

# kybernetiq

AUSGABE 1  
RABI' AL-AWWAL 1437  
DEZEMBER 2015

**„Wir töten auf  
Basis von  
Metadaten.“**

Daten sicher vor  
Geheimdiensten  
und Militär  
verschlüsseln!

Fältstarke  
Verschlüsselung  
unter das  
Waffengesetz?

Alternativen zu  
WhatsApp und  
Telegram

*„Finger weg  
von Asrar2!“*

Werde zum  
Albtraum der  
Geheimdienste!

GnuPG Schritt für  
Schritt Anleitung

# Ky·ber·ne·tik

[.kybə'ne:tɪk]

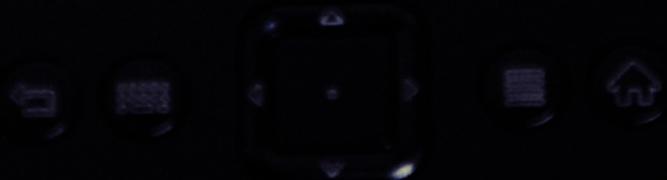
- 1.) **Kybernetik** für Wissenschaft von den dynamischen, selbstregulierenden Systemen (in Natur und Technik).

griech. kybernētikós (κυβερνητικός)  
'zum Steuern gehörig, geeignet'

kybernētiké téchnē (κυβερνητική τέχνη)  
'Steuermannskunst'

abgeleitet kybernán (κυβερνᾶν)  
'steuern, leiten, regieren'

- 2.) **Kybernetiq** das deutschsprachige Magazin mit den Schwerpunkten Informationstechnologie, Telekommunikation und Sicherheit.



# VORWORT

## KYBERNETIQ

das erste deutschsprachige Magazin von Mudschahidin mit den Schwerpunkten Informationstechnologie, Kommunikation und Sicherheit.

Es ist uns sehr wichtig, dass unsere Glaubensgeschwister den richtigen Umgang mit Software und Hardware erlernen. Einst hat das Abendland den technologischen und wissenschaftlichen Fortschritt des Orients beneidet und zugleich hat die Elite der Ungläubigen es als Teufelswerk verbannt.

Zu unserem Nachteil ist es heutzutage umgekehrt. Wir Muslime finden uns in der Rolle der Rückständigen wieder, während dazu geneigt wird, die Fortschritte der Ungläubigen zu verteufeln.

Es ist von enormer Wichtigkeit den verantwortungsbewussten Umgang mit der Technik zu erlernen und richtig anzuwenden.

In den kommenden Ausgaben wollen wir uns zudem die Zeit nehmen, um aktuelle Ereignisse zu kommentieren. Des Weiteren sollen Anleitungen verfasst werden, welche weniger erfahrenen Benutzern leicht und verständlich Software und Hardware näher bringen.

Da wir unter immensem Zeitdruck stehen können wir nicht allzuviel Energie in das Design stecken. Wir bevorzugen es, dass der Inhalt der ersten Ausgaben qualitativ höher ist. In den späteren Ausgaben kann man sich verstärkt auf das Design konzentrieren. Die Entwürfe liegen bereits seit 2014 vor. Zwischenzeitlich musste vieles umgeschrieben werden.

Auf das Veröffentlichen und Verbreiten dieser wichtigen Informationen freuen wir uns sehr und begrüßen jedes Übersetzen unserer Texte in verschiedene Sprachen. Jedwede Kritik seitens der Leser ist eine Bereicherung. Wir hoffen, dass das Informationsmaterial auch auf weiteren Netzwerken von den Lesern verteilt wird.

Und jeder Erfolg ist allein von Allah. Alles Lob gebührt Allah, dem König der Könige.



## INHALTSVERZEICHNIS

### 4 DIGITAL GEBRANDMARKT »Asrar al Mujahideen« unter der Lupe

### 5 BEWEGE DICH UNTER DEM RADAR "Wir töten auf Basis von Metadaten"

### 7 ALTERNATIVE MÖGLICHKEITEN Das Katz- und Mausspiel

### 8 ALBTRAUM ALLER GEHEIMDIENSTE GnuPG Schritt für Schritt Anleitung

### 13 PROLOG "DIE EINHEIT" Islamischer Sci-Fi Roman

TEMPORÄRE KONTAKTMÖGLICHKEIT  
UND ÖFFENTLICHER SCHLÜSSEL AUF  
DER LETZTEN SEITE DES MAGAZINS

ACHTUNG: DIESES DOKUMENT ENTHÄLT KLICKBARE HYPERLINKS.  
UNBEDACHTES KLICKEN UND AUFRUFEN DER WEBSITES  
KANN DAZU FÖRDERN DEINE IDENTITÄT ZU ENTARNEN!

# DIGITAL GEBRANDMARKT

## »Asrar al Mujahideen« unter der Lupe

**Das unbedachte Verwenden von spezifischer Software kann deine Identität enttarnen. Software mit schwachen oder gebrochenen Verschlüsselungsalgorithmen können dir das falsche Gefühl von Sicherheit vermitteln. Verhalte dich unauffällig und operiere unter dem Radar.**

von iMujahid

Als Bruder im Islam fühle ich mich gegenüber euch verpflichtet im Post-Snowden<sup>1</sup> Zeitalter, dringend davon abzuraten, Krypto-Programme mit einem *Mujahid Branding*<sup>2</sup> zu benutzen. Dazu gehören Programme wie *Mujahideen Secrets*<sup>3</sup>, *Amn al-Mujahid*, *Asrar al-Ghurabaa* und diverse mobile Anwendungen.

Versteht mich nicht falsch, ich bin davon überzeugt, dass diese Geschwister zur Gewährleistung der Sicherheit der Ummah, eigene Krypto-Programme schrieben. Schließlich müssen Muslime ebenfalls Werkzeuge und Mittel haben, um sich innerhalb und außerhalb des Internets relativ sicher bewegen zu können. Jedoch weisen die oben aufgezählten Programme Schwachstellen auf, die einige Angriffsflächen darstellen.

Begründen will ich meine Erkenntnis anhand einiger Schwachpunkte im Programm *Asrar al Mujahideen*. Die erste Version hiervon wurde 2007 von GIMF veröffentlicht. Leider konnte ich bis jetzt keine Kopie auftreiben um das Programm näher zu analysieren.

Erst 2008 kam dann der Durchbruch mit *Asrar al Mujahideen 2* oder auch kurz *Asrar2* genannt. Es wurde in der ersten Ausgabe des *Inspire Magazin* vorgestellt und empfohlen. Auch findet man auf den letzten Seiten des Magazins Kontaktmöglichkeiten und den dazugehörigen

öffentlichen Schlüssel. (Inzwischen wurde es aus Sicherheitsgründen wieder entfernt.)

Mit Asrar2 wurde nicht das Rad neu erfunden, sondern auf ein schon bestehendes Verfahren aufgebaut. Die Idee der asymmetrischen<sup>4</sup> Verschlüsselung, wie es in Asrar2 angewendet wird, ist den meisten von euch wohl unter dem Namen *Pretty Good Privacy*<sup>5</sup> oder kurz *PGP* bekannt. Im Gegensatz zur symmetrischen<sup>4</sup> Verschlüsselung, wo beide Gesprächspartner ein und den selben Schlüssel (Passwort) benutzen, basiert die asymmetrische Verschlüsselung auf dem Prinzip des öffentlichen und privaten Schlüssel, auch geheimer Schlüssel, genannt.

Den letzteren bewahrt man an einem sicheren Ort auf und sollte ihn zusätzlich mit einer Passphrase verschlüsseln. Den öffentlichen Schlüssel hingegen kann man auf diversen Plattformen oder Keyservern verteilen oder Kontaktpartnern zuschicken. Diese können mittels dem öffentlichen Schlüssels Dateien und Nachrichten verschlüsseln, sodass nur

der Besitzer des privaten Schlüssels die Informationen wieder entschlüsseln kann.

Soweit so gut. Doch leider ist die Software seit 2008 nicht mehr aktualisiert worden. Das Design ist schlecht und nicht mehr zeitgemäß. Viele kleine Fehler kommen in der Benutzeroberfläche zum Vorschein. Die verwendeten Algorithmen für die Verschlüsselung sind inzwischen gebrochen oder stark abgeschwächt worden, was eines der größten Probleme darstellt.

Wie *PGP* oder *GnuPG*<sup>6</sup>, verwendet auch Asrar2 die bekannten und bewährten Algorithmen wie RSA 2048, AES 256, RC6 256, Mars 256, Serpent 256 und Twofish 256. Wie ihr seht, wurde auch in dieser Hinsicht nichts Weltbewegendes programmiert.

Keiner der Geschwister sollte sich anmuten, eigene Kryptographie Algorithmen zu schreiben. Dieses Fach benötigt tiefes Expertenwissen und ohne hohe Mathematikkenntnisse sollte man die Finger davon lassen. Für erfahrene Programmierer gilt das Benutzen der bekannten Krypto-Bibliotheken und das Durchlesen der dazugehörigen Dokumentationen. Sogar dort könnte man bei der Implementierung Fehler begehen, die später Geschwister in Schwierigkeiten bringen könnten.

### GLOSSAR UND FUSSNOTEN

1. Die Zeit nach den NSA-Enthüllungen. Benannt nach dem ehemaligen Agenten und Whistleblower Edward Joseph Snowden
2. engl.: *branding*, to brand: mit einem Warenzeichen versehen; mit dem Brandeisen kennzeichnen
3. *Asrar al Mujahideen* auch *Mujahideen Secrets* oder *Asrar2* genannt
4. Ein *asymmetrisches Kryptosystem* oder *Public-Key-Kryptosystem* ist ein kryptographisches Verfahren, bei dem im Gegensatz zu einem *symmetrischen Kryptosystem* die kommunizierenden Parteien keinen gemeinsamen geheimen Schlüssel zu kennen brauchen.
5. PGP ist ein von Phil Zimmermann entwickeltes Programm zur Verschlüsselung und zum

- Unterschreiben von Daten. Nähere Informationen siehe Seite 7
6. GnuPG (PGP / GNU Privacy Guard) ist das quelloffene Pendant zu PGP und verwendet ausschließlich nur patentfreie Algorithmen. Kostenlos erhältlich unter [www.gnupg.org](http://www.gnupg.org)
7. Auch proprietäre Software genannt. Quellcode des Programms gehört zum Betriebsgeheimnis. Einstieg durch Dritte ist nicht möglich.
8. Gelöschte Dateien können mit spezieller Software (Recovery) wiederhergestellt werden. File-Shredder überschreibt Dateien mit (Pseudo)zufälligen Daten(müll) und vernichten sie unwiderruflich. <https://de.wikipedia.org/wiki/Datenvernichtung>

Zusammengefasst haben wir ein *Closed-Source*<sup>7</sup> Programm, das neben einer *File-Shredder*<sup>8</sup> Funktion und Datenverschlüsselung nichts

besonderes vorweist, was andere Programme nicht schon können.

Dazu kommt das Einsetzen von veralteten RSA Schlüssellängen von 2048 Bit ohne Ablaufdatum<sup>9</sup>. Empfehlenswert wäre aber ein 4096 Bit Schlüssel mit einem Verfallsdatum von weniger als fünf Jahren, was allerdings in Asrar2 nicht möglich ist.

## Schlüsseldienst erforderlich

Wer ein Antivirusprogramm auf seinem Rechner installiert hat, wird feststellen, dass durch das Öffnen von *Asrar\_2.exe* eine Warnung<sup>10</sup> eingeblendet wird. Auf diese Warnung gehe ich nicht weiter ein.

Falls nicht vorhanden, wird nach dem Start des Programms die Datei, *AsrarKeys.db*, erstellt.

Unter dem Menü *Keys Manager* kann man sich ein Schlüsselpaar generieren. Nun erstellt Asrar2 zwei Dateien mit den Endungen *.akf*. Wahlweise eins für den privaten und eins für den öffentlichen Schlüssel. Anschließend werden die beiden Schlüssel mit dem *Keys Manager* importiert. Folgend wird die *AsrarKey.db* mit dem privaten und öffentlichen Schlüssel, sowie weiteren Informationen wie Benutzernamen, Fingerprint<sup>11</sup>, Schlüssellänge und Erstelltdatum, ergänzt.

Wenn die *.akf* Dateien im *Keys Manager* importiert

**“Wir töten auf Basis von Metadaten.”**

— Michael V. Hayden, Ex-CIA/NSA-Chef

und der private Schlüssel wiederum exportiert wird, stimmen im Anschluss darauf die beiden privaten Schlüssel nicht mehr überein. Sie sind überraschenderweise nicht mehr identisch. Die Key-IDs und Fingerprints sind verschieden.

Anhand der Prüfsumme<sup>12</sup> erkennt man, dass der Inhalt sich geändert hat. Die SHA-Prüfsummen sind folgende:

```
512e616d8fed6927499abe297a5c21f2e5334f16 Private835490F9.akf
e07f6062f8b7288710952f97b4f4720deb733467 Private835490F9-PRI.akf
```

Auch die öffentlichen Schlüssel bringen mich zum Nachdenken:

```
921054e97d0503ef0cd0b22d29765538a3665952 Public2C17D22F.akf
820b159204eaef91171934e8090b9ce84402553e9 Public2C17D22F-PUB.akf
820b159204eaef91171934e8090b9ce84402553e9 Public835490F9-PRI.akf
```

Das Exportieren und (wieder) Importieren der (identischen) öffentlichen und privaten Schlüssel im *Keys Manager* verlaufen nicht fehlerfrei ab. Vielleicht liege ich auch falsch und jemand hat eine logische Erklärung, weshalb die Fingerprints

in der *AsrarKeys.db* nicht mehr überein stimmen. (Siehe Abbildung 1.)

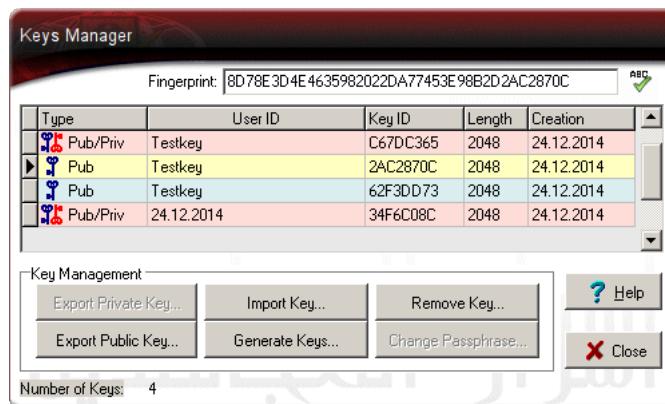


Abbildung 1. Beim nochmaliger Importierung werden verschiedene Key IDs angezeigt und beim Importieren des Schlüsselpaares wird das Erstelltdatum statt des User ID angezeigt.

## Bewege dich unter dem Radar

Das fatalste aller Probleme ist, dass das ganze Konzept unsicher ist. Ein frei verfügbares Programm, welches überwiegend durch Verdächtige und gesuchte Terroristen benutzt wird. Und schon ist man „gebrandmarkt“ mit einem Stempel auf der Stirn/Nacken mit der Aufschrift: „Geheimdienste seht her, ich benutze ein Dschihadisten Verschlüsselungsprogramm!“.

Konspirative Maßnahmen sollten so aussehen, dass den Überwachern erst gar nicht auffällt,

dass man ein potenzieller Terrorist ist. Mit den Enthüllungen Edward Snowdens sollte spätestens jetzt jedem klar werden, welch enormer Aufwand betrieben wird, um die Menschen zu überwachen.

## Proof-of-concept

Es stellt heutzutage wirklich keine große Herausforderung dar, das Internet mit Filtern zu analysieren. Wenn du die Linux Distribution *Ubuntu*<sup>13</sup> benutzt (sollte auch mit jeder anderen Linux Distribution funktionieren), kannst du selber folgendes ausprobieren. Voraussetzungen wären:

- Grundkenntnisse in *Linux*
- Lokaler Webserver und/oder
- Lokaler Emailserver
- *ngrep* Software

Starte mit dem Tastenkürzel **STRG+ALT+T** ein Terminal und installiere dir *ngrep* mit folgenden Befehl (Administrator Recht erforderlich).

```
sudo apt-get install ngrep
```

Nun gebe folgendes Kommando im Terminal ein:

```
sudo ngrep "Ekhlaas|ASRAR" -W byline port 80 or 25 -d 10
```

## GLOSSAR UND FUSSNOTEN

9. Nach Ablauf des Datums wird der PGP-Schlüssel für ungültig erklärt. Höhere Sicherheit.
10. Diverse AV-Hersteller auf [VirusTotal.com](http://VirusTotal.com) erkennen *Asrar\_2.exe* als Schadsoftware. Einige Geschwister sind der Meinung, dies wäre nur zur Einschüchterung und Verunsicherung durch die Ungläubigen.
11. Ein nahezu eindeutiger digitaler Fingerabdruck.
12. Kryptographische Prüfsummen werden eingesetzt, um die Echtheit einer Datei zu verifizieren.
13. Ubuntu kann kostenlos unter [www.ubuntu.com](http://www.ubuntu.com) oder [wiki.ubuntuusers.de](http://wiki.ubuntuusers.de) heruntergeladen werden. (kein HTTPS)

14. Um die Echtheit zu beglaubigen können Nachrichten oder Dateien digital signiert werden.
15. Auf dem Webserver sollte eine Webseite mit einem Kontaktmail oder Kommentarformular vorhanden sein. Andernfalls kann man sich auch per Telnet an den jeweiligen Port verbinden und direkt die Nachricht abschicken.
16. Durch das Senden von gefälschten ARP-Paketen wird die ARP-Tabellen in einem Netzwerk so verändert, dass anschließend der Datenverkehr zwischen den Teilnehmern in einem Computernetz abgehört oder manipuliert werden kann. Dadurch besteht die Möglichkeit, einen *Man-In-The-Middle-Angriff* auf das Netzwerk durchzuführen.

Kurze Erklärung der Parameter:

```
sudo ngrep "Ekhlaas|ASRAR" Ausführen von ngrep als Administrator mit Ekhlaas oder ASRAR als Suchmuster.
```

-W byline Ergebnis zeilenweise formatiert in ASCII darstellen. Für Hexadezimal, Parameter -x verwenden.

port 80 or 25 -d 10 Durchsuchen der Verbindungen zum Webserver (80) und Emailserver (25) über die lokale Netzwerkschnittstelle 10.

*ngrep* verfolgt jetzt alle Pakete in Klartext die Lokal über den Port 80

(HTTP) oder 25 (SMTP) verschickt werden und sucht darin das vordefinierte Muster. Dies trifft natürlich nicht auf verschlüsselte Verbindungen wie HTTPS zu. In unserem Beispiel wird nach dem Muster *Ekhlaas* oder *ASRAR* gesucht. Jene sind in den verschlüsselten Nachrichten, digitalen Signaturen<sup>14</sup>, sowie den öffentlichen und privaten Schlüsseln vorhanden. Sie bilden den Kopf und Fuß der Datei (wahrscheinlich) nach dem Vorbild von PGP.

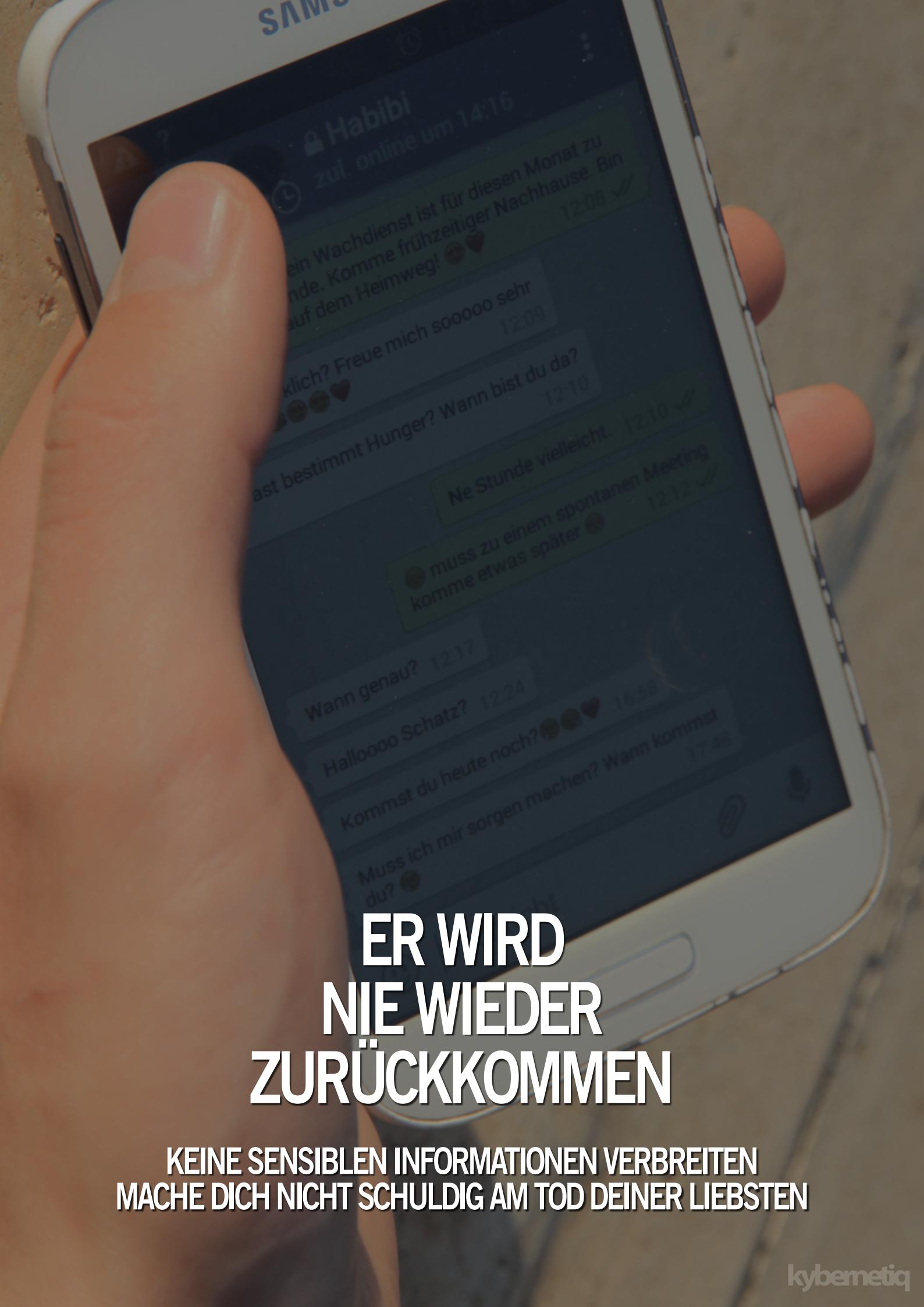
```
### Begin Al-Ekhlaas Network ASRAR El Moujahedeen V2.0 Public Key 2048 bit###
#---End Al-Ekhlaas Network ASRAR El Moujahedeen V2.0 Public Key 2048 bit---
### Begin Al-Ekhlaas Network ASRAR El Mojahedeen V2.0 Private Key 2048 bit###
#---End Al-Ekhlaas Network ASRAR El Mojahedeen V2.0 Private Key 2048 bit---
### Begin ASRAR El Mojahedeen v2.0 Encrypted Message ###
### End ASRAR El Mojahedeen v2.0 Encrypted Message ###
## Begin ASRAR El Mojahedeen V2.0 Message Digital Signature ##
## End ASRAR El Mojahedeen V2.0 Message Digital Signature ##
```

Das Wort Mudschahidin wird auf zwei unterschiedliche Weisen geschrieben: *El Mojahedeen* und *El Moujahedeen*. Entweder konnte(n) sich der (die) Autor(en) nicht für eine lateinische Schreibweise entscheiden oder es waren Schreibfehler beim Programmieren. Es könnte ein Zeichen von schneller und unsauberer Arbeit sein.

## Metadaten können töten

Nun erstelle mit dem *Keys Manager* einen neuen Schlüsselbund. Importiere den öffentlichen und privaten Schlüssel und schließe den *Keys Manager*. Wähle im Hauptfenster die beiden Schlüssel aus und klicke auf *Messaging*. Nun schreibe dir selbst eine Nachricht und klicke auf *Encrypt*. Kopiere die verschlüsselte Nachricht aus Asrar2 und schicke sie an deinen eigenen lokalen Web- oder Emailserver.<sup>15</sup>

Im Terminal müsstest du jetzt *ngrep* das Ergebnis präsentieren (siehe Seite 7). Was du mit simplen Tricks lokal auf deinem Computer nachvollziehen kannst, können Internetanbieter, Behörden, Polizei, Militär und Geheimdienste natürlich auch. Diesen Machbarkeitsnachweis habe ich bewusst lokal gehalten. Mit einem *ARP-Spoofing*<sup>16</sup> Angriff wäre man in der Lage als *Man-in-the-Middle*<sup>16</sup>, daheim, im Firmennetz oder auch



# ER WIRD NIE WIEDER ZURÜCKKOMMEN

KEINE SENSIBLEN INFORMATIONEN VERBREITEN  
MACHE DICH NICHT SCHULDIG AM TOD DEINER LIEBSTEN



Begriffe zu verwenden. Um nicht aufzufallen, gehört auf jedenfall eine enorme Disziplin dazu. Dies gilt auch beim normalen Surfen.

Für Instant-Messaging könnt ihr euren Client nach Wahl benutzen. Ich bevorzuge *Pidgin*<sup>21</sup> mit dem *Off-The-Record (OTR)* Plugin<sup>22</sup>. Registriert euch auch hier eine neue *JabberID* bei einem sicheren und datenschutzfreundlichem Server im Ausland<sup>23</sup>. Verbindet euch zu diesem Server über *Tor* und falls vorhanden, benutzt gleich die *Onion-Adresse*<sup>24</sup> des Jabber Servers.

#### Mobiltelefon - Whatsapp, Telegram und Co.

Dies ist wohl einer der größten Schwachstellen, die wir freiwillig mit uns schleppen. Vor einem Jahr hätte ich vielleicht gesagt, dass *TextSecure* und *ChatSecure* eine gute Wahl wären.

Doch nach der Invasion der Russen und Amerikaner in Syrien, kann ich jedem nur davon abraten, Smartphones zu verwenden. Zumindest haben diese Geräte bei Kämpfen oder an andere sensible Orte, wie Meetings, nichts verloren. Das betrifft auch Geschwister, die sich im Ausland befinden.

Tauscht über Mobiltelefone keine sensiblen Informationen aus, die der Geheimdienst im Nachhinein gegen euch verwenden kann. **Solche Sachen sollten immer vor Ort auf einen Zettel notiert und schnellstens verbrannt werden.**

In der nächsten Ausgabe werden wir uns, so Allah erlaubt, mehr mit Mobiltelefonen beschäftigen.

Ich freue mich auf eure Kommentare und Anregungen.

Bitte vergisst mich nicht in euren Bittgebeten. Alles Lob und jeglicher Dank gebühren Allah allein, dem Herrn der Welten.

## GLOSSAR UND FUSSNOTEN

21. [Pidgin für Linux, Windows und Mac OS X](#)

22. [Off-The-Record Plugin und weitere Informationen](#)

23. Achtung: Nach den NSA-Entthüllungen versprechen viele geldgierige Anbieter Privatsphäre und Datenschutz, die sie nicht einhalten können.

24. Eine Pseudo-Top-Level-Domain (.onion) die nur innerhalb des TOR-Netzes erreichbar ist. Auch *Versteckte Dienste* genannt.

25. Siehe Seite 7 *Infobox*

26. Mehr zum OpenPGP Standard auf [Wikipedia](#)

27. GPL auch GNU General Public License ist die am weitesten verbreitete Software-Lizenz. [Wikipedia](#)

28. Zertifizierungsstelle (engl.: certificate authority oder certification authority, kurz CA) ist eine Organisation, die digitale Zertifikate herausgibt. [Wikipedia](#)



# Werde zum Albtraum der Geheimdienste und des Militärs

## GnuPG Schritt für Schritt Anleitung

**Mit dieser Anleitung wollen wir euch zeigen, wie ihr eure Nachrichten und Dateien sicher vor den Feinden Allahs verschlüsseln könnt.**

von Kybernetiq Redaktion

### Gpg4win gleich Gpg4win?

Beim ersten Entwurf dieser Anleitung wollten wir auf die Webseite von Gpg4win hinweisen. Uns ist jedoch aufgefallen, dass der Hersteller seinen Besucher keine valide HTTPS-Verbindung zur Verfügung stellt. (Abbildung 4)

Somit kann die Software beim Herunterladen von Unbefugten manipuliert werden. Statt der original Software könnten Geheimdienste oder Hacker uns eine manipulierte Version mit einem Trojaner unterjubeln.

Mit den richtigen Programmen wird das sogar

vollautomatisiert zum Kinderspiel. Wir werden, so Allah es uns erlaubt, in den nächsten Ausgaben darauf eingehen.

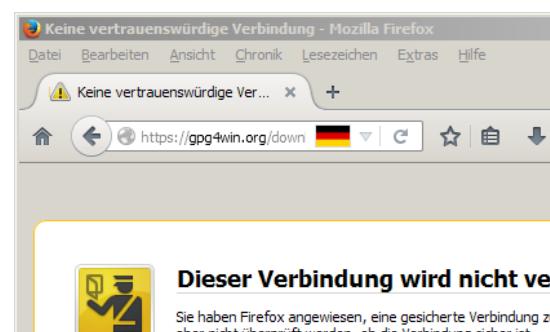


Abbildung. 4. Es ist uns unverständlich wieso Gpg4win keine HTTPS-Verbindung erzwingt. Das manipulieren des Downloads als Man-In-The-Middle wäre ein Kinderspiel. Eine Webseite die Programme zum herunterladen anbietet, sollte zwingend HTTPS statt HTTP verwenden.

Die Hersteller von

Gpg4win bieten ein selbstsigniertes Zertifikat an, aber zwingen es nicht

dem Besucher der Webseite auf. Das liegt wohl daran, dass jeder Browser eine Warnung anzeigt und den Besucher verunsichern würde.

Um dies zu vermeiden, müsste der Betreiber der Webseite sein SSL-Zertifikat von einer Zertifizierungsstelle<sup>28</sup> signieren lassen. Dies ist je nach Anbieter teuer und darum verzichten die meisten komplett darauf.

### Freie Software - offene Quellen

GnuPG basiert auf dem OpenPGP Standard<sup>26</sup> und ist unter der GPL-Lizenz<sup>27</sup> verfügbar. Verwendet werden ausschließlich patentfreie Verschlüsselungsalgorithmen. Es ist kostenlos für alle gängigen Systeme verfügbar. Diese Anleitung bezieht sich auf die Windows Variante Gpg4win.

**Alle Schritte funktionieren auch auf anderen Plattformen.**

Wir werden bewusst nicht den Assistanten zum Erstellen des *Schlüsselbundes* verwenden, sondern beschäftigen uns mit der Kommandozeile von GPG. Es gibt einige grafische Benutzeroberflächen, die noch keine 4096 Bit *Schlüssellängen* unterstützen und uns bei der Erstellung zwingen, eine Email anzugeben. Nach dem Generieren des Schlüsselbundes kann die gewünschte grafische Benutzeroberfläche verwendet werden.

Soweit stellt es kein Problem dar, schließlich bieten die Hersteller von Gpg4win ein selbstsigniertes SSL-Zertifikat an (Abbildung 5). Das ist immer noch besser als seinen Besuchern überhaupt kein HTTPS anzubieten.

Ein selbstsigniertes SSL-Zertifikat könnte sogar sicherer als eines von einer Zertifizierungsstelle sein. Es kam öfters vor, dass bei diesen Organisationen eingebrochen wurde oder die Betreiber unerlaubt falsche Zertifikate für Behörden ausgestellt haben. Diese werden dann bei fast allen Browsern akzeptiert.

Da jeder ein selbstsigniertes Zertifikat erstellen und es uns unterschieben kann, müssen wir zuvor die digitalen Fingerabdrücke abgleichen.

Jedoch gibt es ein grundlegendes Problem, da der Hersteller standardmäßig kein HTTPS zur Verfügung stellt. Deshalb sind die nachfolgenden Links zu den externen Dateien, also in unserem Fall zu den Downloads, immer noch unsichere HTTP-Verbindungen.

Wir sparen uns jetzt die ganzen Details, um euch nicht zu verwirren und bieten euch den direkten sicheren Downloadlink an. (Siehe Beschreibung Abbildung 6)

Nachdem wir uns vergewissert haben, dass wir die Datei vom richtigen Server gezogen haben, rufen wir unseren *Downloads* Ordner auf und überprüfen die kryptographische Prüfsumme. Dafür könnt ihr z.B. das Programm *HashMyFiles*<sup>29</sup> verwenden. (Abbildung 7.)

Die aktuelle Prüfsumme der *Gpg4win light Version 2.2.3* ist folgende:

33308d11ac37c9321277fca1ec22b96ef51a11a0 Gpg4win-light-2.2.6.exe

Je nach Version weichen die jeweiligen Prüfsummen ab. Die aktuellen Prüfsummen erhält man auf der offiziellen Webseite.

Falls bei der Überprüfung die Prüfsumme nicht mit der oberen übereinstimmt, wurde die Software manipuliert. Dies muss aber nicht heißen, dass der Geheimdienst dahinter steckt und euch eine schädliche Variante von GPG unterschieben will.

Es ist auch möglich, dass die Datei beim Download beschädigt wurde. Da der Inhalt der

| <b>Ausgestellt für</b>    |   |
|---------------------------|---|
| Allgemeiner Name (CN)     | wald.intevation.org   |
| Organisation (O)          | Intevation GmbH   |
| Organisationseinheit (OU) | Free Software project hosting   |
| Seriennummer              | 0D  |
| <b>Ausgestellt von</b>    |   |
| Allgemeiner Name (CN)     | Server CA 2013  |
| Organisation (O)          | Intevation GmbH   |
| Organisationseinheit (OU) | <kein Teil des Zertifikats>   |
| <b>Gültigkeitsdauer</b>   |   |
| Beginnt mit               | 09.04.2014  |
| Läuft ab am               | 08.04.2016  |
| <b>Fingerabdrücke</b>     |   |
| SHA-256-Fingerabdruck     | 20:B8:00:01:23:8D:86:21:AE:63:B2:6A:4F:99:53:5A:5D:E0:7C:93:BB:64:C3:39:64:A5:81:88:F2:6A:F3:27 |
| SHA1-Fingerabdruck        | 3B:AD:99:29:43:44:D4:97:15:2E:FB:EE:1C:5A:7E:A1:C4:BE:07:C8                                     |

Abbildung 5. SSL-Zertifikat Informationen und Fingerprints zu https://www.gpg4win.org. Leider sind die Downloads dennoch über eine unsichere HTTP-Verbindung verlinkt.

Datei nicht mehr identisch mit dem Original ist, schlägt die Verifizierung der Datei fehl.

Wenn Fehler auftreten, solltet ihr die Schritte oben noch einmal durchgehen. Kein Grund zur Panik. Irgendwo ist euch vielleicht ein Fehler unterlaufen.

| <b>Ausgestellt für</b>    |   |
|---------------------------|---|
| Allgemeiner Name (CN)     | files.gpg4win.org   |
| Organisation (O)          | Intevation GmbH   |
| Organisationseinheit (OU) | gpg4win file server   |
| Seriennummer              | 06  |
| <b>Ausgestellt von</b>    |   |
| Allgemeiner Name (CN)     | Server CA 2013  |
| Organisation (O)          | Intevation GmbH   |
| Organisationseinheit (OU) | <kein Teil des Zertifikats>   |
| <b>Gültigkeitsdauer</b>   |   |
| Beginnt mit               | 29.01.2014  |
| Läuft ab am               | 29.01.2016  |
| <b>Fingerabdrücke</b>     |   |
| SHA-256-Fingerabdruck     | 29:5B:01:5B:32:CB:21:A6:39:2C:63:60:8B:BB:1E:EB:4F:E9:75:30:9D:31:42:EE:36:C1:B1:6B:26:C0:DE:E0 |
| SHA1-Fingerabdruck        | 63:1A:36:D6:02:FF:FB:B5:2D:80:24:9F:E4:9A:D8:7B:E1:0A:50:6B                                     |

Abbildung 6. SSL-Zertifikat Informationen und Fingerprints zu https://files.gpg4win.org. Durch den direkten Aufruf von https://files.gpg4win.org/gpg4win-light-2.2.6.exe kann die Gpg4win light 2.2.6 (Stand: 26. Oktober 2015) sicher heruntergeladen werden.

Falls jedoch der Fehler immer noch besteht, solltet ihr euch vergewissern, dass euer Internetzugang nicht kompromittiert wurde.

**Alternative Download Webseiten sind nicht zu empfehlen.** Eine Lösung wäre es, die Dateien über einen anderen Internetzugang herunterzuladen. (Internet-Cafe, Nachbars WLAN,...)

## Installation und Einrichtung

Mit einem Doppelklick starten wir die Installation von Gpg4win und klicken uns durch das Setup. Nach erfolgreicher Installation, öffnen wir die Eingabeaufforderung, indem wir auf **Start** klicken und *cmd.exe* eingeben.

Nun tippen wir folgende Befehle ein:

`gpg --gen-key`

Wir werden gefragt, welche Art von Schlüssel wir verwenden wollen. Wir antworten mit einer **1** für RSA und RSA.

Als nächstes werden wir gefragt, welche **Schlüssellänge** wir verwenden wollen. Als Standard ist 2048 Bit eingestellt. Jedoch

verwenden wir aus Sicherheitsgründen und als Präventionsmaßnahme 4096 Bit. Dazu tippen wir einfach 4096 ein und bestätigen es.

Im Schritt darauf werden wir gefragt, wie lange unser Schlüssel **gültig** sein soll. Dieser Schritt ist jedem frei überlassen. Empfehlenswert wäre eine Zeit ab eins bis fünf Jahren.

Als Beispiel stelle ich die Gültigkeit auf 0 für **Schlüssel verfällt nie**, ein. Falls Ihr euch z.B. für ein Jahr entscheidet, dann gibt dazu 1y ein und bestätigt eure Eingabe. GPG rechnet das **Verfallsdatum** aus und erwartet von uns eine weitere Bestätigung.

Für die **User-ID** verlangt GPG von uns **Vorname** und **Nachname**. Natürlich darf ihr hier nicht euren echten Namen eintragen. Religiöse Pseudonyme oder arabische Namen sollten ebenfalls gemieden werden. Sucht euch einen unauffälligen Namen aus.

Im nächsten Schritt können wir unsere **Email-Adresse** eintragen. Dies ist nicht empfehlenswert, aber ist jedem persönlich überlassen. Es hat natürlich Vor- und Nachteile. Für unsere ersten Schritte ist es ausreichend **Email-Adresse** und **Kommentar** frei zu lassen.

GPG fragt uns jetzt, ob unsere Eingaben richtig sind oder ob wir Änderungen vornehmen wollen. Mit **f** bestätigen wir nun, dass wir fertig sind.

Nun erscheint ein Eingabefeld für unsere **Passphrase**. Falls ihr Probleme mit dem Merken von komplizierten Passwörtern habt, könnt ihr auch eine Passwort Datenbank benutzen. Wir bevorzugen *KeePassX*<sup>30</sup>. Mit einem Masterpasswort könnt ihr eure Logins und Passphrasen verwalten.

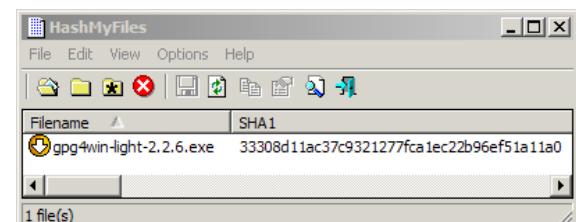


Abbildung 7. HashMyFiles kann verschiedene Hash-Algorithmen berechnen.

Bitte benutzt keine Online Passwort Datenbanken. Schlüssel und Passphrasen haben nichts in der Cloud von Dritten verloren! Würdest du einen Unbefugten deinen Haus- oder Tresorschlüssel überlassen?

Es sind nicht genügend Zufallswerte vorhanden. Bitte führen Sie andere Arbeiten durch, damit das Betriebssystem weitere Entropie sammeln kann!

Zum Generieren braucht GPG eine Menge

## GLOSSAR UND FUSSNOTEN

29. HashMyFiles kann ihr unter [NirSoft.net](http://NirSoft.net) herunterladen (kein HTTPS)

30. KeePassX kann ihr für verschiedene Plattformen auf [www.keepassx.org](http://www.keepassx.org) herunterladen oder unter Debian/Ubuntu mit apt-get install keepassx installieren

Zufallswerte, die wir erzeugen müssen. Ihr könnt dies unterstützen, indem ihr z.B. in einem anderen Fenster/Konsole irgendetwas tippt, die Maus bewegt oder irgendwelche anderen Programme benutzt.

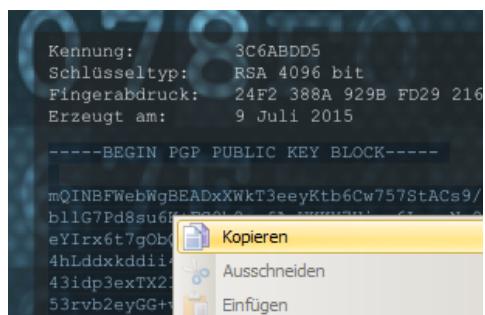


Abbildung. 9. Zum Testen könnt ihr den öffentlichen Schlüssel auf der letzten Seite des Magazins rauskopieren und im Hauptfenster von GPA einfügen.

## Notfall und Prävention

Zur Sicherheit wollen wir noch ein *Schlüsselwiderruf-Zertifikat* erstellen. Dies ist aber nicht unbedingt nötig und kann übersprungen werden. Dazu tippen wir in der Konsole folgenden Befehl ein und ersetzen <User-ID> durch den zuvor von euch gewählten Namen.



Abbildung. 10. Nachricht vor der Verschlüsselung. Aus der GPA Zwischenablage aus kommt ihr direkt Nachrichten ver- und entschlüsseln. Somit hinterlässt ihr keine Spuren auf der Festplatte.

`gpg -o revok --gen-revok <User-ID>`

Wir bestätigen unsere Eingabe mit *j* und geben als Widerrufgrund die Nummer 1 ein. Wer will, kann noch eine Beschreibung hinzufügen und beendet die Eingabe mit *Return*.

Die Nachfrage, ob unsere Eingabe richtig ist,

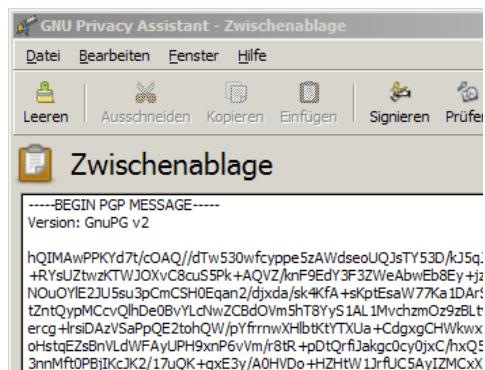


Abbildung. 11. Nach dem Verschlüsseln der Nachricht mit dem öffentlichen Schlüssel des Empfängers, erhält man einen Base64 kodierten Text. Gegebenenfalls könnt ihr den Kommentar Version: GnuPG v2 entfernen und den Rest unverändert kopieren.

bestätigen wir wieder mit *j*. Nach Eingabe der Passphrase wird das Schlüsselwiderruf-Zertifikat erstellt und wir werden aufgefordert, es an einem sicheren Ort aufzubewahren.

## GNU Privacy Guard

Bis hierher haben wir das Komplizierte hinter uns. Jetzt können wir uns der grafischen Oberfläche GPA widmen (Abbildung 8). Wir klicken auf **Start** oder drücken die *Windows-Taste* und suchen nach *GPA* und starten das Programm.

Im Hauptfenster sollte dein (zuvor generierter) Schlüssel angezeigt werden. Um einen Schlüssel zu importieren, klicke oben im **Menü ► Server ► Schlüssel erhalten...**. Hier können wir die User-ID unseres Gesprächspartners eingeben, sofern er seinen öffentlichen Schlüssel auf einem Keyserver hochgeladen hat.

Es ist euch selbst überlassen, ob ihr euren öffentlichen Schlüssel auf den Keyserver hochladen wollt. Ihr könnt euch gegenseitig den öffentlichen Schlüssel auch anderweitig zukommen lassen.

Damit bleibt ihr auch unter dem Radar und es ist nicht mehr so leicht, auf dem Keyserver einen gefälschten öffentlichen Schlüssel unter eurem Namen zu verbreiten.

## Import und Export

Öffentliche Schlüssel deiner Gesprächspartner kannst du auf verschiedene Wege importieren. Bei manchen Systemen reicht ein Doppelklick auf die .asc Datei. Falls sich ein Textverarbeitungsprogramm wie Notepad öffnet, markiere den gesamten Inhalt und füge ihn im Hauptfenster mit **Rechtsklick ► Einfügen** ein oder oben im Menü auf **Bearbeiten ► Einfügen**. (Abbildung 9)

Eine andere Möglichkeit wäre im **Menü ► Schlüssel ► Schlüssel importieren** auszuwählen und die .asc Datei direkt zu importieren.

Mit einem **Rechtsklick** auf unseren *Schlüsselbund* (gekennzeichnet als gelber und blauer Schlüssel) könnt ihr unter *Schlüssel exportieren...* euren öffentlichen Schlüssel und unter *Sicherheitskopie anlegen...* euren privaten Schlüssel exportieren.

## Verschlüsselung und Signierung

**Rechtsklick** auf die zu verschlüsselnde Datei, im Kontextmenü **► Signieren und verschlüsseln** auswählen.

Nun wählen wir den öffentlichen Schlüssel des

| Schlüsselkennung   |            | Erstellt          | Verfallsdatum                   | Benutzervertrauen | Gültig |
|--|------------|-------------------|---------------------------------|-------------------|--------|
|  | P 2040DCB6 | 2015-10-25        | kein Verfallsdatum              | Ultimativ         | voll   |
| <hr/>  |            |                   |                                 |                   |        |
| <b>Details</b>   |            | <b>Signaturen</b> | <b>Untergeordnete Schlüssel</b> |                   |        |
| <p>Dieser Schlüssel hat einen öffentlichen und einen geheimen Teil<br/>Der Schlüssel kann zur Zertifizierung, zum Signieren und zur Verschlüsselung<br/>Benutzerkennung: GuyFawkes<br/>Schlüsselkennung: 2040DCB6<br/>Fingerabdruck: B0E6 769A 37F7 6D9A 3C80 92E4 EDBE 7AA5 2040 DCB6<br/>ungültig ab: kein Verfallsdatum<br/>Benutzervertrauen: Ultimativ<br/>Gültigkeit: voll gültig<br/>Art: RSA 4096 bit<br/>erzeugt am: 2015-10-25</p> |            |                   |                                 |                   |        |
| <hr/>  |            |                   |                                 |                   |        |
| <b>Standard-Schlüssel: 2040DCB6 GuyFawkes</b>  |            |                   |                                 |                   |        |

Abbildung. 8. Die Benutzeroberfläche von GNU Privacy Guard.

Empfängers aus. Die Datei zu signieren, schadet nicht. Dazu setzen wir einen Haken bei *Signieren* und wählen unseren eigenen Schlüssel aus.

Bei Bedarf können wir noch einen Haken bei *ASCII-Verpackung* setzen. Somit ist gewährleistet, dass die verschlüsselte Datei ohne Komplikationen per Email oder Privatnachricht verschickt werden kann. Andernfalls wird eine kleinere PGP-kompatible binäre Datei erstellt.

```
C:\Windows\system32\cmd.exe - gpg --gen-key
C:\>\gpg --gen-key
gpg (GnuPG) 2.0.29; Copyright (C) 2015 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Bitte wählen Sie, welche Art von Schlüssel Sie möchten:
  (1) RSA und RSA (voreingestellt)
  (2) DSA und Elgamal
  (3) DSA <nur signieren/beglaubigen>
  (4) RSA <nur signieren/beglaubigen>
Ihre Auswahl? 1
RSA-Schlüssel können zwischen 1024 und 4096 Bit
Welche Schlüssellänge wünschen Sie? (2048) 4096
Die verlangte Schlüssellänge beträgt 4096 Bit
Bitte wählen Sie, wie lange der Schlüssel gültig sein soll:
  0 = Schlüssel verfällt nie
  <n> = Schlüssel verfällt nach n Tagen
  <n>w = Schlüssel verfällt nach n Wochen
  <n>m = Schlüssel verfällt nach n Monaten
  <n>y = Schlüssel verfällt nach n Jahren
Wie lange bleibt der Schlüssel gültig? <0> 0
Schlüssel verfällt nie
Ist dies richtig? <j/N> j
GnuPG erstellt eine User-ID um Ihren Schlüssel:
Ihr Name (<"Vorname Nachname">): GuyFawkes
Email-Adresse:
Kommentar:
Sie haben diese User-ID gewählt:
  "GuyFawkes"
Ändern: <N>ame, <K>ommentar, <E>-Mail oder <F>ingerprint
Sie benötigen eine Passphrase, um den geheimen Schlüssel zu verschlüsseln.
```

Bei größeren Dateien ist es vorteilhafter, die Dateien ohne *ASCII-Verpackung* zu erstellen. Was den Datentyp angeht, kennt GPG keinen Unterschied, ob es ausführbare Dateien, komprimierte Archive, Bilder, Videos oder Dokumente sind. Alles lässt sich problemlos verschlüsseln.

Falls du nur eine verschlüsselte Nachricht schreiben willst, ohne eine Textdatei zu erstellen, kannst du auch im Hauptfenster auf **Menü ► Fenster ► Zwischenablage** oder auf **Symbol Zwischenablage** klicken (Abbildung 10).

Schreibe direkt deine Nachricht in die *Zwischenablage* und klicke auf *Verschlüsseln*.

Nach Auswahl des öffentlichen Schlüssels des Empfängers wird die Nachricht verschlüsselt und im selben Fenster angezeigt (Abbildung 11).

Die Nachricht kann nun von dort rauskopiert und im Textverarbeitungsprogramm, Email oder Privatnachricht, eingefügt werden.

Zum Entschlüsseln kann auf die gleiche Weise der verschlüsselte Text deines Gesprächspartners in die *Zwischenablage* kopiert werden. Klicke auf *Entschlüsseln* und gebe deine *Passphrase* ein. Nun sollte der entschlüsselte Text erscheinen (Abbildung 12).

## Verschlüsselte Backups

Eine verschlüsselte Festplatte ist sinnvoll und kann Unbefugte davon abhalten, physikalischen Zugriff auf deine Dateien zu erlangen.

Jedoch hat man wenig von diesem Vorteil, wenn die Behörden an deine unverschlüsselten Sicherungskopien herankommen. Darum ist es auch wichtig, die Sicherungskopien zu verschlüsseln.

Leider eignet sich PGP / GPG nur bedingt als Backup Verschlüsselung. Eine asymmetrische Verschlüsselung benötigt eine höhere Rechenleistung und bei Verlust des privaten Schlüssels sind die Sicherungskopien nicht mehr zu retten.

Für Backups eignen sich symmetrische Verschlüsselungsalgorithmen wie AES am besten. So Allah will, werden wir in den nächsten Ausgaben auf diese Programme eingehen.

## Die Schattenseiten

Alle diese Programme helfen dir natürlich wenig, wenn dein Computer von Behörden, Geheimdiensten oder Cyberkriminellen, mit Schadsoftware infiziert wird.

Diese Programme können mit einem *Keylogger* die Tastenschläge aufzeichnen und vom Bildschirm Screenshots erstellen.

Falls Unbefugte an den privaten Schlüssel und die Passphrase kommen, wäre es möglich, nachträglich alle alten und zukünftigen Nachrichten sowie Dateien, die mit dem privaten Schlüssel verschlüsselt wurden, zu entschlüsseln.

Leider unterstützt PGP (und das ist auch bei Asrar2 der Fall) noch kein *Perfect Forward Secrecy* (PFS). Diese Methode verhindert, dass nachträglich ältere Sitzungen entschlüsselt

werden können.

Die NSA sammelt und archiviert wichtige verschlüsselte Kommunikationen, falls sie in Zukunft den Schlüssel brechen oder anderweitig in den Besitz des Schlüssels kommen. So können sie die Daten im nachhinein entschlüsseln.

Das soll aber keinen von uns demoralisieren und davon abhalten auf Verschlüsselung zu verzichten. Der Feind ist zwar oft im Vorteil, er ist aber nicht allmächtig und seine Ressourcen sind auch irgendwann ausgeschöpft. So schadet man ebenfalls dem Feind, in dem man ihn dazu zwingt, seine Ressourcen zu verbrauchen.

Ein weiteres Problem ist auch, dass die meisten Menschen faul und bequem sind, solche Programme einzusetzen. Einige argumentieren auch oft damit, dass die Installation schwer und die Handhabung kompliziert sei. Merkwürdig ist jedoch, dass genau die gleichen Leute es schaffen, sich ein Skype- oder ein Facebook Konto einzurichten oder andere komplizierte Vorgänge zu bewältigen.

Nun liegt es an euch. Seid achtsam und euren Feinden immer ein Schritt voraus. Werdet nicht leichtsinnig und neigt nicht zur Paranoia. Versucht die Waagschale im Gleichgewicht zu halten.

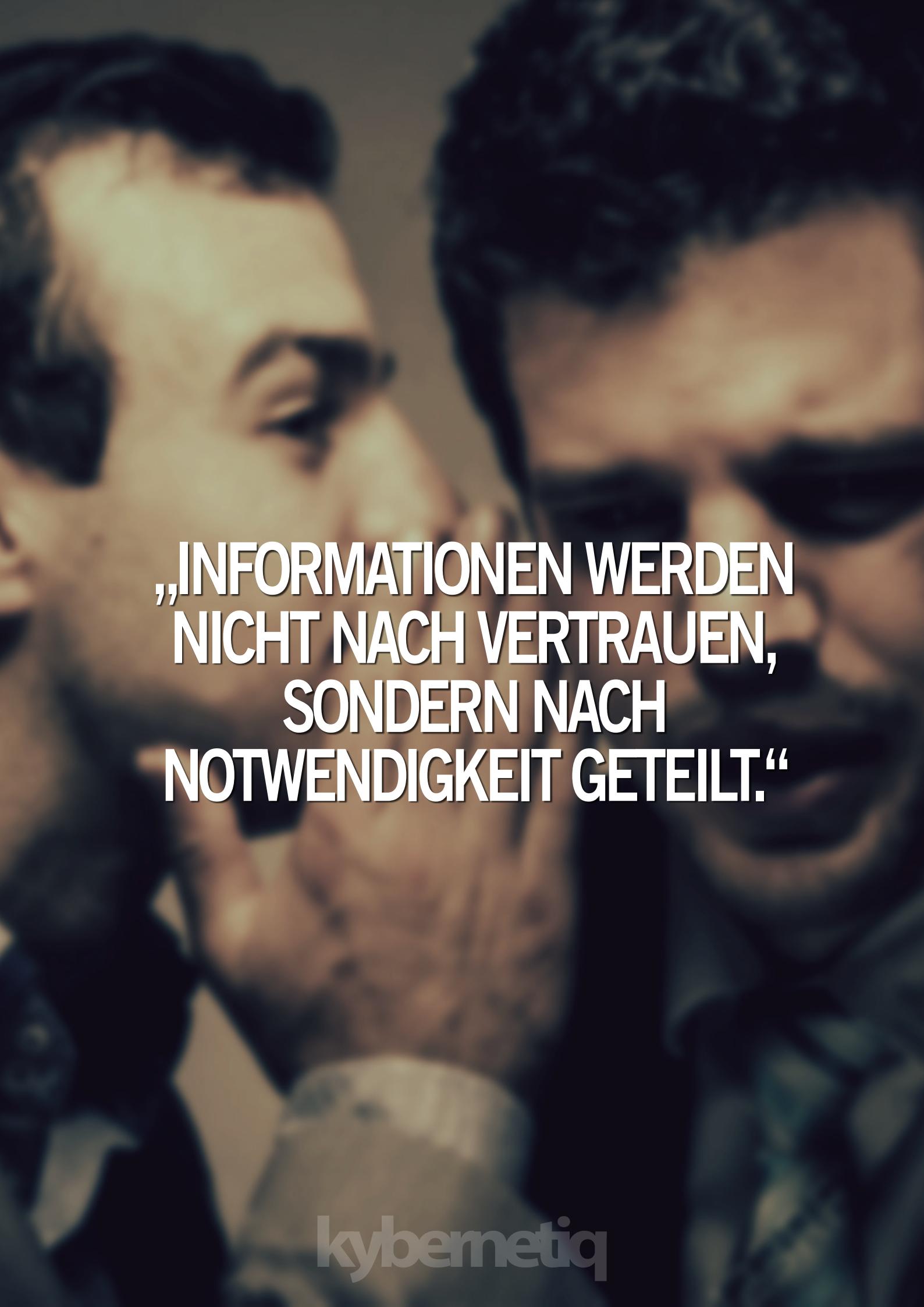
Auf die ersten verschlüsselten Nachrichten von euch freuen wir uns jetzt schon.



Abbildung 12. Im gleichen Fenster lässt sich auch die verschlüsselte Nachricht deines Gesprächspartners entschlüsseln.



**Der Feind liest mit.  
Bleibe wachsam und  
unterschätze ihn nicht.**



„INFORMATIONEN WERDEN  
NICHT NACH VERTRAUEN,  
SONDERN NACH  
NOTWENDIGKEIT GETEILT.“

kybernetiq

# Die Einheit

DIE ERSTE ISLAMISCHE SCI-FI NOVELLE

Die Autoren von *Kybernetiq* haben es sich zur Aufgabe gemacht, in jeder Ausgabe eine fiktive Kurzgeschichte zu veröffentlichen. Die Protagonisten sind vielfältig, doch die Geschichte finde immer an gleichen Orten statt. Achtung: Natürlich handelt es sich hier lediglich um Fiktionen, die Muslimen weltweit Motivation und Denkanstöße vermitteln soll.

## Prolog

„Inzwischen betrug die sozialistische Republik Kurdistan schon eine Landfläche von ca. 270.000km<sup>2</sup>. In den letzten Jahrzehnten ist sie besonders durch ausländische Hilfen noch einmal enorm gewachsen. Mittlerweile hat es wohl den Höhepunkt erreicht und die Bevölkerung scheint zufrieden zu sein. Bereit für Waffenruhe, obwohl der halbe nahe Osten in Schutt und Asche gelegt wurde. Ihre Utopie wurde wahr. Jedoch braut sich momentan in der Region etwas gewaltiges auf, was die Ruhe stören könnte.“

Was das Glück des einen ist, ist das Unglück des anderen. Somit blieb der Türkei nichts anderes übrig als das Land, angefangen von Mersin quer über Sivas bis nach Trabzon, mit einem künstlichen Wassерgraben von ungefähr 600km Länge und ca. 1km Breite und einem 15m hohen High-Tech Betonzaun, zu trennen. Der Kanal hat komplexe Schleusen und beinhaltet Seeminen. Dadurch entstand eine Art Nimmerland zwischen der Westtürkei und den kurdischen Gebieten. Die Hauptstadt wurde nach Izmir verlegt. Es ist nun der Sitz der Neolazistischen Türkei. Ein herber Rückschlag für die Jungtürken.

Alleine die Überwachungskameras und die Selbstschussanlagen brauchen wohl ein eigenes Kraftwerk. Die Bauarbeiten nach der großen Explosion gingen recht schnell. Die Nato-Mächte machten großen Druck auf die neue laizistische Regierung Anatoliens. Sie wussten genau irgendwann werden wir, wie ein Feuer dass sich durch trockenes Gras frisst, bis nach Konstantinopel, durchbrechen.

Fasst der ganze Irak wurde verschluckt und gehört nun zum iranischen Reich, wie es nun heute offiziell heisst. Der marode Irak wurde durch Unbekannte mit einem geheimnisvollen Erstschatz wortwörtlich in den Erdbothen gestampft. Fast der komplette Irak und ihre Einwohner wurden ausgelöscht. Damit ist auch ein neues Zeitalter eingetreten.

Die einen beschuldigen Israel, das mit einem nuklearen Präventivschlag seine Gegner in Schach halten wollte, und die anderen waren der Meinung die Nato stecke dahinter. Wenn ihr mich fragt, ich bin überzeugt, es war der Iran. Nach diesem schwarzen Tag für die Muslime, ging es für die schiitische Sekte Berg auf. Sie überrannten das Land

und machten es wieder bewohnbar als hätten sie schon die ganze Zeit das Gegenmittel parat.

Der Exodus begann und die nicht-persischen Schiiten wurden in den ehemaligen Irak umgesiedelt. Für das Regime waren sie weniger Wert und stellten somit auch eine Art Versuchskaninchen dar. Sie errichteten nun in fast jeder Stadt eine Statue von Ali ibn Abu Talib (ra) und redeten den Bewohnern ein, ihr Schutzpatron aus Stein würde über sie wachen und kein Mensch oder Tier würde durch die geheimnisvolle Substanz, die alles Leben zuvor auslöscht, zu Schaden kommen.

Ein Bruder vom Nachrichtendienst Sakina erzählte mir, dass unsere Jungs von der elektronischen Kampfbrigade 13, sehr weit in das Netzwerk der Nationalgarde des Iranischen Reichs vorgedrungen sind. Sie kamen anbrisantes Material, welches Ayatollah Chomeini II. bei einem Briefing zeigt. Er spricht vom Hauch Ali's, der über das Land der Babylonier hinweg fegen und alles ungläubige auslöschen wird. Der Schura Rat hält noch Absprache, ob sie diese Leaks veröffentlichen werden.

Das angrenzende Kurdistan hat einen Waffenstillstand ausgehandelt. Der läuft schon seit langer Zeit auch recht stabil. Armenien hat widerstandslos kapituliert und wurde in Kurdistan integriert. Das brachte natürlich die Aserbaidschaner in große Schwierigkeiten. Sie verbündeten sich mit Georgien und errichteten die kaspische Mauer.

Was nun uns, die Mudschahidin, betrifft, kontrollieren wir große Gebiete in der Levante bis runter zu Damaskus. Ein Teil Libanons wird de facto vom iranischen Reich regiert. Es wurde über Nacht geputscht und Damaskus wurde zur Hauptstadt ausgerufen. Beirut aufwärts wird durch uns, den vereinigten islamischen Imirate Schām, kontrolliert.

Wir stehen kurz davor die letzte Bastion zu zerschlagen und in Damaskus einzumaschieren. Was für glorreiche Tage, was für glorreiche Tage...

...und alles Lob gebührt Allah, dem Herrn der Welten.“

Prof. Dr. Yuito 'Abdullah' Deisuke  
Kommandeur des 3. Cyborg Regiments und  
Forschungsleiter der Vereinigten islamischen Imirate Schām

53 ; kybernetiq pseudo asml warfe  
54 ; information eine takt.  
55 Diesseits:  
56 call ummah ; rufe "ummah" auf  
57 push iman ; steigere "iman" auf  
58 push muslims ; bewege "muslims"  
59 mov jihad ; dividiere "kuffar"  
60 zum "jihad"  
61 div kuffar ; renne zu "jannah"  
62 jmp jannah ; transferiere  
63 Jenseits:  
64 \_greenbird ; transferiere  
65 mov soul, greenbird ; transferiere  
66 "soul" in "greenbird"

# WARNUNG

Bevor du uns kontaktierst, solltest du dir sicher sein, dass deine Leitung nicht abgehört wird und dein Computer sicher vor Spionage Software ist.

Benutze das Betriebssystem **Tails**, wenn du den Verdacht hast, dass deine Arbeitsumgebung kompromittiert wurde. Um deine Spuren im Internet zuverwischen, greife auf den **Tor Browser Bundle** zurück.

## Temporäre Email Adresse und Öffentlicher Schlüssel

Eine Anleitung wie du PGP anwendest, kannst du auf Seite 8. dieses Magazins nachlesen. Mit unserem öffentlichen Schlüssel kannst du uns verschlüsselte (ggf. auch signierte) Nachrichten und Dateien zuschicken.

Erstelle für die Kontaktaufnahme **unbedingt** eine neue Email-Adresse außerhalb deines Landes und vermeide Emailanbieter wie Gmail, GMX, Web, Yahoo und Hotmail.

Verwende auf keinen Fall gleiche Benutzernamen, Passphrasen und Email-Adressen, die Rückschlüsse auf deine Identität ziehen.

Verwende **Tor** um deine Spuren im Internet zu verwischen. Eine gute Möglichkeit ist es, **Tails** zu verwenden. Tails beinhaltet alle wichtigen Programme. Es kann auf eine DVD gebrannt oder auf einen USB-Stick installiert werden.

Nachdem ersten Kontakt ist auch eine sichere Kommunikation über **XMPPT** oder **Ricochet** möglich.

Kybernetiq Redaktion

kybernetiq@ruggedinbox.com

Kennung: 3C6ABDD5  
Schlüsseltyp: RSA 4096 bit  
Fingerabdruck: 24F2 388A 929B FD29 216A 71AF 2678 E1AE 3C6A BDD5  
Erzeugt am: 9 Juli 2015

-----BEGIN PGP PUBLIC KEY BLOCK-----

```
mQINBFWebWgBEADxXWkT3eeyKtb6Cw7578tACs9/ldwuhTG1qUMvjfAGbsmo2rME
b1L7Pd8su6K+FG9h9sufAuWKKY7UiZu6LqezeNm9mkeJwa/a2vry/nH5m9ib8GY4
eYIx6t7gObQEzhdRGbntef4iUKNytkPlUeidyG/0KAxgxfqAgxj0SvpowEwj57
4hLddxkddi4qN7W/Lyi2ZQ7nW95gz0bGzaNDV/paZ6YOG8N1pxaKLyQDHN2W9
43idp3exTX23pHrG2APw5nLhxjUyS4kuuAnpdAIsPgjLAcgRQMO2h8Av9wyQMNFp
53rvb2eyGG+v4nclxy6UEy9svzLL5DLuH08Dn7Spbx11XyNcnEa0wvRERQer/h6v
31CnwEgEBI806MWvSggA+PtqEe8iXde5w1XsfjrITxm9M//VmQzfL5jk5rJ/u0W6R
BWlNo2800KkP810wg0mEq3q5a1KKl1fv2uiG/yiE5pzcLdbjkGObm2eB3/u0
OAqNxE5v1Y1wTLKdmdLwkyU1X3Qqk9s2ABN9RQy7LKSNPYi5dqM8uXdfBoeANF6
rKbctUxis2Hy8kTQCVxSaOxojWL3JbY+N5zWxmWXoIdNL+WZQZGs9AYWNgNhgZ59
1cjjeVgmaCoUevRvoVkgR+2AhoFluriPgT3vh27cyzPwup8qHyXhvTiuwARAQAB
tBjreWjlcm51dGlxIGlh2F6aW6JAjgEEwECACI1Fa1WeBwgCGwMGcwkIBwMCbhUI
AgkKcwQWaGMAh4BAheAAoEJCZ44a48ar3V6owQAJBxe3o7ut0zHBTz1w61qmO
7qP0zq7fbM2X184IbtBD34ISFxPJ6yix21SK5c2y5a4HVmgH+gnHxfFr1Uy2taxF
Q0w1FedzSLZM0JAr/uf6g26USBqb2I0MDkIFYmJ9sF+7cP4ITHp0Pqy1286hzQP
ca1GRZEtOy6Thb/SyQrdeot3LyNSTXLHD/M1f+sDLix1dVDM8i85Dmb6S+tU/DoX
RBK3JpOdXEfbnNhbEspwm59i1hYi5/49rN9SSG3XCfcVk2Wnv6TgnqcEsmtj
r7ciVnlurAl1yz+r/kn7fPY8ogsLT9wQxsAXCT1JGkw5j/wwVQ6RGBgDIEUYU+uZY
CPTXS6Kltt/rbu2wkoTNJMdElh/PgmkGQAD3ueZbPsndw82I32RqSFrzpt8x5Ms1
h/ytzdP3B5N1+cDQt/+Nm1RH1InQdxuqn9uH1PdpIG/eFFacU/5kGZGVsA1D9Gd
Z5GeV1LyEStLQmcKb1H/4+a+SdF42Ph+mRcV01q7VfjRVYYYGc/6V9Ed2eKa8Ze
4EoqWZyDEtDu79J9nErVn7stKudjiflx4pjdyT9Hnu2ZcJpgET+at1BpytlMx0
e21RoyEkXkJ20+/ozJG2a5menVt7ozEj2Pa/6VEVgl+sHEWwpAaWb++hots4Bxg
+dBX0105Df1wYDKSSwFGuQ1NBFWebWgBEADRxweiNCIMTuhs418K1YQccptSo+Kn
6/WPbT5P/CpNJbk900gZrqp6gOucuFhWrJNv+wWaAkSj1L2hURQ7DWM82iZTxqi0
hcu2fAbivAjz09v9gB7ovGxfNRIHZfHt3nxGi1hNc9odGDBD1yyaiF5eOPZ1HP2
UnGwlW1RkmkeY51Wu4ua7zRwYX58/+P+8uNzUTxo2N1Jlc088VB9sfBWMbdxu
Njtuz7Me3XXSeRJEBuX7RqrpyNrW06a3UwS33Mz7H7PIihjKiKPgDLJWb2Mzod
DeUrh8wz+DOWiFH5KeJW61AiCsFhRFFXDwyoW6RqfN1dDz1bWMQetZLm1D9BaBY
0ocY741lnsaJozCx+nQFVXXwsYoaACNcJQhuCwbQ4kqi4TGuDyBNQccJ1vXozFGd
5tgXB0QKjbJNm72J1Qa0gk16taQ0ry0PGRHY49MM+V07+43J0WON0cdLBVMS0
M01Gi3AJ0t7H+ff51Wu1844AtrfYrfQtc3Qj0e9qomPljPiOs0+crjFM4SbsDKb
nEsgQsb0VcFODUw69x4PT1Mu2yCbezbN+y/sge07rH4Ad/6XRI/w2kO1hDdtGa
+4gbMw1lfJ/ug20yft6kEzqshIhmD4QBeCT0F9P0pHF7qVZQ60Qf+Ehh1Rk3eYVh
qDJUFme2kNaPgQARAQABiQfBBgBAGJBQJVnm1oAhsMAAoJECZ44a48ar3V+P0Q
AOyzwXusd2+86jLP/Ezh8015Bg7KN5BLHegRpT9bLjHTA1eI1LFxqE1v0teJdx
if7Fdj6KnjMDiZez7nxdOE4gBk4UluBhKL1eR6TnnZ1+CX823Y10Kyjch8UTY2
MRoh3Mt1g+SCAVFdf9TTC80GRWXFKuU1o9e7JgLUtjOMTaUpB/A8199XE44qVmwt
mobX2crFzWyRfAqyct0aJMH1SawWqUdwBxEjiBQzoXtsyUYZIXZEBNuDeJm5vh
CMChOBkRh0w39HeRAcozdYpe48sZmrgEAjQ6i0a4Ujj9GSfjCFZud/Je7Bg42xAp
UXOYCswgFy6/cQ28qdy8QJ21/C6rtBE0tEjkPmpSQX9JLcymrXjEtwxVnG6JZZRO
VqlNQsfl/BMKYG36RIog5T5EXMS85zqgHG2u9Qzh1HnsBSa2uuW4JRGvpZIBqnHW
s9eDVtpjkrxY9k1hU1u9hQB+NESv8L9EONJTeM00/8pxTNcBfZUn8rvW+etrsB3x
YBySLT8zxfiazlregudrsRC9xiWNxfLDQxf7LK7rUL9R+CdQxCHb59AEadKCI13
rayyygr43MqrIEt1rj5PXzxHhIj4gTeymxzZcKohcSG4kjZv/yf2500CIqnVZULw
nssqS39v0IjQeGowBpVFcW5uB8gg8DzxHn0c1KPDwg19
=0dt3
-----END PGP PUBLIC KEY BLOCK-----
```