A simple introduction to what PassLok does

(This tutorial is loosely based on understanding public key private key concepts, by Blake Smith, and uses some artwork from it)

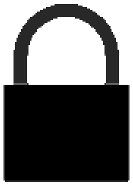
PassLok uses digital Keys and Locks in order to secure your messages and files.

You start with a **master Key**:

Which is actually a piece of text that you can remember so well that you never have to write it down. A good Key contains small case as well as capital letters, numbers, and other characters. When real words are used, it is best to misspell them in non-standard ways. Let's say your master Key is:

I'll eat 42 Bananas

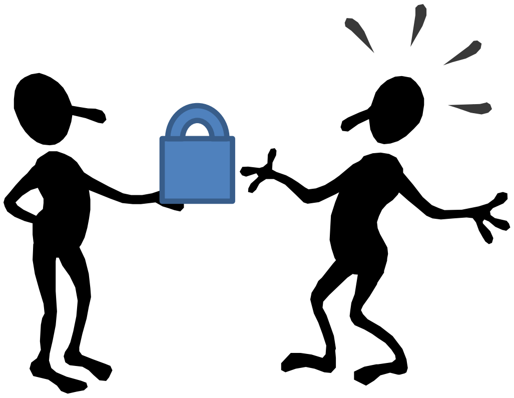
From this master Key, you make a **Lock**:



This is also a piece of text, but it is random-looking except for identifying tags at either end. PassLok makes the Lock for a given Key if you click **Keys**, followed by **master Key**, then write your master Key in that box, and click the **Make Lock** button. This is your Lock:

PL16lok=VVtTCE/pYd2HFwBPMG4VvP+r6UEfvg1cagKYHBH2vLXHPbohF2OyMteT1e0VxcQZSTN8aRDRkFp jg+do6Cnce/z=PL16lok

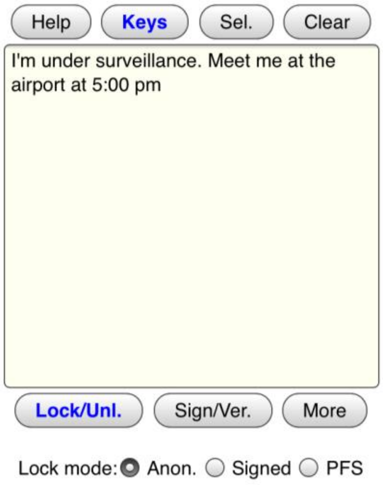
Now you give your Lock to everybody you know. You add it to your email signature. You put it on your business card. You Tweet it left and right. It's not a secret, and people are going to need it in order to communicate with you securely.



For the same reason, you want to obtain all of your friends' Locks. You can store them within PassLok itself, if you want, or anywhere, really.

Because the Lock isn’t secret and nobody can get the Key from the Lock, it doesn’t matter if somebody’s watching and copying everything.

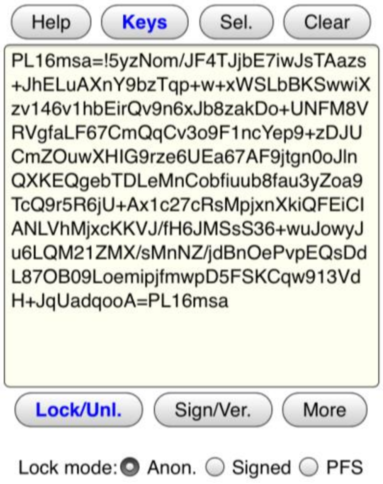
Now that your friend has your Lock and you’ve got his, you can both go to PassLok and use them to lock messages (files too!) that only the person having the matching Key will be able to read. Let’s say your friend wants to tell you something very important, which he writes into PassLok.



I'm under surveillance. Meet me at the airport at 5:00 pm

Lock mode: ● Anon. ○ Signed ○ PFS

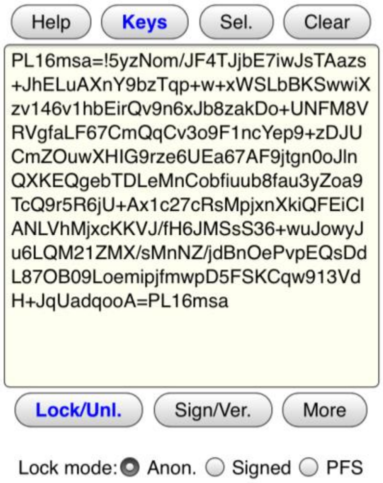
He has selected your Lock in his database (accessed through the **Keys** button), so when he clicks **Lock/Unlock**, this is what PassLok displays:



```
PL16msa=!5yzNom/JF4TJjbE7iwJsTAazs
+JhELuAXnY9bzTqp+w+xWSLbBKSwwiX
zv146v1hbEirQv9n6xJb8zakDo+UNFM8V
RVgfaLF67CmQqCv3o9F1ncYep9+zDJU
CmZOuwXHIG9rze6UEa67AF9jtgn0oJln
QXKEQgebTDLeMnCobfiuub8fau3yZoa9
TcQ9r5R6jU+Ax1c27cRsMpjxnXkiQFEiCl
ANLVhMjxcKKVJ/fH6JMSsS36+wuJowyJ
u6LQM21ZMX/sMnNZ/jdBnOePvpEQsDd
L87OB09LoemipjfmwpD5FSKCqw913Vd
H+JqUadqooA=PL16msa
```

Lock mode: ● Anon. ○ Signed ○ PFS

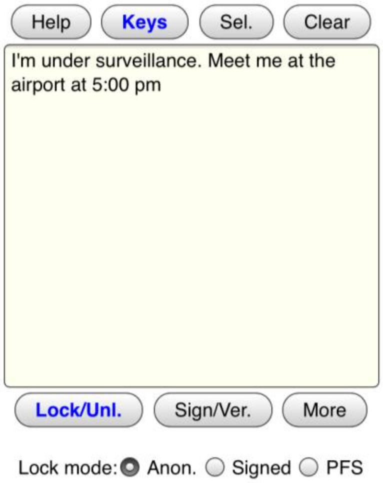
This is an anonymous **locked message**, which he then copies, pastes into his email program, and emails you. Anybody who intercepts it can copy the locked message into the main PassLok window as in the picture, and then click **Lock/Unlock**. But PassLok won’t unlock it unless the right master Key has been entered. Like this:



PL16msa=!5yzNom/JF4TJjbE7iwJsTAazs
+JhELuAXnY9bzTqp+w+xWSLbBKSwwiX
zv146v1hbEirQv9n6xJb8zakDo+UNFM8V
RVgfaLF67CmQqCv3o9F1ncYep9+zDJU
CmZOuwXHIG9rze6UEa67AF9jtgn0oJln
QXKEQgebTDLeMnCobfiuub8fau3yZoa9
TcQ9r5R6jU+Ax1c27cRsMpjxnXkiQFEiCl
ANLVhMjxcKKVJ/fH6JMSsS36+wuJowyJ
u6LQM21ZMX/sMnNZ/jdBnOePvpEQsDd
L87OB09LoemipjfmwpD5FSKCqw913Vd
H+JqUadqooA=PL16msa

Lock mode: ● Anon. ○ Signed ○ PFS

If you did this, PassLok unlocks the message for you to read when you click Lock/Unlock:



I'm under surveillance. Meet me at the airport at 5:00 pm

Lock mode: ● Anon. ○ Signed ○ PFS

Remember that nobody else knows your master Key. Lots of people know your Lock, including those who have placed your friend under surveillance, but they cannot unlock the message because they don't have your Key, and it is impossible to get a Key from its Lock.

So when you reply to your friend, you lock your reply message with his Lock, which he gave you some time before (or could have sent you along with his first message, it really doesn't matter so long as you know it's his for sure). When your friend gets your locked reply, he will unlock it with his master Key (which you don't know, but it doesn't matter), and the loop has been closed. Whoever has placed him under surveillance won't know what you have told each other.