TTKS0600, Encryption Techniques and Systems, Lecture assignment 3

Bordi Tuukka

Lehosvuo Timo

1 Review questions

1.1 Plaintext, Encryption algorithm, Public key, Private key, Ciphertext and Decryption algorithm

1.2 Encryption/Decryption, Digital signature and Key exchange

1.3 A construction which takes an input message and partitions it to fixed-size blocks. These blocks are processed in order and the output of the previous iteration is fed into the next iteration. When all iterations are done the sponge construction return the output, which might vary in length (so output is not fixed in length). The sponge function itself takes three parameters: **f**, which is the internal function which processes the blocks, **r**, which is the bitrate of the input blocks and **pad**, which specifies the padding algorithm used.

1.4 Message digest (hash function), message authentication code, digital signature and message encryption

1.5 All that needs to be done is to remove the existing hash function module and drop in the new module

1.6 Key Distribution Center is a system that is authorized to transmit temporary session keys to principals. Each session key is transmitted in encrypted form, using a master key that the key distribution center shares with the target principal

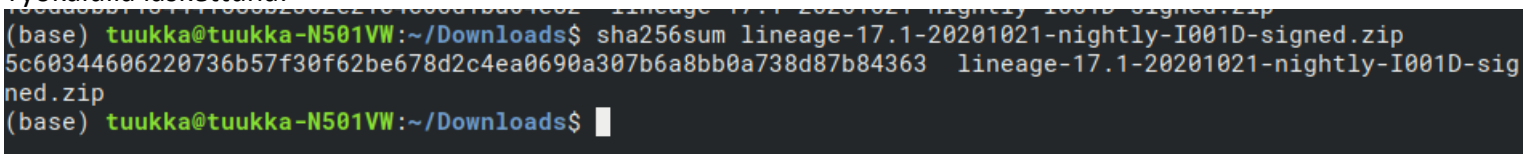
1.7 Public Key Certificate is a certificate that consists of a public key, an identifier of the key owner, and the whole block signed by a Certificate Authority (CA). CA is trusted by the user community for example a government agency or a financial institution. A user can present his or her public key to the authority and obtain a certificate. The user can then publish the certificate. Anyone needing this user's public key can obtain the certificate and verify that it is valid by way of the attached trusted signature.

1.8 The purpose of X.509 is to provide a framework for the provision of authentication services by the X.500 directory to its users. The resulting directory may serve as a repository of public-key certificates.

1.9

Sivuston ilmoittama:

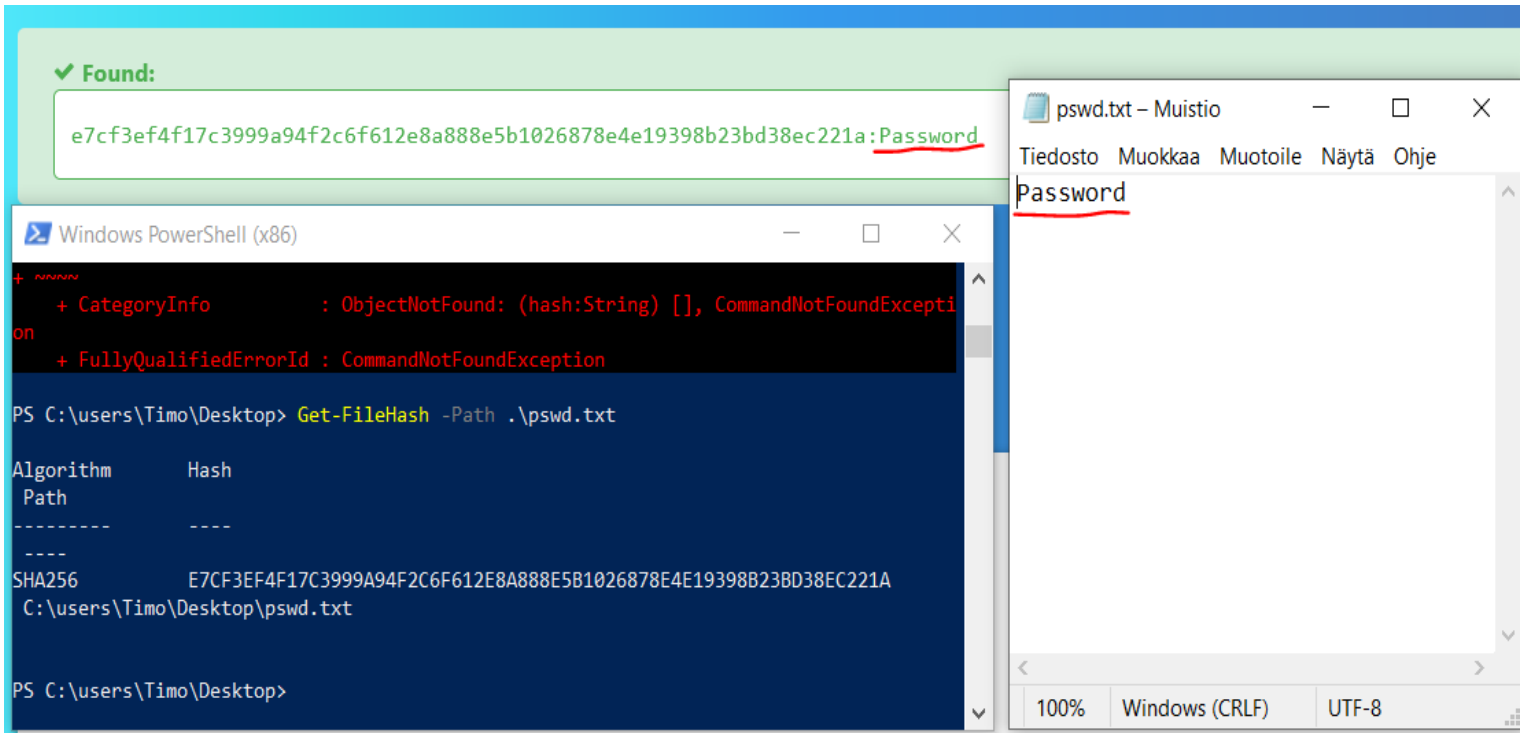
Työkalulla laskettuna:



Täsmäävät!

1.10

Piti käyttää eri sivustoa, kun linkatut sivut eivät toimineet, mutta saimme tiedoston sisällön selvitettyä. Käytimme sivustoa https://hashes.com/en/decrypt/hash.



2 VPN

2.1.1 **VPN-server.crt (2 kuvaa)**

```
  GNU nano 4.8                    VPN-server.crt
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            a9:88:25:50:cf:3c:aa:3e:56:a0:70:73:d8:e3:23:54
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN=VPN-server
        Validity
            Not Before: Oct 25 14:04:29 2020 GMT
            Not After : Oct 10 14:04:29 2023 GMT
        Subject: CN=VPN-server
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:de:ed:f3:13:06:e3:6c:ba:d7:c4:24:de:6b:45:
                    6e:b7:26:9e:d8:2f:39:2d:e9:d0:3e:bb:79:cb:29:
                    1e:fe:b6:a5:ce:db:fd:b8:71:77:1f:d3:1f:d1:7e:
                    f4:51:47:1d:68:87:72:c3:dc:2d:49:6a:ee:10:82:
                    11:04:46:b2:ba:4b:2e:df:0a:79:cd:b7:b0:70:96:
                    00:fc:fd:32:b7:de:64:7c:32:83:f4:81:40:cb:41:
                    ac:7a:73:1d:72:52:6e:64:2b:4e:4e:c6:e5:47:cc:
                    d4:06:1a:6c:d1:97:71:b3:51:2e:38:4a:56:0b:bc:
                    9b:e7:76:f9:d9:6b:e7:f7:d6:b5:1a:c2:ed:2f:3b:
                    e4:9e:bc:e9:e9:7d:56:85:6b:72:74:1e:8f:2c:11:
                    53:96:b4:cd:68:a8:20:45:93:9f:ca:38:df:f7:90:
                    39:be:b8:f1:d7:1f:e8:70:a9:a3:8b:57:a0:4c:16:
                    f0:25:93:e9:cf:8f:2b:f2:16:06:ad:ed:40:4f:2f:
                    f2:87:0b:99:e8:0f:b4:b9:3c:eb:8b:bd:53:9c:fe:
                    31:fe:9d:76:4a:62:63:93:ac:44:af:7f:59:67:28:
                    96:de:d2:8f:e5:bc:8e:29:30:0b:0b:7a:b9:43:f6:
                    a7:b7:6a:be:7d:7f:98:f0:a1:14:80:ba:ec:a0:8c:
                    7b:df
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Subject Key Identifier:
                14:9D:78:2E:55:F9:E9:E4:B5:8E:E7:78:7D:43:0F:22:16:14:1E:57
            X509v3 Authority Key Identifier:
                keyid:15:D1:B0:EA:02:18:A4:72:42:67:2D:D2:05:F5:BE:A5:59:CF:85:>
                DirName:/CN=VPN-server
                serial:48:12:B5:A9:3A:60:59:F8:EC:CF:EB:37:17:2D:E2:8C:94:D4:1B>

^G Get Help   ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos
^X Exit       ^R Read File  ^\ Replace    ^U Paste Text ^T To Spell   ^_ Go To Line
```

```
            X509v3 Extended Key Usage:
                TLS Web Server Authentication
            X509v3 Key Usage:
                Digital Signature, Key Encipherment
            X509v3 Subject Alternative Name:
                DNS:VPN-server
    Signature Algorithm: sha256WithRSAEncryption
         79:25:15:c6:7e:9a:49:20:c5:e4:4b:d3:f0:71:52:3d:6f:5f:
         5a:b7:79:f9:ce:f4:41:a5:e7:6c:2b:88:39:7f:4a:d0:e0:f9:
         45:34:4d:ec:92:a0:83:bf:9a:36:5b:b0:8b:6c:75:88:e4:14:
         26:e8:34:27:04:11:c6:29:6a:33:6b:27:b9:c2:a3:41:c2:62:
         98:cb:45:25:ba:50:b7:52:8d:b5:01:e7:b6:4e:e7:e9:2e:ef:
         da:bc:9f:1c:6c:1d:8a:e1:20:50:c7:83:f4:8f:fb:c3:1a:d9:
         39:0f:be:21:91:14:e8:0c:58:0f:92:2b:b1:aa:3e:f9:d2:d5:
         1c:17:bf:62:cc:24:8c:80:41:84:9c:4c:df:79:58:c4:1f:91:
         b9:a2:7e:3e:fa:97:91:31:4b:98:5f:1b:3f:c6:15:08:14:a6:
         ad:88:d0:09:83:86:9c:fa:b9:09:1e:64:ea:00:25:12:fe:25:
         a3:f7:0e:ec:0e:5d:29:6d:cc:42:a4:f4:0b:8a:dd:25:cb:2b:
         2b:47:e9:f5:10:f0:58:2a:73:4d:fd:01:ae:54:79:2d:46:f2:
         b8:34:e4:f3:11:9f:8f:32:3e:20:33:2b:46:7a:81:27:fd:90:
         e0:25:3a:ca:78:99:05:be:b3:c9:cf:fc:63:69:16:dc:33:a2:
         1f:2f:f8:63
-----BEGIN CERTIFICATE-----
MIIDbjCCAlagAwIBAgIRAKmIJVDPPKo+VqBwc9jjI1QwDQYJKoZIhvcNAQELBQAw
FTETMBEGA1UEAwwKVlBOLXNlcnZlcjAeFw0yMDEwMjUxNDA0MjlaFw0yMzEwMTAx
NDA0MjlaMBUxEzARBgNVBAMMClZQTi1zZXJ2ZXIwggEiMA0GCSqGSIb3DQEBAQUA
A4IBDwAwggEKAoIBAQDe7fMTBuNsutfEJN5rRW63Jp7YLzkt6dA+u3nLKR7+tqXO
2/24cXcf0x/RfvRRRx1oh3LD3C1Jau4QghEERrK6Sy7fCnnNt7BwlgD8/TK33mR8
MoP0gUDLQax6cx1yUm5kK05OxuVHzNQGGmzRl3GzUS44SlYLvJvndvnZa+f31rUa
wu0vO+SevOnpfVaFa3J0Ho8sEVOWtM1oqCBFk5/KON/3kDm+uPHXH+hwqaOLV6BM
FvAlk+nPjyvyFgat7UBPL/KHC5noD7S5POuLvVOc/jH+nXZKYmOTrESvf1lnKJbe
0o/lvI4pMAsLerlD9qe3ar59f5jwoRSAuuygjHvfAgMBAAGjgbgwgbUwCQYDVR0T
BAIwADAdBgNVHQ4EFgQUFJ14LlX56eS1jud4fUMPIhYUHlcwUAYDVR0jBEkwR4AU
FdGw6gIYpHJCZy3SBfW+pVnPhSShGaQXMBUxEzARBgNVBAMMClZQTi1zZXJ2ZXKC
FEgStak6YFn47M/rNxct4oyU1BtQMBMGA1UdJQQMMAoGCCsGAQUFBwMBMAsGA1Ud
DwQEAwIFoDAVBgNVHREEDjAMggpWUE4tc2VydmVyMA0GCSqGSIb3DQEBCwUAA4IB
AQB5JRXGfppJIMXkS9PwcVI9b19at3n5zvRBpedsK4g5f0rQ4PlFNE3skqCDv5o2
W7CLbHWI5BQm6DQnBBHGKWozaye5wqNBwmKYy0UlulC3Uo21Aee2TufpLu/avJ8c
bB2K4SBQx4P0j/vDGtk5D74hkRToDFgPkiuxqj750tUcF79izCSMgEGEnEzfeVjE
H5G5on4++peRMUuYXxs/xhUIFKatiNAJg4ac+rkJHmTqACUS/iWj9w7sDl0pbcxC
pPQLit0lyysR+n1EPBYKnNN/QGuVHktRvK4NOTzEZ+PMj4gMytGeoEn/ZDgJTrK
eJkFvrPJz/xjaRbcM6IfL/hj
-----END CERTIFICATE-----
```

CA.crt (1 kuva)

```
  GNU nano 4.8                          ca.crt
-----BEGIN CERTIFICATE-----
MIIDSDCCAjCgAwIBAgIUSBK1qTpgWfjsz+s3Fy3ijJTUG1AwDQYJKoZIhvcNAQEL
BQAwFTETMBEGA1UEAwwKVlBOLXNlcnZlcjAeFw0yMDEwMjUxNDAzNDJaFw0zMDEw
MjMxNDAzNDJaMBUxEzARBgNVBAMMClZQTi1zZXJ2ZXIwggEiMA0GCSqGSIb3DQEB
AQUAA4IBDwAwggEKAoIBAQDhmEQ30ixrGRei+vC5iW5MwQPySV2rlxUK+D0Cd/c6
HO1i+ZmWSC2jezXGH0ixDpsIFh4gx5W6ou4JWOsrosnol22le8urxZUkQuiFj81c
ORrfL77zIavD0pR//q+YcfpAXb30CTKt4vYX/GkZ3L1Wct6rwjHNfTQ1gsIshSDr
PMKxoX0IgiRE+1tRESnA84/TUQytiX13I43nQ0Z11XEij1uFMbudW8VngOSwlE7T
6ZsegsDddqILIjPCsaEDcrnyBTbi00dWw8JzSvG2en38yDkyRbEdTTs0gXZeM3gC
o/7RZjc479S99+3/flvYM0f2iqjlJWK3Xb4eaaGs2lTJAgMBAAGjgY8wgYwwHQYD
VR0OBBYEFBXRsOoCGKRyQmct0gX1vqVZz4UkMFAGA1UdIwRJMEeAFBXRsOoCGKRy
Qmct0gX1vqVZz4UkoRmkFzAVMRMwEQYDVQQDDApWUE4tc2VydmVyghRIErWpOmBZ
+OzP6zcXLeKMlNQbUDAMBgNVHRMEBTADAQH/MAsGA1UdDwQEAwIBBjANBgkqhkiG
9w0BAQsFAAOCAQEAn6m9S2n/g7IDvmCmoIz2N7YOYYgJ4ZP7sW6TiZzbSEy6UD6Z
JXQfa1ivFTrhxLLT1LfC0LhqSK+OH527iDCxwne5kRaMcJ7JWQ0FdizvZqaQkVjd
rTozMCDofj+FQAV4QjVLvH4UFJLP84KcL712zJejMv2HZhZk14s7YwKAktRbu7pF
5SSV1W2M/r+IAsxGUu9FEV7ZtliXDNGk0P2pDLsomJHZieHE+J4divpHuBG99QPv
VwJfk7P+YOc0i9PmTZiMeWlyguW78fh0/xLI/2yDu9rare7fecP1a+Wgl4VISXOc
Lu/96I1gKLtLmYTHLY7mjkpVWoaIkSEUqV9GEw==
-----END CERTIFICATE-----

^G Get Help   ^O Write Out ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos
^X Exit       ^R Read File ^\ Replace    ^U Paste Text^T To Spell   ^_ Go To Line
```

VPN-client.crt eli tehtävänannon VPN-client1.crt (2 kuvaa)

```
  GNU nano 4.8                    VPN-client.crt
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            bd:22:f4:3d:91:6d:8c:67:24:f7:c3:3f:5b:d4:6c:d7
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN=VPN-server
        Validity
            Not Before: Oct 25 14:09:41 2020 GMT
            Not After : Oct 10 14:09:41 2023 GMT
        Subject: CN=VPN-client
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:b7:e4:37:db:c1:85:3a:4d:b5:33:d0:3f:00:85:
                    cd:d9:75:c6:9e:d3:24:eb:16:2b:04:75:61:c6:53:
                    4b:9e:17:ed:21:ea:d8:11:93:cf:f5:f5:e2:3f:6e:
                    31:64:6c:0f:1d:c5:23:50:fa:33:5b:6a:3d:70:d5:
                    b2:fc:d6:97:99:48:97:2a:04:65:40:ac:6d:02:e1:
                    24:20:39:f8:9f:45:c6:37:9f:30:51:fb:6a:1c:a1:
                    b8:bb:86:27:88:47:c6:e3:5d:42:ea:70:f9:13:a8:
                    c8:d9:6d:37:20:49:dd:15:da:4a:c1:c8:bb:45:c5:
                    2a:37:76:e8:4f:49:93:d5:7d:71:f6:32:36:0a:93:
                    64:af:94:03:dc:40:4f:7d:13:12:08:b4:36:21:37:
                    f6:1e:d6:59:0d:34:1b:a7:be:b6:42:e0:28:20:9d:
                    26:d8:f4:66:13:4d:f6:01:6a:c2:45:26:37:07:20:
                    09:98:c4:a1:2d:7a:81:9d:7c:2b:57:a3:2f:7a:03:
                    e2:72:fc:4c:d3:e2:c1:e7:2b:da:6e:e3:67:92:3e:
                    8e:96:01:c8:f6:a2:76:64:b8:eb:a7:a9:85:7f:43:
                    da:f6:bc:2b:78:09:ce:90:4d:01:5c:b1:57:77:02:
                    4e:9d:0a:87:c3:93:d5:b8:15:0f:01:63:1b:98:43:
                    31:a5
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Subject Key Identifier:
                40:A5:E9:99:5F:7D:81:B8:05:96:4F:34:6E:A3:ED:75:F4:C3:75:27
            X509v3 Authority Key Identifier:
                keyid:15:D1:B0:EA:02:18:A4:72:42:67:2D:D2:05:F5:BE:A5:59:CF:85:>
                DirName:/CN=VPN-server
```

```
  GNU nano 4.8                    VPN-client.crt
                serial:48:12:B5:A9:3A:60:59:F8:EC:CF:EB:37:17:2D:E2:8C:94:D4:1B>

            X509v3 Extended Key Usage:
                TLS Web Client Authentication
            X509v3 Key Usage:
                Digital Signature
    Signature Algorithm: sha256WithRSAEncryption
         c1:67:d0:3c:48:ca:0b:71:e7:1d:dc:6d:e6:18:af:c9:a0:07:
         04:3c:c3:39:b2:1d:ec:77:7f:97:ff:c9:d5:3a:63:4d:1e:ef:
         e6:c3:fc:a3:83:9b:25:0e:cd:50:0b:7f:d6:f7:f7:cc:8f:24:
         6a:ca:49:f0:75:a5:32:97:d2:06:d9:97:ae:47:ee:60:a1:34:
         40:27:81:3f:74:69:4f:77:57:27:da:89:5f:d6:57:93:6d:9e:
         62:e4:62:a0:37:e0:75:b5:08:8e:88:7d:ce:df:29:87:ee:e5:
         79:23:42:ce:6d:50:c9:ac:2f:78:3f:ac:4b:e2:ca:fb:21:b3:
         0b:69:c4:fc:76:cd:10:be:c2:4e:cd:1d:df:b9:ce:88:2b:96:
         04:90:83:a5:b0:de:ad:8a:80:3c:56:b2:18:a7:ce:ec:cb:54:
         a5:4f:86:5b:0d:f8:21:df:1a:f5:1f:49:f3:98:3e:7e:fa:a2:
         92:a6:37:7c:16:92:11:8f:72:69:28:86:95:af:98:ab:7d:75:
         ee:ed:99:44:fc:de:8f:c3:60:ba:5c:3d:d9:9f:7a:89:58:40:
         2a:93:21:33:d8:7e:a0:5b:4b:c2:93:c1:81:31:3e:a4:a3:7e:
         b8:63:65:31:3e:c1:9d:d8:6f:d6:1f:7d:0f:9d:3f:a8:7a:1c:
         18:36:9f:e3
-----BEGIN CERTIFICATE-----
MIIDVzCCAj+gAwIBAgIRAL0i9D2RbYxnJPfDP1vUbNcwDQYJKoZIhvcNAQELBQAw
FTETMBEGA1UEAwwKVlBOLXNlcnZlcjAeFw0yMDEwMjUxNDA5NDFaFw0yMzEwMTAx
NDA5NDFaMBUxEzARBgNVBAMMClZQTi1jbGllbnQwggEiMA0GCSqGSIb3DQEBAQUA
A4IBDwAwggEKAoIBAQC35DfbwYU6TbUz0D8Ahc3Zdcae0yTrFisEdWHGU0ueF+0h
6tgRk8/19eI/bjFkbA8dxSNQ+jNbaj1w1bL81peZSJcqBGVArG0C4SQgOfifRcY3
nzBR+2ocobi7hieIR8bjXULqcPkTqMjZbTcgSd0V2krByLtFxSo3duhPSZPVfXH2
MjYKk2SvlAPcQE99ExIItDYhN/Ye1lkNNBunvrZC4CggnSbY9GYTTfYBasJFJjcH
IAmYxKEteoGdfCtXoy96A+Jy/EzT4sHnK9pu42eSPo6WAcj2onZkuOunqYV/Q9r2
vCt4Cc6QTQFcsVd3Ak6dCofDk9W4FQ8BYxuYQzGlAgMBAAGjgaEwgZ4wCQYDVR0T
BAIwADAdBgNVHQ4EFgQUQKXpmV99gbgFlk80bqPtdfTDdScwUAYDVR0jBEkwR4AU
FdGw6gIYpHJCZy3SBfW+pVnPhSShGaQXMBUxEzARBgNVBAMMClZQTi1zZXJ2ZXKC
FEgStak6YFn47M/rNxct4oyU1BtQMBMGA1UdJQQMMAoGCCsGAQUFBwMCMAsGA1Ud
DwQEAwIHgDANBgkqhkiG9w0BAQsFAAOCAQEAwWfQPEjKC3HnHdxt5hivyaAHBDzD
ObId7Hd/l//J1TpjTR7v5sP8o4ObJQ7NUAt/1vf3zI8kaspJ8HWlMpfSBtmXrkfu
YKE0QCeBP3RpT3dXJ9qJX9ZXk22eYuRioDfgdbUIjoh9zt8ph+7leSNCzm1Qyawv
eD+sS+LK+yGzC2nE/HbNEL7CTs0d37nOiCuWBJCDpbDerYqAPFayGKfO7MtUpU+G
Ww34Id8a9R9J85g+fvqikqY3fBaSEY9yaSiGla+Yq3117u2ZRPzej8Ngulw92Z96
iVhAKpMhM9h+oFtLwpPBgTE+pKN+uGNlMT7Bndhv1h99D50/qHocGDaf4w==
-----END CERTIFICATE-----
```

Erot:

VPN-server.crt on siitä erilainen, että sillä voidaan enkryptoida avaimia, jotka voi näin lähettää clientille (kts. Key Usage -kenttä sertifikaatista). Kun molemmilla on tämä avain, voidaan muodostaa salattu yhteys osapuolien välillä. VPN-client.crt:n avulla voi pelkästään tunnistautua (Client Authentication), eikä sillä voi enkryptata avaimia tai mitään muutakaan. VPN-server.crt:n yksi käyttötavoista on TLS Web server Authentication, eli sillä palvelin voi tunnistautua TLS-palvelimeksi, eli tämäkin ero sertifikaateilla on.

Traceroute:

```
user@client-VirtualBox:~/Desktop$ sudo traceroute google.com -i tun0
[sudo] password for user:
traceroute to google.com (216.58.211.14), 30 hops max, 60 byte packets
 1  10.8.0.1 (10.8.0.1)  0.972 ms  2.287 ms  2.214 ms
 2  10.0.2.1 (10.0.2.1)  2.133 ms  2.043 ms  1.956 ms
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
user@client-VirtualBox:~/Desktop$
```

Kuva 1: Jouduimme käyttämään NAT:in sijaan NAT networkia, jonka takia ip-osoite on 10.0.2.1. Syytä emme tiedä minkä takia tämä ei toiminut NATilla

Jännää, että ei saada mitään väliaikatietoja. Jos tekee saman komennon host-koneella (jossa pyörii Virtualbox), niin se toimii oletetunlaisesti. Kuitenkin google.com vastaa VPN-clientin pingiin:

```
user@client-VirtualBox:~/Desktop$ ping google.com -I tun0
PING google.com (216.58.211.14) from 10.8.0.6 tun0: 56(84) bytes of data.
64 bytes from arn09s20-in-f14.1e100.net (216.58.211.14): icmp_seq=1 ttl=113 time
=40.0 ms
64 bytes from arn09s20-in-f14.1e100.net (216.58.211.14): icmp_seq=2 ttl=113 time
=71.6 ms
64 bytes from arn09s20-in-f14.1e100.net (216.58.211.14): icmp_seq=3 ttl=113 time
=68.3 ms
64 bytes from arn09s20-in-f14.1e100.net (216.58.211.14): icmp_seq=4 ttl=113 time
=39.1 ms
^C
--- google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 39.103/54.746/71.627/15.261 ms
user@client-VirtualBox:~/Desktop$
```

2.2 Capture 1:ssä liikenne sivustolle oli salaamatonta. Esimerkiksi pystyimme näkemään haetun sivuston sisällön:

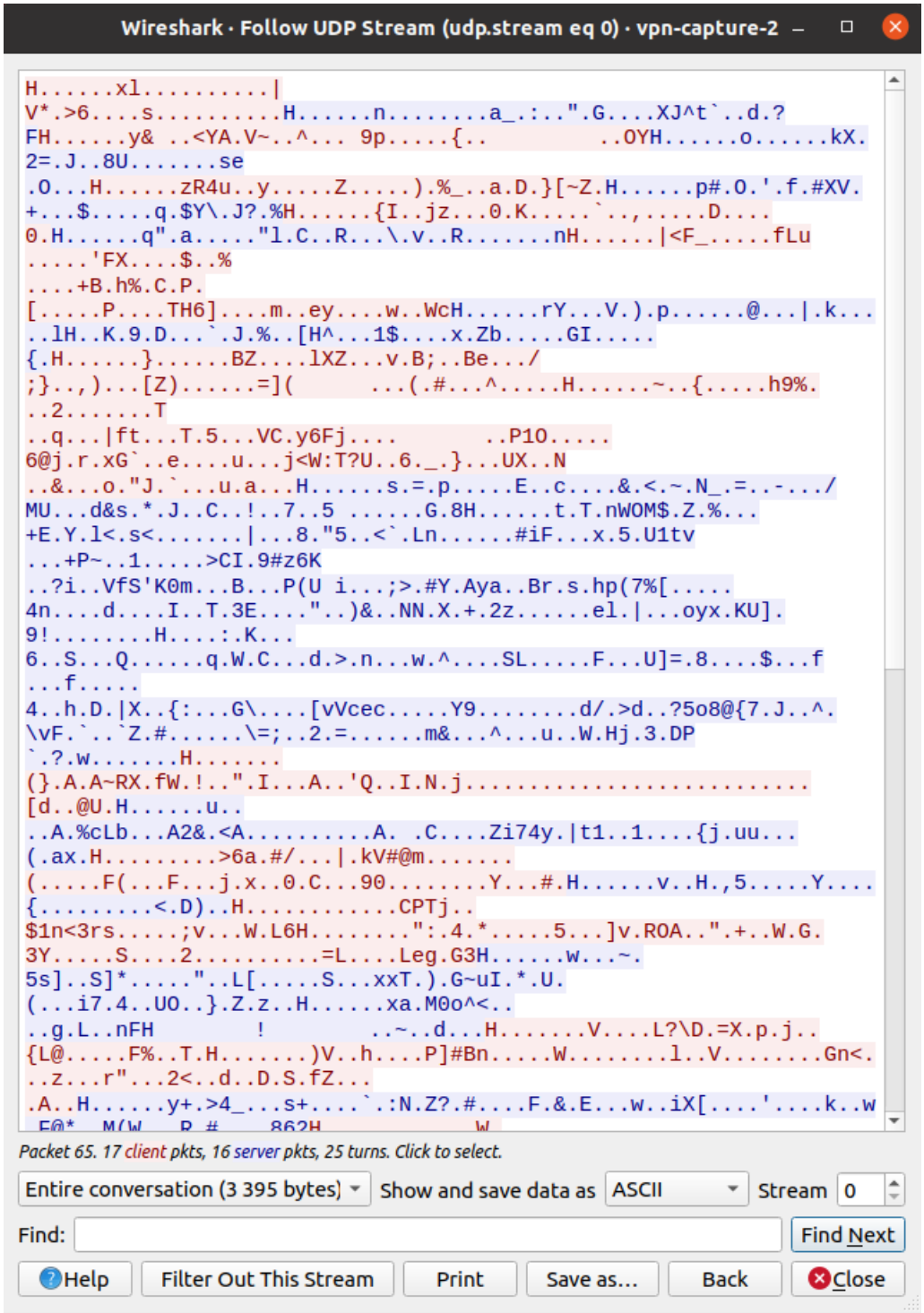
Wireshark · Follow TCP Stream (tcp.stream eq 11) · vpn-capture-1

```
GET / HTTP/1.1
Host: 192.168.2.2
Accept-Encoding: identity

HTTP/1.1 200 OK
Date: Sun, 25 Oct 2020 14:42:51 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Sun, 25 Oct 2020 14:39:21 GMT
ETag: "6e-5b27fc7859249"
Accept-Ranges: bytes
Content-Length: 110
Vary: Accept-Encoding
Content-Type: text/html

<!DOCTYPE html>
<html>
<body>
        <b>Hello! Simple site is working!<br></b>
        <p>...Or is it?</p>
</body>
</html>
```

Capture 2:ssa ei tätä pystynyt tekemään. Näkyi vain tällaista:



Pääsisältö capture 1:ssä oli mielestämme salaamaton tcp-yhteys verkkosivustoihin, joka löytyy seuraavasta kuvasta:

No.	Time	Source	Destination	Protocol	Length	Info
104	51.742539	192.168.2.2	192.168.1.101	ICMP	118	Destination unreachable (Network unreachable)
105	51.742866	192.168.1.101	8.8.8.8	DNS	101	Standard query 0xd8f9 A incoming.telemetry.mozilla.org OPT
106	51.742867	192.168.1.101	8.8.4.4	TCP	74	47456 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T…
107	52.766433	192.168.1.101	192.168.2.2	TCP	74	43104 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T…
108	52.766872	192.168.2.2	192.168.1.101	TCP	74	80 → 43104 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SA…
109	52.767307	192.168.1.101	192.168.2.2	TCP	66	43104 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3091339920…
110	52.767544	192.168.1.101	192.168.2.2	HTTP	130	GET / HTTP/1.1
111	52.767878	192.168.2.2	192.168.1.101	TCP	66	80 → 43104 [ACK] Seq=1 Ack=65 Win=65152 Len=0 TSval=488405498…
112	52.768919	192.168.2.2	192.168.1.101	HTTP	427	HTTP/1.1 200 OK (text/html)
113	52.769313	192.168.1.101	192.168.2.2	TCP	66	43104 → 80 [ACK] Seq=65 Ack=362 Win=64128 Len=0 TSval=3091339…
114	52.770444	192.168.1.101	8.8.4.4	TCP	74	[TCP Retransmission] 47456 → 53 [SYN] Seq=0 Win=64240 Len=0 M…
115	54.786390	192.168.1.101	8.8.4.4	TCP	74	[TCP Retransmission] 47456 → 53 [SYN] Seq=0 Win=64240 Len=0 M…
116	54.786831	192.168.2.2	192.168.1.101	ICMP	102	Destination unreachable (Network unreachable)
117	54.787284	192.168.1.101	8.8.4.4	TCP	74	47460 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T…
118	55.810435	192.168.1.101	8.8.4.4	TCP	74	[TCP Retransmission] 47460 → 53 [SYN] Seq=0 Win=64240 Len=0 M…
119	56.992582	192.168.1.101	8.8.8.8	DNS	101	Standard query 0x47e3 AAAA incoming.telemetry.mozilla.org OPT
120	57.771751	192.168.2.2	192.168.1.101	TCP	66	80 → 43104 [FIN, ACK] Seq=362 Ack=65 Win=65152 Len=0 TSval=48…
121	57.814568	192.168.1.101	192.168.2.2	TCP	66	43104 → 80 [ACK] Seq=65 Ack=363 Win=64128 Len=0 TSval=3091344…
122	57.826403	192.168.1.101	8.8.4.4	TCP	74	[TCP Retransmission] 47460 → 53 [SYN] Seq=0 Win=64240 Len=0 M…
123	59.258354	192.168.2.2	192.168.1.101	OpenVPN	82	MessageType: P_DATA_V2
124	59.258771	192.168.1.101	192.168.2.2	OpenVPN	82	MessageType: P_DATA_V2
125	61.890546	192.168.1.101	8.8.4.4	TCP	74	[TCP Retransmission] 47460 → 53 [SYN] Seq=0 Win=64240 Len=0 M…
126	61.891144	192.168.2.2	192.168.1.101	ICMP	102	Destination unreachable (Network unreachable)
127	61.891988	192.168.1.101	8.8.8.8	DNS	101	Standard query 0xd8f9 A incoming.telemetry.mozilla.org OPT
128	61.892228	192.168.1.101	8.8.4.4	TCP	74	47462 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T…
129	61.892452	192.168.2.2	192.168.1.101	ICMP	129	Destination unreachable (Network unreachable)
130	61.892924	192.168.1.101	8.8.8.8	DNS	101	Standard query 0xd8f9 A incoming.telemetry.mozilla.org OPT

Pääsisältö Capture 2:ssa oli DNS-pyynnöt ja OpenVPN –liikenne, joka näkyy seuraavasta kuvasta:

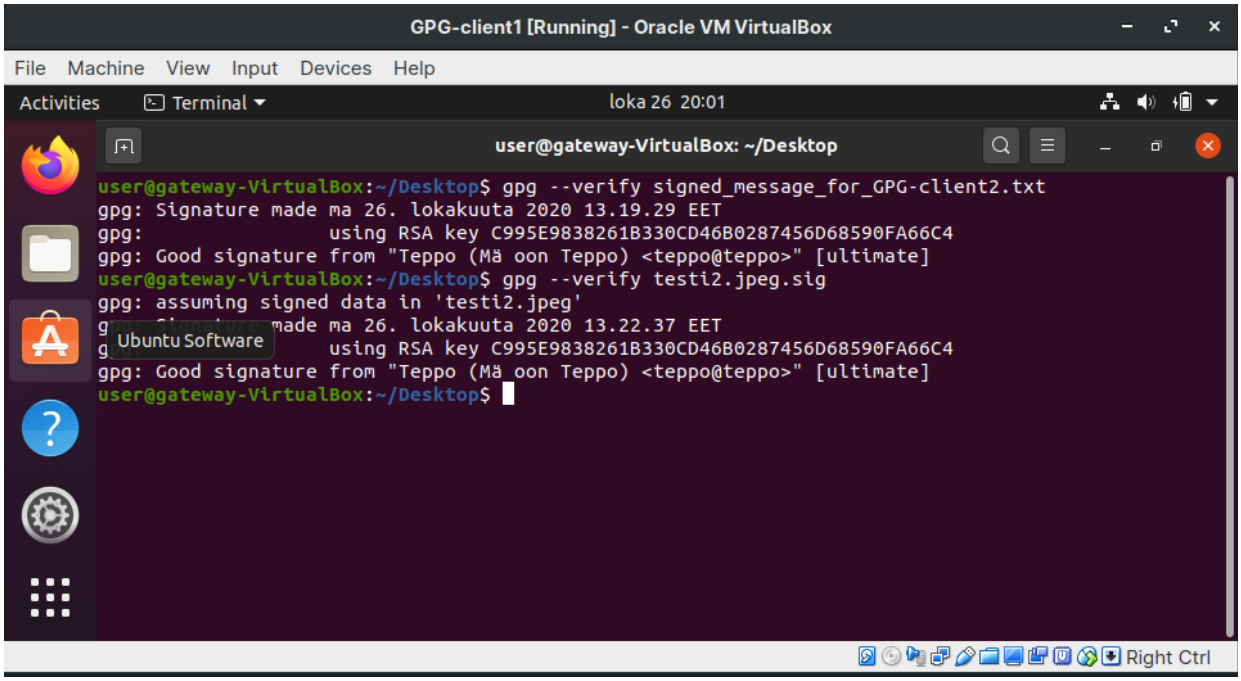
No.	Time	Source	Destination	Protocol	Length	Info
75	33.921670	192.168.1.101	8.8.8.8	DNS	101	Standard query 0x17ea AAAA incoming.telemetry.mozilla.org OPT
76	34.469578	192.168.1.101	8.8.4.4	DNS	87	Standard query 0xa240 AAAA services.addons.mozilla.org
77	34.943677	192.168.1.101	8.8.4.4	TCP	74	[TCP Retransmission] 47500 → 53 [SYN] Seq=0 Win=64240 Len=0 M…
78	35.957067	192.168.2.2	192.168.1.101	OpenVPN	82	MessageType: P_DATA_V2
79	36.959558	192.168.1.101	8.8.4.4	TCP	74	[TCP Retransmission] 47500 → 53 [SYN] Seq=0 Win=64240 Len=0 M…
80	36.991642	192.168.1.101	13.33.240.122	TLSv1.2	482	Application Data
81	37.217388	192.168.1.101	192.168.2.2	OpenVPN	126	MessageType: P_DATA_V2
82	37.217949	192.168.2.2	192.168.1.101	OpenVPN	126	MessageType: P_DATA_V2
83	37.218371	192.168.1.101	192.168.2.2	OpenVPN	118	MessageType: P_DATA_V2
84	37.218523	192.168.1.101	192.168.2.2	OpenVPN	179	MessageType: P_DATA_V2
85	37.219190	192.168.2.2	192.168.1.101	OpenVPN	118	MessageType: P_DATA_V2
86	37.220758	192.168.2.2	192.168.1.101	OpenVPN	479	MessageType: P_DATA_V2
87	37.221180	192.168.1.101	192.168.2.2	OpenVPN	118	MessageType: P_DATA_V2
88	37.427696	192.168.1.101	8.8.4.4	DNS	90	Standard query 0xe4f9 AAAA incoming.telemetry.mozilla.org
89	38.924711	PcsCompu_7b:c4:2a	PcsCompu_b8:58:7a	ARP	42	Who has 192.168.1.101? Tell 192.168.1.1
90	38.925108	PcsCompu_b8:58:7a	PcsCompu_7b:c4:2a	ARP	60	192.168.1.101 is at 08:00:27:b8:58:7a
91	38.972799	192.168.1.101	8.8.8.8	DNS	100	Standard query 0xfcc9 AAAA connectivity-check.ubuntu.com OPT
92	38.972920	192.168.1.101	8.8.4.4	DNS	90	Standard query 0x5e5b A incoming.telemetry.mozilla.org
93	38.973181	192.168.2.2	192.168.1.101	ICMP	128	Destination unreachable (Network unreachable)
94	38.973522	192.168.1.101	8.8.8.8	DNS	100	Standard query 0xfcc9 AAAA connectivity-check.ubuntu.com OPT
95	39.719270	192.168.1.101	8.8.4.4	DNS	87	Standard query 0xa240 AAAA services.addons.mozilla.org
96	40.716696	fe80::a00:27ff:fe7b…	ff02::2	ICMPv6	70	Router Solicitation from 08:00:27:7b:c4:2a
97	41.087709	192.168.1.101	8.8.4.4	TCP	74	[TCP Retransmission] 47500 → 53 [SYN] Seq=0 Win=64240 Len=0 M…
98	42.222457	192.168.2.2	192.168.1.101	OpenVPN	118	MessageType: P_DATA_V2
99	42.263664	192.168.1.101	192.168.2.2	OpenVPN	118	MessageType: P_DATA_V2
100	42.432236	192.168.1.101	8.8.8.8	DNS	101	Standard query 0xe4f9 AAAA incoming.telemetry.mozilla.org OPT
101	42.495700	192.168.1.101	8.8.8.8	DNS	87	Standard query 0x0cf6 A aus5.mozilla.org OPT
102	42.495928	192.168.1.101	8.8.8.8	DNS	87	Standard query 0x6457 AAAA aus5.mozilla.org OPT
103	44.219361	192.168.1.101	8.8.8.8	DNS	101	Standard query 0x5e5b A incoming.telemetry.mozilla.org OPT
104	44.219768	192.168.2.2	192.168.1.101	ICMP	129	Destination unreachable (Network unreachable)
105	44.220209	192.168.1.101	8.8.4.4	TCP	74	47504 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T…
106	44.969474	192.168.1.101	8.8.8.8	DNS	98	Standard query 0xa240 AAAA services.addons.mozilla.org OPT
107	45.247806	192.168.1.101	8.8.4.4	TCP	74	[TCP Retransmission] 47504 → 53 [SYN] Seq=0 Win=64240 Len=0 M…
108	47.265065	192.168.1.101	8.8.4.4	TCP	74	[TCP Retransmission] 47504 → 53 [SYN] Seq=0 Win=64240 Len=0 M…

Eli ero captureitten välillä oli se, että kaikki HTTP-liikenne oli salattua capture 2:ssa vrt. Capture 1.

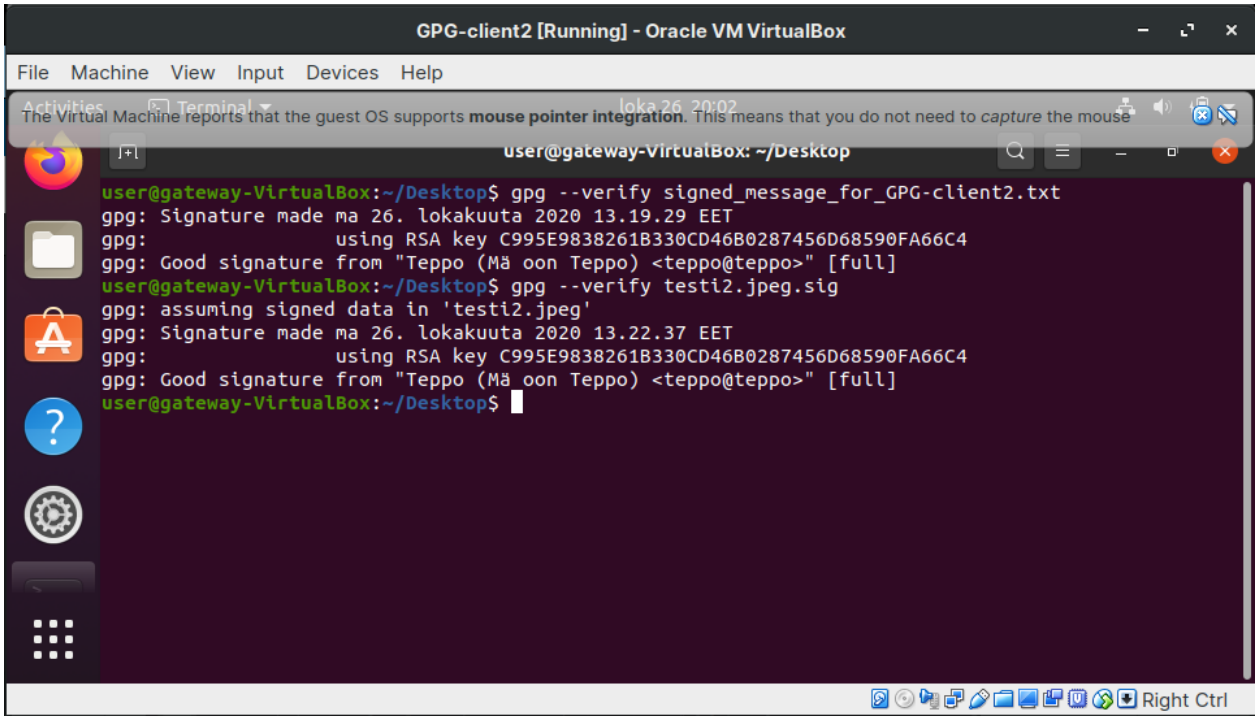
3 GPG

3.1

GPG-client1 (kloonattu gateway, siksi sama user & hostname molemmissa kuvissa):



GPG-client2:



3.2 Tämä tehdään komennolla gpg –edit-key <s-posti tai key-id> ja kirjoittamalla valinnaksi **trust** ja valitsemalla itselle oikealta tuntuva vaihtoehto valinnoista. Seuraavat kuvat havainnollistavat asian:

```
user@gateway-VirtualBox:~/Desktop$ gpg --edit-key teppo@teppo
gpg (GnuPG) 2.2.19; Copyright (C) 2019 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.


pub  rsa3072/7456D68590FA66C4
     created: 2020-10-25  expires: 2021-03-26  usage: SC
     trust: never         validity: full
sub  rsa3072/124B60CAB63DCC56
     created: 2020-10-25  expires: 2021-03-26  usage: E
[  full  ] (1). Teppo (Mä oon Teppo) <teppo@teppo>

gpg> trust
```

```
gpg> trust
pub  rsa3072/7456D68590FA66C4
     created: 2020-10-25  expires: 2021-03-26  usage: SC
     trust: never         validity: full
sub  rsa3072/124B60CAB63DCC56
     created: 2020-10-25  expires: 2021-03-26  usage: E
[  full  ] (1). Teppo (Mä oon Teppo) <teppo@teppo>

Please decide how far you trust this user to correctly verify other users' keys
(by looking at passports, checking fingerprints from different sources, etc.)

  1 = I don't know or won't say
  2 = I do NOT trust
  3 = I trust marginally
  4 = I trust fully
  5 = I trust ultimately
  m = back to the main menu

Your decision? 1
```

```
Your decision? 1

pub  rsa3072/7456D68590FA66C4
     created: 2020-10-25  expires: 2021-03-26  usage: SC
     trust: undefined     validity: full
sub  rsa3072/124B60CAB63DCC56
     created: 2020-10-25  expires: 2021-03-26  usage: E
[  full  ] (1). Teppo (Mä oon Teppo) <teppo@teppo>
Please note that the shown key validity is not necessarily correct
unless you restart the program.

gpg>
```

3.3 **Avaimien tuonti:**

Valitse Key Management osiosta File → Import keys from file. Valitse ASC tiedosto (julkinen avain), jonka olet saanut toiselta henkilöltä joko sähköpostilla tai muuta kautta (tai lisätäksesi oman avainparin). Enigmail lisää tämän avaimen avainnippuusi.

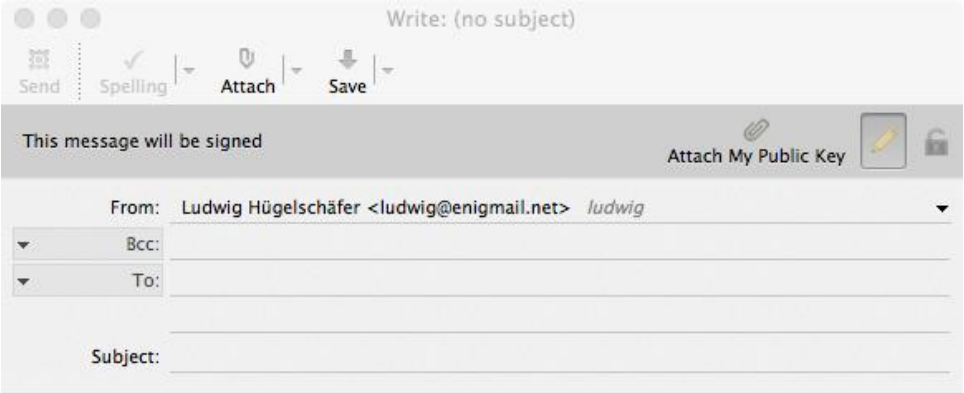
Toinen tapa lisätä toisen henkilön julkinen avain avainnippuusi on ladata se julkiselta avainpalvelimelta. Valitse Keyserver → Search for keys ja valitse hakutermi, jolla haluat etsiä avainta. Avainpalvelin palauttaa listan avaimista, jotka täsmäävät hakutermeihin. Valitse tuotava avain ruksimalla laatikko avaimen vasemmalla puolella ja Enigmail tuo avaimen avainnippuusi.

Viestien salaus:

Kirjoita viesti. Valitse vaihtoehto "Encrypt message" ennen lähetystä. Varmista, että lukon kuva on päällä, eli kellertävä . Tämän jälkeen valitse aukenevasta listasta haluamasi vastaanottajan julkinen avain ja valitse "send".

Viestien allekirjoittaminen:

Viestin kirjoitusosiossa on työkalurivi, jossa on kynän kuva, (alla oleva kuva, kuvat osoitteesta https://enigmail.net/index.php/en/user-manual/signature-and-encryption):



Viesti tullaan allekirjoittamaan, jos kynä on keltainen ( )

Viestiä ei allekirjoiteta, jos kynä on tummanharmaa ( )

Kun lähetät viestin, sinulta tullaan kysymään yksityisen avaimesi salasana.

3.4 Allekirjoitus varmistaa, että viesti on sinun lähettämäsi. Se on eräänlainen alkuperätodistus viestille. Tämä myös takaa sen, että se mitä lähetit tuli sinulta, etkä voi enää jälkeenpäin kumota sitä, että viesti tuli sinulta.

General comments about assignment

- Tehtiin kaikki työt kahdestaan
- Tehtävä oli työläs
- Aikaa meni noin 1.5 päivää
- Shared folder ei toiminut ilman root oikeuksia
- Muutama ohjeen komennoista oli väärin tai puuttui parametrejä (en muista mitkä 😊)
- Jossakin easyrsa komennosssa conf tiedoston piti olla eri paikassa kuin ohjeissa
- Osassa gpg komennoissa piti olla tarkkana, ettei käytä ”sudo” komentoa tai hommat eivät toimi