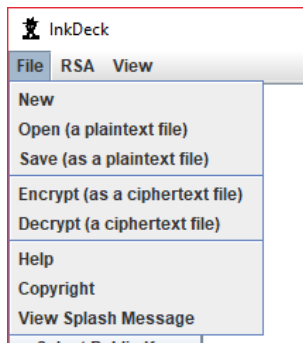
Figure 4 The "File" tab of the menu bar when opened.

New – Clears the textbox.

Open (a plaintext file) – Opens a dialog box prompting you to select a plaintext message.

Save (as a plaintext file) – Opens a dialog box prompting you to select where you'd like the plaintext message to be saved and what name it should have.

Encrypt (as a ciphertext file) – Opens a dialog box prompting you to select where you'd like the encrypted message to be saved and what name it should have.

Decrypt (a ciphertext file) – Opens a dialog box prompting you to select an encrypted message.

Help – Displays a brief message encouraging the user to read the manual.

Copyright – Displays copyright information about InkDeck.

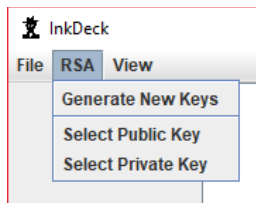View Splash Message – Displays the message shown when InkDeck was opened.

Figure 5 The "RSA" tab of the menu bar when opened.

Generate New Keys – Creates a new Private and Public Key in the same folder as the InkDeck jar (with a title based on the given "codename"). InkDeck automatically sets the current Private Key to the newly generated Private Key.

Note: If you are using InkDeck for the first time, you should experience the same result as clicking this option when InkDeck opens.

Select Public Key – Opens a dialog box prompting you to select a Public Key. (This is the same action as pressing the "Select Public Key" button)

Select Private Key – Opens a dialog box prompting you to select a Private Key. (This is the same action as pressing the "Select Private Key" button)
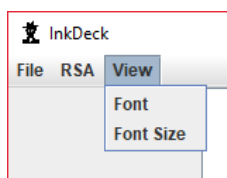

Figure 6 The "View" tab of the menu bar when opened.

Font – Opens a dialog box prompting you to select a font from a dropdown list.

Font – Opens a dialog box prompting you to select a font size from a dropdown list.

Proper Usage (How to be a spy)

1. First, you'll need someone else's public key. Have them send it to you via e-mail or another file sharing service. Send them yours, too (if you're using InkDeck for the first time, you should already have generated your Public and Private Keys when InkDeck opened)! Remember, send your Public Key, **not your Private Key**. By default, both can be found in the same folder where InkDeck is stored.
2. Using the "Select Public Key" button, select the public key of the individual you'd like to send a message to and your own private key (if you just generated new keys, your private key should already be selected).
3. Type out a message in InkDeck. Make it as long or short as you'd like.
4. Click on the menu bar File>Encrypt to open a dialog box. This will ask where you'd like to save the encrypted file and what you'd like to name it.
5. Send the encrypted text file to your recipient of choice via e-mail or another file sharing service.
6. When they send an encrypted text file back, open InkDeck.
7. Click on the menu bar File>Decrypt to open a dialog box. This will ask what file you'd like to open. Select the text file you received.
8. You should see the unencrypted contents of the file displayed in the text area.
9. Repeat steps 3-8 for any messages you send/receive.

Note: Unicode characters, such as ☺, ▣, and … can't be encrypted or decrypted. These will cause the program to crash. Only use ASCII characters in your messages.

Acknowledgements and a Word from the Author

I'd like to thank Southern Utah University and its' professors for not only instructing me not only in the ways of Computer Science, but how to be a lifelong learner. A special thanks goes to Dr. Michael Grady for teaching me the principles of RSA Encryption. Your patience with me as I slowly understood the concept was greatly appreciated.

I'm really quite proud of how this software has grown. It may not look like a professional grade product, but I'm proud of all the features I've put into it. Every time I finished a major release, I thought "you know what would make this even better?", then went off to write another TODO note.

The software is by no means complete. At least, not in my mind. As Open Source software, I believe it's constantly in development. I'd also like to believe it could be a starting point for someone who wants to understand RSA Encryption and Java Programming. The concepts are somewhat advanced, but I hope it can be a resource for at least one dedicated student.

– Justin Thomas

My GitHub account: https://github.com/justinthomas1

Copyright

The image used for the logo of InkDeck was retrieved from https://commons.wikimedia.org/wiki/File:Spy.png

As denoted in the "Licensing" section:

> "This file is made available under the Creative Commons CC0 1.0 Universal Public Domain Dedication.
>
> The person who associated a work with this deed has dedicated the work to the public domain by waiving all of his or her rights to the work worldwide under copyright law…You can copy, modify, distribute and perform the work, even for commercial purposes, all without asking permission."

InkDeck is licensed under the GNU General Public License v3.0. For more information, please see https://www.gnu.org/licenses/gpl-3.0.en.html