Nutzung von Schlüsseln der Volksverschlüsselung unter iOS

Eine Anleitung für technisch Versierte

Michael Herfert

16. November 2016

Zusammenfassung

Die Volksverschlüsselungs-Software ist zurzeit noch nicht für iOS verfügbar. Wer einen Windows-PC hat, um dort die Volksverschlüsselungs-Software zu benutzen, kann die Schlüssel aber exportieren und sie unter iOS nutzen. Dieser Anleitung beschreibt den Weg dorthin.

Die Ausführungen hier entsprechen nicht dem Anspruch der Volksverschlüsselung an Laientauglichkeit und Benutzungsfreundlichkeit. Sie richten sich an Experten, die ihre Schlüssel sofort unter iOS nutzen möchten, noch bevor die Volksverschlüsselung für dieses Betriebssystem zur Verfügung steht.

1 Ausgangssituation

Wir gehen von folgendem Szenario aus:

- Der Nutzer hat Schlüssel über die Volksverschlüsselung erfolgreich erzeugt.
- Er befindet sich Zuhause in seinem WLAN-Netz.
- Das iOS-Gerät ist im WLAN eingeloggt.

2 Export der Schlüssel

Zunächst müssen die privaten und öffentlichen Schlüssel aus der Volksverschlüsselung so exportiert werden, dass iOS sie importieren kann. Dazu startet man die Volksverschlüsselungs-Software (im Folgenden »VV-App«) und klickt im linken Toolbar auf das Zahnrad (Tooltip »Zertifikatsverwaltung«) und anschließend auf `Schlüssel exportieren`. Wenn man Schlüssel für mehrere Mailadressen besitzt, erhält man nun die Möglichkeit eine Mailadresse auszuwählen. Andernfalls erscheint sofort eine Maske `Zielverzeichnis auswählen`. Rechts unten hat man die Möglichkeit das Datenformat der Export-Datei zu wählen. Voreingestellt ist `.vv-backup`. Man ändert es auf `.zip`, damit die VV-App drei PKCS#12-Dateien in eine ZIP-Datei schreibt:

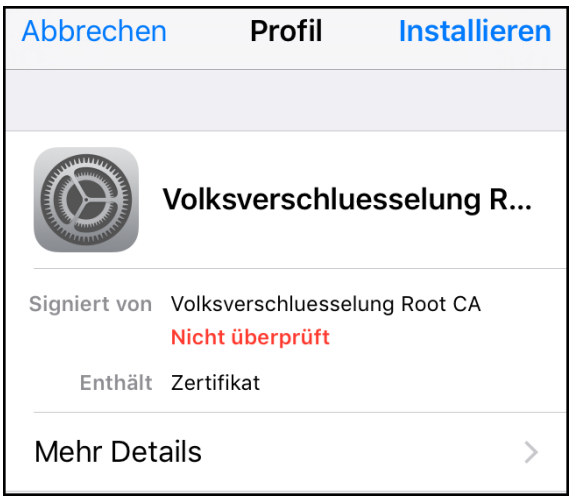
Anschließend vergibt man noch ein Passwort, das sich auf die PKCS#12-Dateien auswirkt, nicht auf die ZIP-Datei. Sofern man das voreingestellte Verzeichnis nicht geändert hat, liegt im Ergebnis auf dem Desktop eine Datei vor, die im vorliegenden Falle den Namen `Schlüssel von herfert (2016-11-03).zip` trägt. Die VV-App kann nun geschlossen werden.

3 Import der übergeordneten Zertifikate

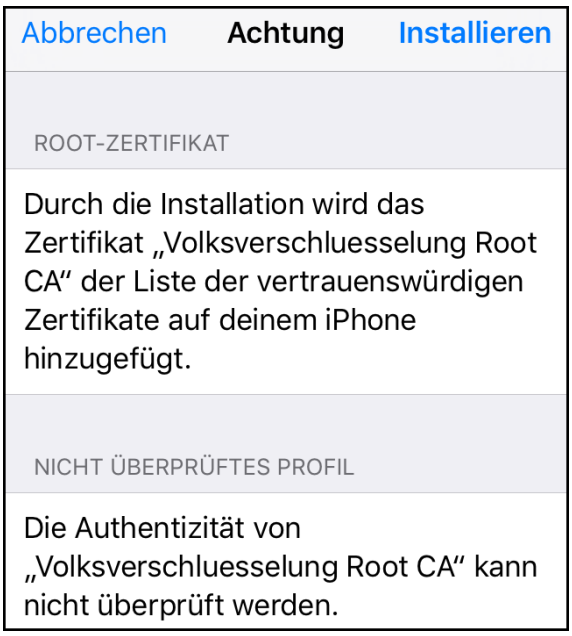
Zuerst installiert man das Wurzel-Zertifikat der Volksverschlüsselung, indem man unter iOS mit Safari den folgenden Link anklickt:

`https://volksverschluesselung.de/cert/VV-Root-CA.crt`

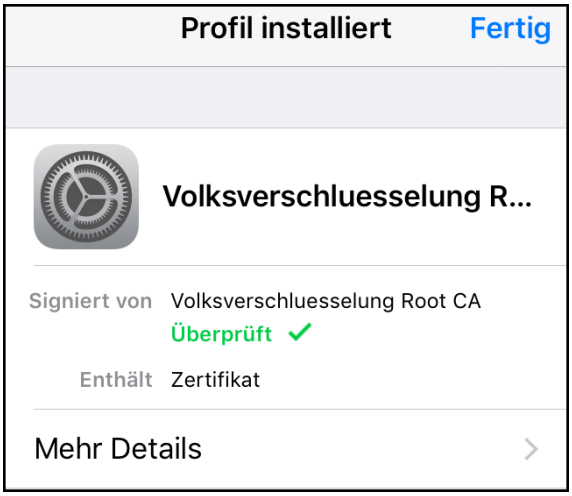
Safari reagiert mit einem Import-Dialog:



Man tippt auf `Installieren` und erhält eine Warnung, die man akzeptieren muss:



Die Erfolgsmeldung sieht so aus:



Anschließend lädt man mit Safari das Zertifikat der Privat CA

`https://volksverschluesselung.de/cert/VV-Private-User-CA.crt`

Es ist ohne Warnhinweis installierbar, weil es durch das Wurzel-Zertifikat signiert ist.

Die Webseite der Volksverschlüsselung authentifiziert sich durch ein TLS-Zertifikat, das sich unter iOS aber nicht anzeigen lässt. Beim Import von Zertifikaten zeigt iOS keine Fingerabdrücken an. Um die Korrektheit des Wurzel-Zertifikats zu verifizieren, ist man auf die Verifikation der Signatur angewiesen, die sich durch `Mehr Details` anzeigen lässt. Wir empfehlen, die Signatur mindestens in Ausschnitten zu verifizieren, wenn auch ihre hexadezimale Darstellung 512 Zeichen umfasst. Die Signatur ist in Anhang 1 abgedruckt.

4 Import der Schlüssel

Die exportierten Schlüssel müssen nun in iOS importiert werden. Dazu stellen wir mehrere Möglichkeiten vor, wobei der Weg über E-Mail nur eine Notlösung ist, falls die anderen Varianten nicht möglich sind.

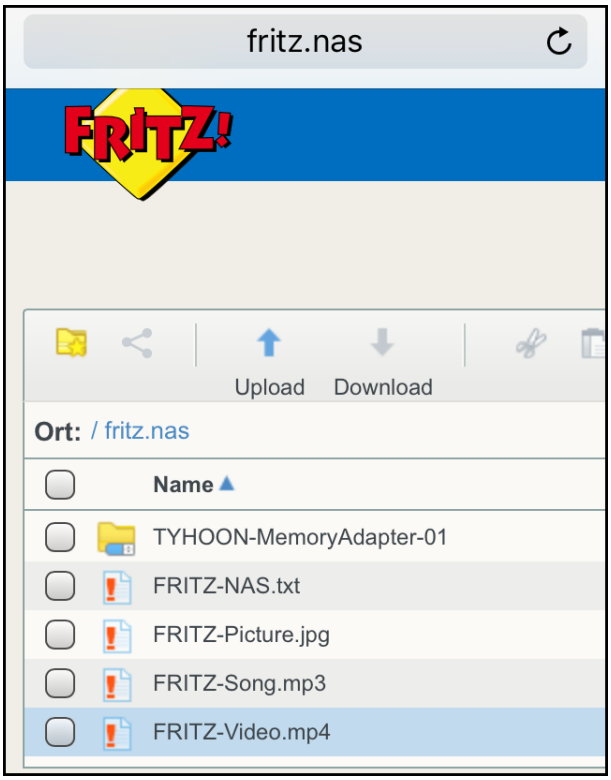
4.1 Import der Schlüssel über die FritzBox

Die FritzBox erlaubt den Anschluss eines USB-Speichersticks, dessen Inhalt anschließend im lokalen Netz über die URL `http://fritz.nas` zugänglich ist. Um diesen Weg zu wählen, legt man auf einem USB-Stick ein neues Verzeichnis an, im Beispiel `vv`, und entpackt die eben erzeugte ZIP-Datei in dieses Verzeichnis. Dort liegen nun drei Dateien:

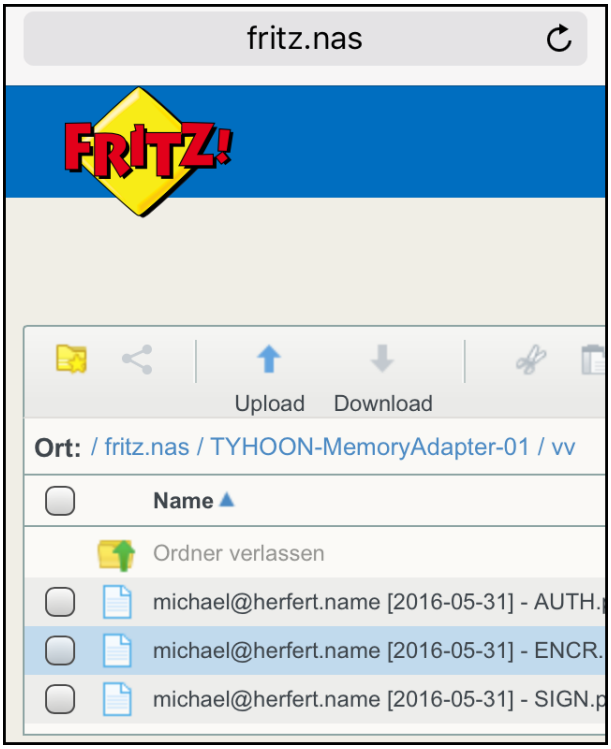
```
michael@herfert.name [2016-05-31] - SIGN.p12
michael@herfert.name [2016-05-31] - ENCR.p12
michael@herfert.name [2016-05-31] - AUTH.p12
```

Die erste Datei enthält den privaten Schlüssel und die Zertifikate für die Entschlüsselung, die zweite ist für das Signieren verantwortlich und die Dritte für die client-seitige kryptografische Authentifizierung.

Man steckt den Stick nun in die FritzBox und gibt auf dem iOS-Gerät die URL `http://fritz.nas` ein. Nachdem der Zugriff durch Eingabe der FritzBox-PIN freigeschaltet ist, erscheint eine Seite, die typischerweise so aussieht:

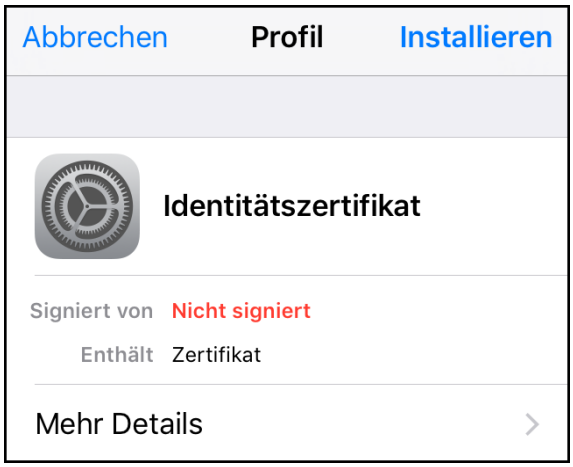


Im vorliegenden Fall ist `TYHOON-MemoryAdapter-01` der Name des USB-Sticks. Ein Klick darauf und dann nochmal auf `vv` zeigt die Schlüsseldateien an:

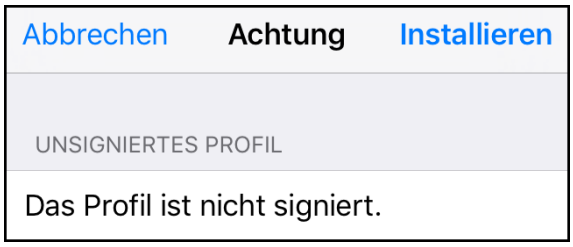


Die drei Dateien tippt man nun der Reihenfolge SIGN-Zertifikat, ENCR-Zertifikat, AUTH-Zertifikat an.

Zunächst `michael@herfert.name [2016-05-31] - SIGN.p12`:



Den anschließenden Hinweis ignoriert man und tippt wieder auf `Installieren`:



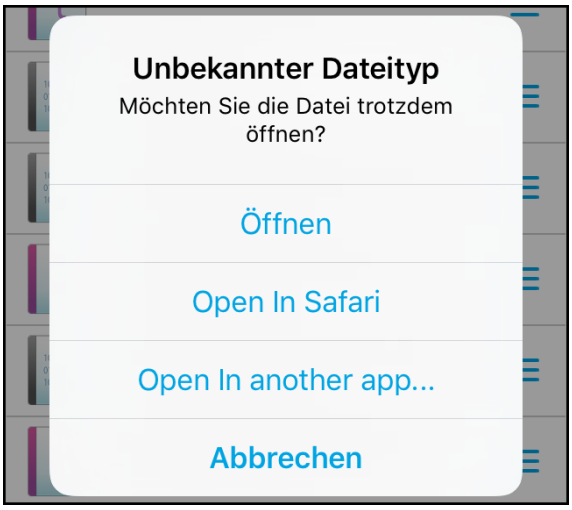
Im folgenden Passwort-Dialog gibt man das Passwort ein, das man in der VV-App für den Export gewählt hat.

Analog verfährt man mit den anderen beiden `p12`-Dateien.

4.2 Import der Schlüssel über einen Samba-Server

Wer in seinem lokalen Netz einen Samba-Server hat, kann die `.p12`-Dateien auch dort ablegen. Um sie unter iOS zu lesen, benötigt man eine App. Eine große Auswahl findet man, indem man im App-Store nach `smb` sucht.

Tippt man eine `.p12`-Datei an, erzeugt der hier verwendete Client eine Anfrage an den Nutzer:



Man wählt `Open in Safari` und verfährt dann so, wie in Abschnitt 4.1 beschrieben.

Bei anderen Clients kann es erforderlich sein, die Dateien erst herunterzuladen, um sie anschließend im Download-Bereich des Clients anzutippen, weil möglicherweise nur dort die Möglichkeit besteht, die Datei mit Safari zu öffnen.

4.3 Import der Schlüssel über eine Windows-Freigabe

Wenn ein Windows-Rechner im Netzwerk ist, kann man das von der VV-App erzeugte ZIP-File auch dort in ein Verzeichnis extrahieren, das man anschließend im Explorer über `Rechte Maustaste|Freigabe` freischaltet. Anschließend verfährt man wie im Abschnitt 4.2 beschrieben. Nach erfolgreichem Import sollte man die Freigabe zurücknehmen.

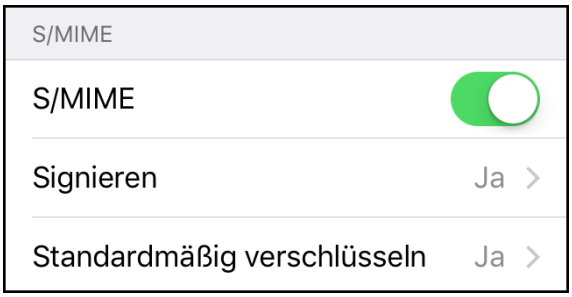
Bei einer Stichprobe von iOS-Samba-Clients hat sich gezeigt, dass viele von ihnen auf einen Samba-Server zugreifen konnten, der Zugriff auf eine Windows-Freigabe aber deutlich weniger Programmen gelang.

4.4 Import der Schlüssel über *Mail*

Der Import der Zertifikate per Mail ist von allen Varianten die gefährlichste, weil man private Schlüssel über das Internet verschickt. Wir raten von diesem Weg ab. Wer ihn dennoch gehen will, muss unbedingt ein sehr langes Passwort wählen. Anschließend werden die `.p12`-Dateien als Mail-Anhang an das iOS-Gerät geschickt. Man tippt sie in Apples *Mail* an, unter Beachtung der in in Abschnitt 4.1 beschriebenen Reihenfolge.

5 Einstellungen für *Mail*

Nun muss noch *Mail* so eingestellt werden, dass die Zertifikate auch benutzt werden. Dazu wählt man zunächst über `Einstellungen|Mail|Accounts` den passenden Account aus, tippt nochmals auf Account und erhält eine Seite, die mit `IMAP-ACCOUNTINFO` beginnt. Ganz unten auf dieser Seite tippt man auf `Erweitert`. Ganz unten dort sieht man nun die S/MIME-Einstellungen:



Man stellt `Signieren` auf `ja` und sieht dann die zur Verfügung stehenden Zertifikate. An den Einstellungen sollte man zunächst nichts ändern. Wenn etwas nicht funktionieren sollte, kann man die Einstellungen gemäß Abschnitt 8 vornehmen.

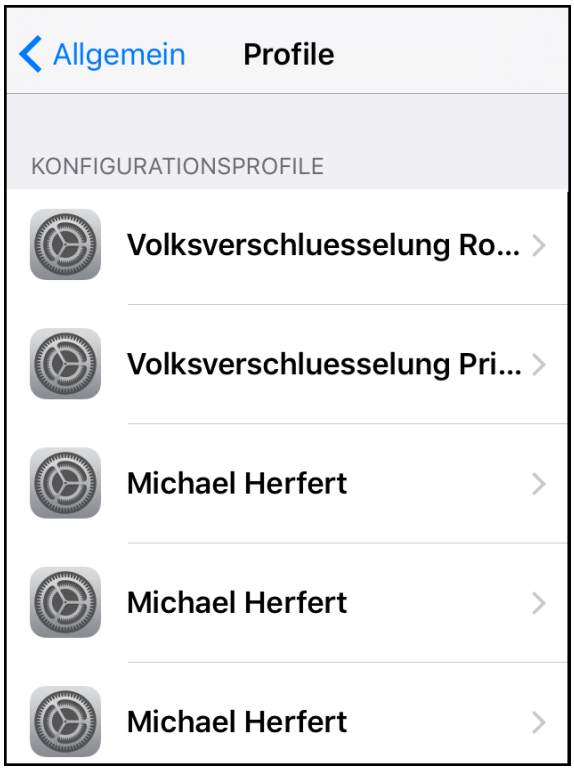
Anschließend stellt man `Standardmäßig verschlüsseln` auch auf `ja` und belässt auch diese Einstellungen in ihrem vorgewählten Zustand.

6 Verschlüsseltes Senden

Wenn Alice eine verschlüsselte Nachricht an Bob senden möchte, benötigt sie dazu Bobs öffentlichen Schlüssel. Mailtools wie Thunderbird holen diesen Schlüssel automatisch aus dem Verzeichnisdienst der Volksverschlüsselung. Leider arbeitet Apples-*Mail* nicht mit Verzeichnisdiensten zusammen, um dort Zertifikate abzuholen. Apple beschreibt unter der URL `https://support.apple.com/de-de/HT202345` wie man dennoch verschlüsselte Nachrichten schicken kann.

7 Erfolgsmessung

1. (**Import**) Den erfolgreichen Import der Schlüssel kann man in den Einstellungen kontrollieren. Unter `Einstellungen|Allgemein|Profile` müssen nun 5 neue Profile zu sehen sein:



2. (**Signieren**) Stellen Sie zunächst in den S/MIME-Optionen (Kapitel 5) den Wert von `Standardmäßig verschlüsseln` auf `nein`. Schicken Sie dann eine Nachricht an sich selbst. Aufgrund der S/MIME-Einstellungen ist diese automatisch signiert. Im Posteingang erscheint diese Mail mit einem Check-Haken am Ende der `Von`-Zeile:

Durch Antippen dieses Haken lassen sich Details zum Zertifikat des Absenders anzeigen. Installieren Sie Ihr eigenes Zertifikat nun so, wie in Kapitel 6 beschrieben. Dieser Schritt ist wichtig, weil Sie sonst nicht für sich selbst verschlüsseln können.

Stellen Sie abschließend in den S/MIME-Optionen (Kapitel 5) den Wert von `Standardmäßig verschlüsseln` wieder auf `ja`.

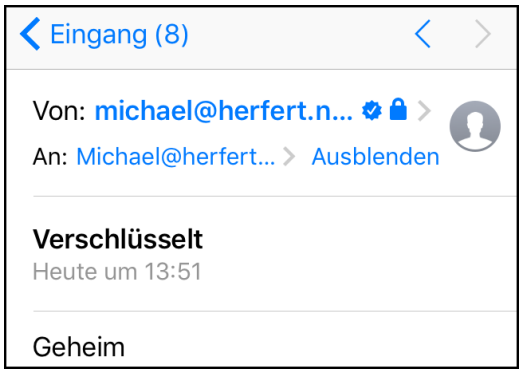
3. (**Entschlüsseln**) Der Erfolg lässt sich in *Mail* testen. Dort findet man eine von `noreply@volksverschluesselung.de` verschickte Nachricht mit dem Betreff `Testnachricht [verschlüsselt]` vor. Diese sollte unmittelbar lesbar sein.

4. (**Verschlüsseln**)

   - Schicken Sie eine verschlüsselte Nachricht an sich selbst. Aufgrund der S/MIME-Einstellungen wird jede Mail automatisch verschlüsselt. iOS signalisiert die Möglichkeit zur Verschlüsselung durch das in blau geschriebene Wort `Verschlüsselt` zwischen `Abbrechen` und `Senden`:

   Sollte eine Verschlüsselung nicht möglich sein, erscheint an gleicher Stelle eine in rot geschriebene Warnung.

   Im Posteingang ist eine verschlüsselte Mail an einem Schloss in der `Von`-Zeile erkennbar:



   Die abgebildete Nachricht ist zusätzlich signiert, daher erscheint auch ein Check-Haken.

   - Bitten Sie einen anderen Teilnehmer der Volksverschlüsselung, Ihnen eine signierte Nachricht zu senden. Verfahren Sie damit

wie in Kapitel 6 beschrieben. Antworten Sie darauf mit einer verschlüsselten Nachricht.

8 Testsystem

Diese Anleitung ist auf den folgenden Systemen getestet worden:

- FritzBox Fon WLAN 7360, FritzOS 06.50
- FritzBox 3370, FritzOS 06.03
- VV-App Release#2 unter Windows 7
- iPhone 5 (A1429), iOS 10.1.1
- iPhone 5S (A1457), iOS 9.3.5
- iPad Air (A1475), iOS 10.0.2
- FileBrowserLite , v8.7 vom 31.08.2016
- smbd 2:4.3.11+dfsg-0ubuntu0.16.04.1 unter ubuntu 16.04

Anhang 1: Signatur des Wurzelzertifikats der Volksverschlüsselung

iOS unterstützt leider keine Fingerabdrücke von Zertifikaten. Um die Authentizität eines Zertifikates zu überprüfen, ist man daher auf die Verifikation der Signatur angewiesen. Sie lässt sich durch `Einstellungen|Allgemein|Profile|Volksverschlüsselung Root CA|Mehr Details|Volksverschlüsselung Root CA` anzeigen. Scrollt man auf dieser Seite ganz nach unten, dann erscheint sie unter der Überschrift `Signatur`. Die Formatierung hängt von Displaygröße und -orientierung des verwendeten iOS-Geräts ab. Die Signatur ist:

```
91 0a ff 51 f3 f4 40 1f 5b 82 75 f7 06 0b d9 f4
e1 e2 82 a0 c8 e5 ab 6f 58 cb 9a 2a 98 7f 87 3c
99 8f 48 0f 28 52 bd 89 c0 69 1e d3 c1 91 c1 4a
cf a6 d1 10 75 49 34 82 b9 fc 4e 00 c8 6f 4e 8b

f8 1d 62 f6 d3 4f 4f 0a ff ff 4f 61 f9 aa 8c 7f
3b 41 99 0e 76 01 36 91 9c fa d4 57 14 a5 5d 2e
d1 17 cf 93 a8 47 65 01 a8 5a d5 b9 a4 84 d7 50
24 90 3e c9 80 8f 1d f1 ca 31 51 fd 2d e0 70 0d

e4 99 86 76 55 e6 c2 fc 27 5b a9 83 36 34 03 b8
75 54 4b 24 b8 d6 dc 61 66 5c 87 e6 d3 10 0e da
a5 17 29 b7 ce d6 e1 80 47 7b 6f 69 79 e6 78 7a
5e d5 f4 9b ef e2 6f 8f 75 30 f9 ef 3a 6a 05 bc

95 2e 87 3a 7d 83 54 26 46 fa 99 b6 ad c3 57 bb
b8 e6 72 c0 34 8b 07 45 ed 54 e3 5b de 4f a4 87
09 2a 37 bf f6 f0 73 fa 18 51 7f 25 28 f6 b1 37
e8 b7 6a c1 9a fb 4b 32 fa 44 42 f1 ab e3 f7 a1

1d 1e d7 3d 6c 5a eb b4 16 da 55 16 71 f8 41 33
c6 47 be 94 86 01 41 0a 51 c1 f3 92 93 5a 44 e6
4e 11 7b 7c e0 66 7c 11 20 8e ce 8b 45 a4 54 b8
63 e8 52 2d 70 bc 2a 06 2b 73 88 b5 fa 5d 6d 14

26 54 c5 9b 7d e6 16 cc 98 09 c6 04 45 c2 aa 0a
1f 43 3e 67 4d 30 07 cc 7d 64 b7 ea ee 24 09 51
29 2d d7 ab 95 7f a9 cc 6d b0 31 e5 fe 09 e0 0a
3a 05 aa da ce db f8 4a e0 84 33 75 09 d6 e7 5d

e2 c4 51 82 d0 f1 e7 07 f7 b8 6b 32 a7 ba f7 33
73 27 0d 73 a7 c2 f1 1d a2 45 fb f2 84 ff e1 c0
5a e7 03 fc a9 7c d6 2e 12 73 07 27 11 a6 3e 91
15 9a 99 00 99 74 e4 2e 8f f5 da a5 09 c6 5d 56

e7 5f cd 53 a2 58 8f 83 57 12 bd 80 62 01 62 25
0b 00 88 73 50 a8 ab da cf d3 ee e5 1f 34 2f 9e
31 bd ae e0 30 dd 77 03 8c 6a 1b eb c8 fc cd cd
42 90 67 87 d5 69 fb 45 4b 7c a7 34 c9 90 d7 31
```