Anleitung zu Open_ProtectYourDataFromGovernment Version 0.01

Inhaltsverzeichnis

Los geht's!

Damit du mit dem Programm umgehen kannst, werden wir beide ein Szenario durchgehen, das mithilfe von Bildern beschrieben wird.
Es gibt also eher wenig Lesearbeit für dich.

Bitte beachte, dass du die Java JVM braucht um das Programm ausführen zu können.
Es könnte sein, dass dieses Programm jedoch schon installiert ist, ohne dass du davon etwas weißt (Das ist bei den meisten Leuten irgendwie der Fall).

Es geht los mit Anna und Arthur.
Weil Anna und Arthur schlaue Köpfe sind, wissen sie, dass sie's Maul halten sollen.
Nicht nur gegenüber der Exekutive oder Geheimdiensten sondern auch in der Öffentlichkeit und vor allem im Internet.
Anna und Arthur wissen, dass bspw. die Vorbereitung einer Demonstration Repression nach sich ziehen kann.
Daher wollen Anna und Arthur jeglichen politischen Austausch über ein verschlüsseltes Medium absichern.

Schritt 1:
Anna möchte Arthur mitteilen, dass die Polizei in Bayern bald die Befugnisse dazu hat Handgranaten tragen zu dürfen und Personen ohne anwaltlichen Beistand bis zu drei Monate einzusperren.
Außerdem möchte sie gegen diese Befugnisse gerne demonstrieren gehen.

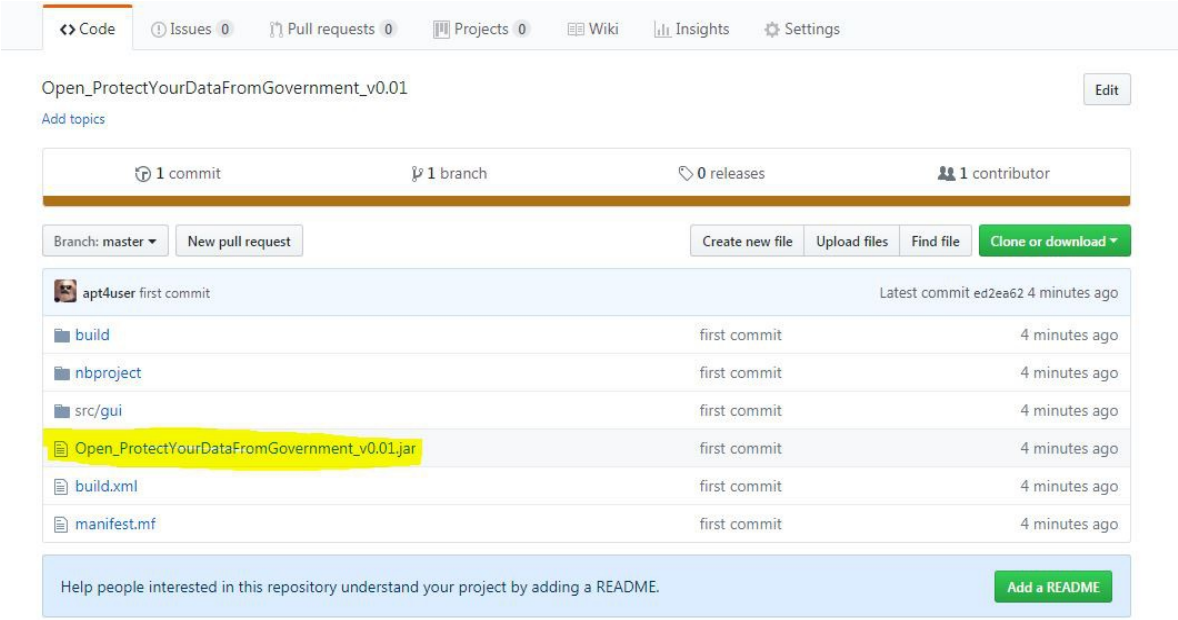
Anna muss sich also ein Verschlüsselungsprogramm downloaden um mit Arthur darüber kommunizieren zu können.

Downloadlink zu Open_ProtectYourDataFromGovernment_v0.01:
https://github.com/apt4user/Open_ProtectYourDataFromGovernment_v0.01

Anmerkung: Es gibt einige Offline-Programme um Daten zu verschlüsseln.
Aber nahezu keines ist für Nutzer brauchbar, die sich nicht mit der Thematik der Verschlüsselung befassen. Daher habe ich das Programm (ich hoffe aus dem „ich" wird bald ein „wir"!) programmiert, damit Menschen ohne Vorkenntnisse trotzdem Nachrichten verschlüsselt versenden können.

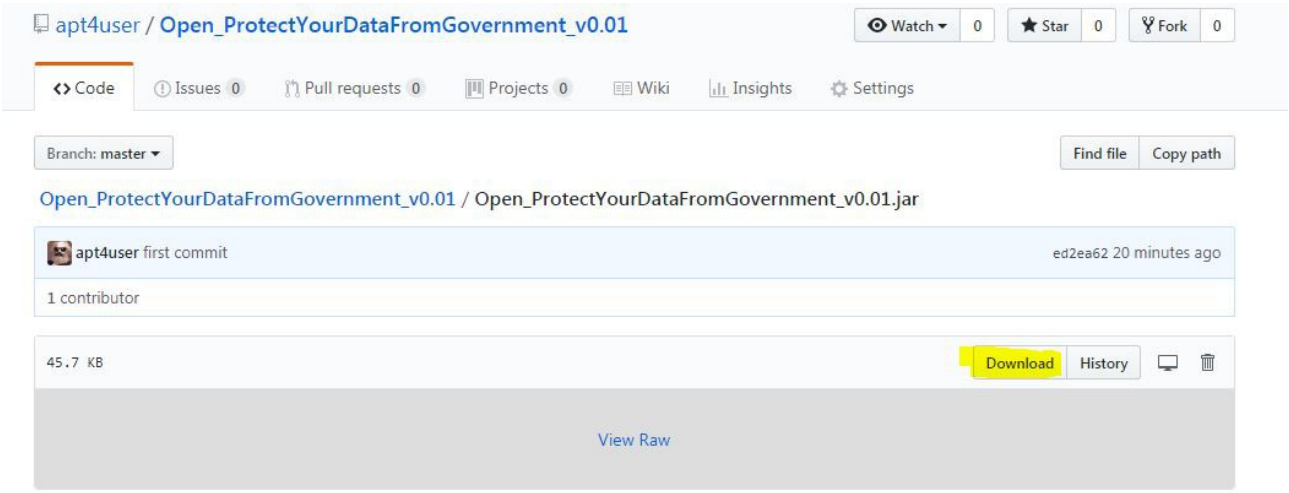
Da sich diese Anleitung auch primär an Personen richtet, die keine/ wenige Vorkenntnisse besitzen, stehen aus diesem Grund die technischen Daten eher an letzter Stelle (Nach den How-tos).

- Anna besucht also die oben angegebene Seite wie im beigefügten Bild auf Seite 3 veranschaulicht.

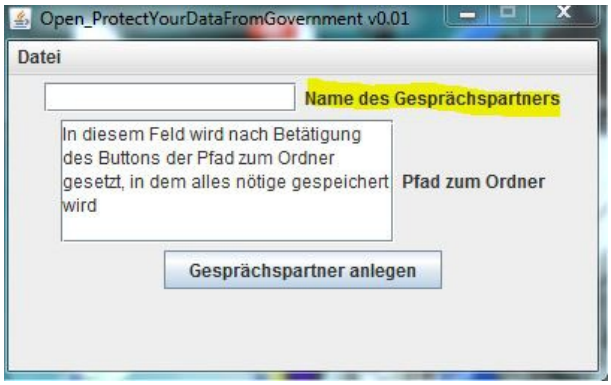


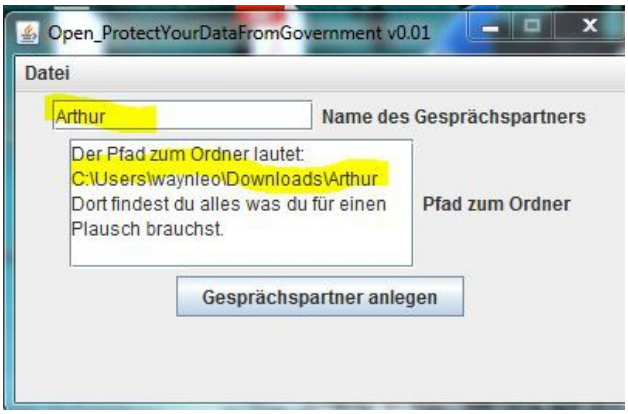
Schritt 1.1: Anna klickt auf das Programm „Open_ProtectYourDataFromGovernment_v0.01“, welches im Bild zur besseren Orientierung gelb hinterlegt ist.

Schritt 1.2: Anschließend drück Anna auf den Download-Button, der im unteren Bild zur besseren Orientierung gelb hinterlegt ist.



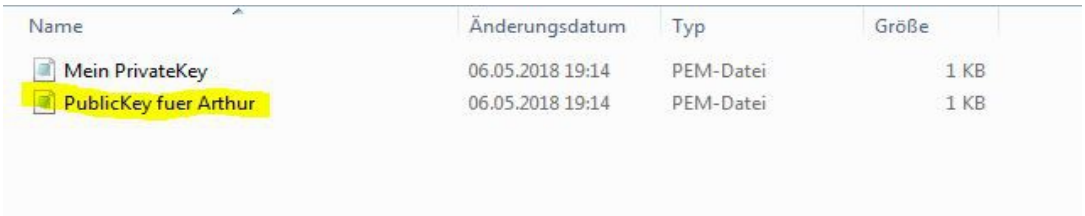
Schritt 1.3: Anna öffnet das Programm durch doppelklick.
Im Anschluss öffnet sich ein Fenster.
Hier muss Anna nun den Namen „Arthur“ im Feld „Name des Gesprächspartners“ eingeben.
Kurzes technisches Detail: Die Eingabe des Namens bewirkt, dass ein Ordner erstellt wird und die Dateien auch Bezug auf den Namen des Gesprächpartner nehmen.





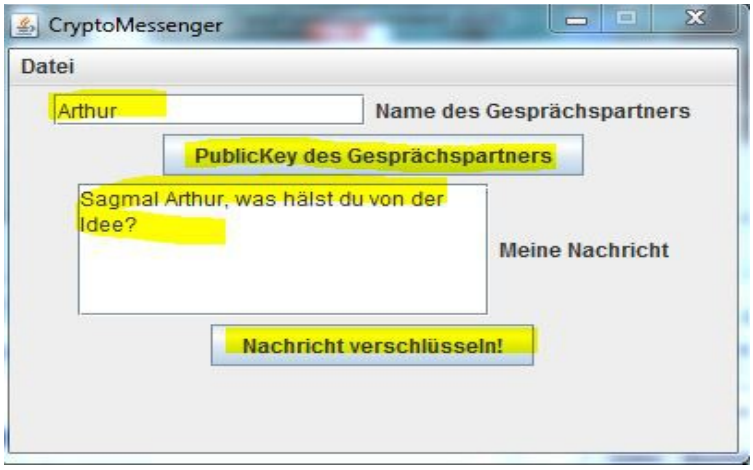
Es wurde somit ein Ordner erstellt, der den Namen des Gesprächspartners trägt.
Also „Arthur“.
Der Ordner wird immer an dem Ort angelegt, an dem ihr auch das Programm untergebracht hat.
In Anna's Fall wäre dies der „Download-Ordner“.

Schritt 1.4: Damit Anna mit Arthur Kontakt aufnehmen kann, braucht Arthur den Annas PublicKey.
Diesen findet Anna im Ordner „Arthur“.
Anna muss den PublicKey nun also an Arthur schicken. Bspw. Über einen Chat, E-Mail etc.



Arthur braucht also die komplette Datei, damit Anna mit ihm (oder er mit ihr), kommunizieren kann.
Um das zu gewährleisten muss auch Arthur die selben Schritte gehen, die Anna gegangen ist.
Demzufolge muss auch Arthur der Anna einen PublicKey zusenden.
Im Feld „Name des Gesprächpartners“ wählt sie wieder den Namen Arthur.
Anschließend muss Anna auf den Button „PublicKey des Gesprächpartners“ klicken.
Nun sucht sie sich den PublicKey den sie von Arthur bekommen hat und wählt diesen aus.
Anmerkung: Bitte beachte, dass in dem GUI-Design noch keine „Auswählbestätigung“ implementiert wurde. D.h., dass unabhängig davon ob eine Datei ausgewählt wurde oder nicht, keine Bestätigung oder Fehlermeldung darüber im Fenster angezeigt wird.

Solltest du dir unsicher darüber sein ob du die richtige Datei erwischt hast, dann klicke einfach nochmal auf den Button und wähle die Datei aus.
Sollte eine falsche Datei ausgewählt werden, wird die Nachricht entweder nicht oder falsch verschlüsselt bzw. man erhält eine leere Datei.



Schritt 1.5: Anna verschlüsselt nun mit Arthurs PublicKey die erste Nachricht, in dem sie in die Menüleiste auf „Datei“ geht und „Eine Nachricht verschlüsseln“ anklickt.

Wir halten also bis hier hin Fest:
1: Zuerst gibt Anna den Namen „Arthur“ in das Textfeld ein.
2: Dann wählt sie den PublicKey, den sie von Arthur bekommen hat.
Dieser heißt „PublicKey fuer Anna“
3: Anschließend gibt sie den zu verschlüsselnden Text ein.
4: Im Anschluss drück sie den Button „Nachricht verschlüsseln!“

Schritt 1.5: Die Nachricht ist verschlüsselt!
Die Nachricht kann nun Arthur an Arthur versendet werden.
Damit Arthur die Nachricht entschlüsseln kann muss Anna in den Ordner „Arthur“ gehen und die 4 Dateien:

- „IV fuer Arthur“
- „Nachricht fuer Arthur“
- „SecretKey fuer Arthur“
- „Nachricht fuer Arthur“

an Arthur senden (Wieder geht dies über ein Chat, E-Mail, Whatsapp etc.)

Schritt 1.6: Arthur hat Anna auf die Nachricht geantwortet.
Damit Anna nun die Nachricht entschlüsseln kann, braucht sie die Dateien:

- „IV fuer Anna“
- Nachricht für Anna
- „SecretKey fuer Anna“
- „Nachricht fuer Anna“

von Arthur.
Hat sie die Daten erhalten, startet Anna -sofern nicht vorher geschlossen - das Programm „Open_ProtectYourDataFromGovernment_v0.01“ .
Anschließend klickt sie in der Menübar wieder auf „Datei“ und dann auf die Rubrik „Eine Nachricht entschlüsseln“.

Dort sind einige Buttons, über die man die Benötigten Dateien auswählen muss.

Die Datei „Mein PrivateKey“ liegt im Ordner „Arthur“. Es ist Annas PrivateKey, mit dem Sie die Nachrichten entschlüsseln kann.
Danach braucht Sie:

- „IV fuer Anna“
- „SecretKey fuer Anna“.

Und: „Nachricht des Gesprächpartners“ Also die Datei „Nachricht fuer Anna“

Nun kann Anna die Antwort lesen:

Zum Projekt selber

Datensicherheit ist heute wichtiger denn je.
Es sollte ein Warnschuss für alle sein, dass die bayerische Polizei Befugnisse erhält, Personen ohne Tatverdacht 3 Monate wegsperren zu dürfen.
Mit diesem Programm möchte ich Personen helfen und ermutigen, ihre Meinung auch weiterhin kundzutun.
Ferner ist dieses Programm für jeden bestimmt, der einfach nur Nachrichten mit seinen Freunden/ Freundinnen verschlüsselt teilen will.

Mehr Infos über das PAG in Bayern findet ihr bspw. auf:
https://www.heise.de/tp/features/Bayerische-Polizei-darf-kuenftig-auch-ohne-Verdacht-auf-konkrete-Straftaten-im-Internet-ermitteln-4005287.html
https://www.heise.de/newsticker/meldung/Experten-kritisieren-massiv-geplante-bayerische-Polizeirechtsreform-4001651.html
https://www.heise.de/newsticker/meldung/Gruene-legen-Verfassungsbeschwerde-gegen-bayerisches-Gefaehrdergesetz-ein-4008119.html
https://www.heise.de/newsticker/meldung/Buntes-Buendnis-warnt-vor-Bayerischem-Praeventionsstaat-4028708.html

Ein paar technische Details.

Verschlüsselt wird nach dem PGP-Mechanismus.
Ein RSA-Key beträgt 128 Byte.
Verschlüsselt wird dann letztlich mit RSA und AES.
Der AES-Schlüssel wird über einen RSA-Algorithmus verschlüsselt, der im Betriebsmodi „ECB“ instanziert wird.
Ferner wird mit PKCS#1Padding verschlüsselt.

ECB ist für Verschlüsselungen von einzelnen Schlüsseln mehr als ausreichend,
da sich durch den AES-Schlüssel keine statistischen Werte auf die Verschlüsselung selber ergeben.

Die AES-Verschlüsselung geschieht im Betriebsmodi CTR.
CTR , aus diesem Grund, weil sich dieser Betriebsmodi als sehr sicher erweist.

Die RSA-Schlüssel werden serialisiert in eine Datei geschrieben.
Das sieht zwar nicht schön aus, jedoch bedarf es noch etwas an Arbeit, wenn man mit KeySpecs arbeiten möchte.
Im nächsten Update werde ich also mein Hauptaugenmerk auf RSAPublicKeySpec und RSAPriavteKeySpec legen, um lediglich den Algorithmus zu „extrahieren“.

Wie geht’s in Zukunft weiter?

Ich werde versuchen alle 2 Wochen ein Update rauszubringen.
Jedoch spätestens alle 4 Wochen.

OpenSource heißt: Mitmachen!
Daher bitte ich dieses Programm zu verbreiten, damit viele Leute an dem Programm arbeiten und mitwirken können.