SSH key file formats HW

Author: Prompt Eua-anant

Private Key

Hypothesis: key info → DER encoding → PEM (Base64) → result below

-----BEGIN RSA PRIVATE KEY-----
MIIG5AIBAAKCAYEA5erdtoTLq3fidLF2/UTpnTPkbfFUW5iT90Zskp3Jfj5/aKbY
wXTcrKdfRQI0IR1jNHFwz9eHvmjmT3Mz9b8DF7o5KcUfh3uFXSum38FWZ79seFK9
TaN/6QW+IQk85ZM9o4buCvGWtFVbxKJSZJNTJ5dACBpEBsF0GEhBjGemk6FttUra
mOYE2VUiqhg5CgcdGNPmEGAqOCclXRHcgmy8VFZeMtFoBwdWH9HW9y19UXIhtr4N
BIA2kUat5/bE7hN04S7svxsOWKhaQhI9+kcJPiW6JoBm+qYECAudnCNBnjLRsxlR
g0Drysu1RApERtrof3VBHnuMngnxgwXDQ1VadSEWtw6i753ZI9NuMUsyrZpQZhYV
mLyiKJJrMI4Lphz6WVdm9kCSgxdx9L5ZeWZthGrNpXjizsLDFFtD2txJwz53PJeE
zCwc0/AvsTASuvZvTUg138gt744jmip7F17hZlaShr5fA8StrLsFi8XYx6Rx2NlT
6o6FN/U3nQ1gcJc9AgMBAAECggGAMiV10hdIrM9rDvSd9UOQiH8G9YvLUGcI7sfn
alsL1YMgGt05LYilkOq4dr6yS/6y4n9TkaF6s+cBRJbl4FWXARfW2+toow4n2lho
/yiWBe7UY7H4I/TjMxnTjDUNmSzyJraJOM3UhuSPLWYR/mm7m0j76EiCSc7r2Vf5
I/x/cnelDAOVhf+1Uwmkk+DQoAVJLV8aMLwouTKgjZoVtESvFt33kbHmtJG/ERWd
gy/iw17XR5pQEIk+XZVC3PMPpLWNQKcEdxFC4tUHADYNkOcA/TT+y0D+AfgouHEx
BtD7YEQ0JyZacSwxH4mOhIlycrOCQLuzVVAeF8QgPiJxuji6Ao29SpUdhQZ5ZGzG
RdzBkot8wJ2sVd6k0j/SkO1vlWKXk5pOBBzlRMGSSH6aCRwHISI3FqOOo/O3za9x
Otro7iyD5qAt7JPzQgeMtCjHFoJUeVHYwZ9mpWCBQ91H30HZ4gONN3Ufjabumd7u
E+vXO1HjVzDq2u/xaXoeaMS7uiJpAoHBAPoX+HwpUi1jQuCgb3NbHCNSLX3W03Ux
ak55iyfBjaNzVy2AuJOhMPsHvz2Jk/4hlmsT1/kFTB6Aok2Jqs1AYTxuv+LkteoA
wYt6uKNs3vzXW98TmqjQiTj7l8aC4WY5jWjELe2+S1rIQvOobbnEH8SQlLQfAnU7
7x4fZB1FH1oeowtntuj+OqJXfWwc+ItiwGlnaGfICExidaffwPTzRmqvmAT8xvhV
fZZfSPbvZ6eNNuX28q9jU3+KuvCFaDRwxwKBwQDrWOnD06XQ73NXnHiv43mMVnf8
lzbW+h9ItK7XWZq9ilnm8ZRlPjBNsZW0sTS9rKjLKratQy8zGB7ZKpLOzErLc9Zg
EP5tdCSwV6hu1KFJlUxasZVYGlPg2x5VqZWVx5zTmXZP/NzH1UWtN4uvw9ODb+gw
4gCYhrmS4oZCQyxlqOhfrbwbhm5/fSNkY9EFGw/uQo1KStxx3N2df35XsEAcsA35
dT67w4BziFUex2m5zoqOOkeD+ZQN9e7r3/f3+9sCgcEA0Vh9ZRmFs36SfctuX6aV
kC966wqHqWL69MOjK11GvdqP0AQe/V0BzjA28kEWw7TD39AVilrX0/SjZ7pkYjmQ
63BdaYU/jaiiWqoYopxAsG9pdPtJDCS7qRpZew8VtGdaqqcFNyyCkXRvLtz/NHAq
k3TfNUN74DySNanbOPEihGJ+4s4nezNMS5Zm47gAiVTZcaHg8HauE5qbmDGhqKl3
eViRLSOXPkr5vIT4Y9QU9Vks6iTkEtJXE71CLJHPn44DAoHBAKLilLhFzWdzslKa
mvSw7Tjxx41sYqoa5nf9hVzKSUyRanNqE5iWl/vNwp0SYDw+OXyTjWcRLqOgOAl5
a63wunthKqfGWzEJxzK9GHfMdexlhjjm20PkxNTFEpObEUpeou3YMohdq7gqpVSj
MuxtDgDT/NGIOX1XESzV1rIZp6qcYmeF6MDsI6HczBf49XshJb9zFDKs6TFs+Xy9
9oVeGKFCQAm82bQ+NLLBUphAz62ng0G4mDKBE7Ut1zQtCIP7LQKBwBNTaLR8E6Wt

Z6x8+bxbwRjKkdvd3pxfC9FRk+gM9n6fZdMHd2X7uTOWb7A4OTpDHIhqHNAMEcWz
BoOtfl6pyS/2POCYN7SDDDykJPZA1Vud843C1StQFlyWPR6NuD0/K6xt2bVns2mZ
ekEBS0yknF4xBG9HUQZBktwmdCxvKJ8lJZXVnUeh5M5frrMY/0VOrUMtG/6o4AjB
BVOycXT5azf4YVxh6WXy+aGC1tHRj5oZrpm24PinWxU8achfHtFm0A==
-----END RSA PRIVATE KEY-----

Items I expect to be contained in the file

- Version number
- Prime numbers p and q
- n, the number that is modded to
- d, the exponent that is used for decryption
- exponent1, d mod (p-1)
- exponent2, d mod (q-1)
- coefficient, 1/q
- otherprimeinfo, optional parameters containing a *prime*, *exponent*, and a *coefficient*

How I decode:

1. I copied the contents of the private key file to my clipboard, with the section markers (the start and end headers) removed.
2. Then, I opened Lapo Luchini's ASN.1 decoder and paste it from my clipboard.

version

- Value: 0
- Meaning: the version number of the ASN specifications. This allows compatibility with future revisions to the document. Version number 0 means current version of the document, and the multi-prime is not used.
- Offset: 4
- DER encoding:
    - Type: 02 (INTEGER)
    - Length: 01 (the value 0 requires one byte to store)
    - The remaining bytes represent the value of the integer 0

modulus

- Meaning - the result of pq, used as part of encrypting or decrypting messages via the formula M^e mod n
- Value: 0x 00 E5 EA DD B6 84 CB AB 77 E2 74 B1 76 FD 44 E9 9D 33 E4 6D F1 54 5B 98 93 F7 46 6C 92 9D C9 7E 3E 7F 68 A6 D8 C1 74 DC AC A7 5F 45 02 34 21 1D 63 34 71 70 CF D7 87 BE 68 E6 4F 73 33 F5 BF 03 17 BA 39 29 C5 1F 87 7B 85 5D 2B A6 DF C1 56 67 BF 6C 78 52 BD 4D A3 7F E9 05 BE 21 09 3C E5 93 3D A3 86 EE 0A F1 96 B4 55 5B C4 A2 52 64 93 53 27 97 40 08 1A 44 06 C1 74 18 48 41 8C 67 A6 93 A1 6D B5 4A DA 98 E6 04 D9 55 22 AA 18 39 0A 07 1D 18 D3 E6 10 60 2A 38 27 25 5D 11 DC 82 6C BC 54 56 5E 32 D1 68 07 07 56 1F D1 D6 F7 2D 7D 51 72 21 B6 BE 0D 04 80 36 91 46 AD E7 F6 C4 EE 13 74 E1 2E EC BF 1B 0E 58 A8 5A 42 12 3D FA 47 09

3E 25 BA 26 80 66 FA A6 04 08 0B 9D 9C 23 41 9E 32 D1 B3 19 51 83 40 EB CA CB B5 44 0A 44 46 DA E8 7F 75 41 1E 7B 8C 9E 09 F1 83 05 C3 43 55 5A 75 21 16 B7 0E A2 EF 9D D9 23 D3 6E 31 4B 32 AD 9A 50 66 16 15 98 BC A2 28 92 6B 30 8E 0B A6 1C FA 59 57 66 F6 40 92 83 17 71 F4 BE 59 79 66 6D 84 6A CD A5 78 E2 CE C2 C3 14 5B 43 DA DC 49 C3 3E 77 3C 97 84 CC 2C 1C D3 F0 2F B1 30 12 BA F6 6F 4D 48 35 DF C8 2D EF 8E 23 9A 2A 7B 17 5E E1 66 56 92 86 BE 5F 03 C4 AD AC BB 05 8B C5 D8 C7 A4 71 D8 D9 53 EA 8E 85 37 F5 37 9D 0D 60 70 97 3D

- Offset: 7
- DER encoding
    - Type: 02 (INTEGER)
    - Length: 82 01 81
        - 82: A marker for length that's greater than 127 bytes. Ignoring the most significant bit amounts to 2, which is how many bytes are required to store the actual length of the integer
        - 01 81: actual length of the integer (385 bytes)
        - The remaining bytes represent the value of the integer. The first byte is 00 because the first bit is always the signed bit, and since the most significant bit of this positive integer is 1, an extra byte of value 00 is added to indicate a positive integer.

publicExponent

- Value: 0x 01 00 01
- Meaning: e, or value that's part of the public key and used when encrypting messages with the formula M^e mod n
- Offset: 396
- DER encoding
    - Type: 02 (INTEGER)
    - Length: 03 (the integer requires three bytes to store)
    - The remaining bytes represent the value of the integer

privateExponent

- Value: 0x 32 25 75 D2 17 48 AC CF 6B 0E F4 9D F5 43 90 88 7F 06 F5 8B CB 50 67 08 EE C7 E7 6A 5B 0B D5 83 20 1A DD 39 2D 88 A5 90 EA B8 76 BE B2 4B FE B2 E2 7F 53 91 A1 7A B3 E7 01 44 96 E5 E0 55 97 01 17 D6 DB EB 68 A3 0E 27 DA 58 68 FF 28 96 05 EE D4 63 B1 F8 23 F4 E3 33 19 D3 8C 35 0D 99 2C F2 26 B6 89 38 CD D4 86 E4 8F 2D 66 11 FE 69 BB 9B 48 FB E8 48 82 49 CE EB D9 57 F9 23 FC 7F 72 77 A5 0C 03 95 85 FF B5 53 09 A4 93 E0 D0 A0 05 49 2D 5F 1A 30 BC 28 B9 32 A0 8D 9A 15 B4 44 AF 16 DD F7 91 B1 E6 B4 91 BF 11 15 9D 83 2F E2 C3 5E D7 47 9A 50 10 89 3E 5D 95 42 DC F3 0F A4 B5 8D 40 A7 04 77 11 42 E2 D5 07 00 36 0D 90 E7 00 FD 34 FE CB 40 FE 01 F8 28 B8 71 31 06 D0 FB 60 44 34 27 26 5A 71 2C 31 1F 89 8E 84 89 72 72 B3 82 40 BB B3 55 50 1E 17 C4 20 3E 22 71 BA 38 BA 02 8D BD 4A 95 1D 85 06 79 64 6C C6 45 DC C1 92 8B 7C C0 9D AC 55 DE A4 D2 3F D2 90 ED 6F 95 62 97 93 9A 4E 04 1C E5 44 C1 92 48 7E 9A 09 1C 07 21 22 37 16 A3 8E A3 F3 B7 CD AF 71 3A DA E8 EE 2C 83 E6 A0 2D EC 93 F3 42 07 8C B4 28 C7 16 82 54 79 51 D8 C1 9F

66 A5 60 81 43 DD 47 DF 41 D9 E2 03 8D 37 75 1F 8D A6 EE 99 DE EE 13 EB D7 3B 51 E3 57 30 EA DA EF F1 69 7A 1E 68 C4 BB BA 22 69

- Meaning: d, which is part of the private key, and used for decrypting a message encrypted by the public key (n,e). The decryption formula is Z^d mod p, where Z is the encrypted message.
- Offset: 401
- DER encoding
    - Type: 02 (INTEGER)
    - Length: 82 01 80
        - 82: A marker for length that's greater than 127 bytes. Ignoring the most significant bit amounts to 2, which is how many bytes are required to store the actual length of the integer.
        - 01 80: actual length of the integer (384 bytes)
        - The remaining bytes represent the value of the integer

prime1

- Value: 0x 00 FA 17 F8 7C 29 52 2D 63 42 E0 A0 6F 73 5B 1C 23 52 2D 7D D6 D3 75 31 6A 4E 79 8B 27 C1 8D A3 73 57 2D 80 B8 93 A1 30 FB 07 BF 3D 89 93 FE 21 96 6B 13 D7 F9 05 4C 1E 80 A2 4D 89 AA CD 40 61 3C 6E BF E2 E4 B5 EA 00 C1 8B 7A B8 A3 6C DE FC D7 5B DF 13 9A A8 D0 89 38 FB 97 C6 82 E1 66 39 8D 68 C4 2D ED BE 4B 5A C8 42 F3 A8 6D B9 C4 1F C4 90 94 B4 1F 02 75 3B EF 1E 1F 64 1D 45 1F 5A 1E A3 0B 67 B6 E8 FE 3A A2 57 7D 6C 1C F8 8B 62 C0 69 67 68 67 C8 08 4C 62 75 A7 DF C0 F4 F3 46 6A AF 98 04 FC C6 F8 55 7D 96 5F 48 F6 EF 67 A7 8D 36 E5 F6 F2 AF 63 53 7F 8A BA F0 85 68 34 70 C7
- Meaning: p, or one of the prime numbers that's a factor of n.
- Offset: 789
- DER encoding
    - Type: 02 (INTEGER)
    - Length: 81 C1
        - 81: The most significant bit indicates that the length is greater than 127 bytes. The 1 indicates that the actual length requires one byte to store
        - C1: actual length of the integer
        - The remaining bytes represent the value of the integer

prime2

- Value: 00 EB 58 E9 C3 D3 A5 D0 EF 73 57 9C 78 AF E3 79 8C 56 77 FC 97 36 D6 FA 1F 48 B4 AE D7 59 9A BD 8A 59 E6 F1 94 65 3E 30 4D B1 95 B4 B1 34 BD AC A8 CB 2A B6 AD 43 2F 33 18 1E D9 2A 92 CE CC 4A CB 73 D6 60 10 FE 6D 74 24 B0 57 A8 6E D4 A1 49 95 4C 5A B1 95 58 1A 53 E0 DB 1E 55 A9 95 95 C7 9C D3 99 76 4F FC DC C7 D5 45 AD 37 8B AF C3 D3 83 6F E8 30 E2 00 98 86 B9 92 E2 86 42 43 2C 65 A8 E8 5F AD BC 1B 86 6E 7F 7D 23 64 63 D1 05 1B 0F EE 42 8D 4A 4A DC 71 DC DD 9D 7F 7E 57 B0 40 1C B0 0D F9 75 3E BB C3 80 73 88 55 1E C7 69 B9 CE 8A 8E 3A 47 83 F9 94 0D F5 EE EB DF F7 F7 FB DB
- Meaning: same as p, and pq = n
- Offset: 985

- DER encoding
    - Type: 02 (INTEGER)
    - Length: same as p
    - The remaining bytes represent the value of the integer

exponent1

- Value: 0x 02 81 C1 00 D1 58 7D 65 19 85 B3 7E 92 7D CB 6E 5F A6 95 90 2F 7A EB 0A 87 A9 62 FA F4 C3 A3 2B 5D 46 BD DA 8F D0 04 1E FD 5D 01 CE 30 36 F2 41 16 C3 B4 C3 DF D0 15 8A 5A D7 D3 F4 A3 67 BA 64 62 39 90 EB 70 5D 69 85 3F 8D A8 A2 5A AA 18 A2 9C 40 B0 6F 69 74 FB 49 0C 24 BB A9 1A 59 7B 0F 15 B4 67 5A AA A7 05 37 2C 82 91 74 6F 2E DC FF 34 70 2A 93 74 DF 35 43 7B E0 3C 92 35 A9 DB 38 F1 22 84 62 7E E2 CE 27 7B 33 4C 4B 96 66 E3 B8 00 89 54 D9 71 A1 E0 F0 76 AE 13 9A 9B 98 31 A1 A8 A9 77 79 58 91 2D 23 97 3E 4A F9 BC 84 F8 63 D4 14 F5 59 2C EA 24 E4 12 D2 57 13 BD 42 2C 91 CF 9F 8E 03
- Meaning: d mod (p - 1)
- Offset: 1181
- DER encoding
    - Type: 02 (INTEGER)
    - Length: same as p
    - The remaining bytes represent the value of the integer

exponent2

- Value: 0x 02 81 C1 00 A2 E2 20 B8 45 CD 67 73 B2 52 9A 9A F4 B0 ED 38 F1 C7 8D 6C 62 AA 1A E6 77 FD 85 5C CA 49 4C 91 6A 73 6A 13 98 96 97 FB CD C2 9D 12 60 3C 3E 39 7C 93 8D 67 11 2E A3 A0 38 09 79 6B AD F0 BA 7B 61 2A A7 C6 5B 31 09 C7 32 BD 18 77 CC 75 EC 65 86 38 E6 DB 43 E4 C4 D4 C5 12 93 9B 11 4A 5E A2 ED D8 32 88 5D AB B8 2A A5 54 A3 32 EC 6D 0E 00 D3 FC D1 88 39 7D 57 11 2C D5 D6 B2 19 A7 AA 9C 62 67 85 E8 C0 EC 23 A1 DC CC 17 F8 F5 7B 21 25 BF 73 14 32 AC E9 31 6C F9 7C BD F6 85 5E 18 A1 42 40 09 BC D9 B4 3E 34 B2 C1 52 98 40 CF AD A7 83 41 B8 98 32 81 13 B5 2D D7 34 2D 08 83 FB 2D
- Meaning: d mod (q - 1)
- Offset: 1377
- DER encoding

coefficient

- Value: 0x 02 81 C0 13 53 68 B4 7C 13 A5 AD 67 AC 7C F9 BC 5B C1 18 CA 91 DB DD DE 9C 5F 0B D1 51 93 E8 0C F6 7E 9F 65 D3 07 77 65 FB B9 33 96 6F B0 38 39 3A 43 1C 88 6A 1C D0 0C 11 C5 B3 06 83 AD 7E 5E A9 C9 2F F6 3C E0 98 37 B4 83 0C 3C A4 24 F6 40 D5 5B 9D F3 8D C2 D5 2B 50 16 5C 96 3D 1E 8D B8 3D 3F 2B AC 6D D9 B5 67 B3 69 99 7A 41 01 4B 4C A4 9C 5E 31 04 6F 47 51 06 41 92 DC 26 74 2C 6F 28 9F 25 25 95 D5 9D 47 A1 E4 CE 5F AE B3 18 FF 45 4E AD 43 2D 1B FE A8 E0 08 C1 05 53 B2 71 74 F9 6B 37 F8 61 5C 61 E9 65 F2 F9 A1 82 D6 D1 D1 8F 9A 19 AE 99 B6 E0 F8 A7 5B 15 3C 69 C8 5F 1E D1 66 D0
- Meaning: 1/q mod p
- Offset: 1573

- DER encoding
    - Type: 02 (INTEGER)
    - Length: 81 C0
        - 81: The most significant bit indicates that the integer's length is more than 127 bytes. The 1 indicates that the length requires one byte to store.
        - C0 is the actual length of the integer (192 bytes)
    - The remaining bytes represent the value of the integer

Public key

ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQDl6t22hMurd+J0sXb9ROmdM+Rt8VRbmJP3RmyS
ncl+Pn9optjBdNysp19FAjQhHWM0cXDP14e+aOZPczP1vwMXujkpxR+He4VdK6bfwVZnv2x4Ur
1No3/pBb4hCTzlkz2jhu4K8Za0VVvEolJkk1Mnl0AIGkQGwXQYSEGMZ6aToW21StqY5gTZVSK
qGDkKBx0Y0+YQYCo4JyVdEdyCbLxUVl4y0WgHB1Yf0db3LX1RciG2vg0EgDaRRq3n9sTuE3
ThLuy/Gw5YqFpCEj36Rwk+JbomgGb6pgQIC52cl0GeMtGzGVGDQOvKy7VECkRG2uh/dUEee
4yeCfGDBcNDVVp1IRa3DqLvndkj024xSzKtmlBmFhWYvKIokmswjgumHPpZV2b2QJKDF3H0vl
l5Zm2Eas2leOLOwsMUW0Pa3EnDPnc8l4TMLBzT8C+xMBK69m9NSDXfyC3vjiOaKnsXXuFm
VpKGvl8DxK2suwWLxdjHpHHY2VPqjoU39TedDWBwlz0= prompt@Prompts-MacBook-Air.local

Items I expect to be contained in the decoded string

- e - the public exponent
- n - the modulus
- Length of each

How I decode

- I removed the ssh-rsa part and decode it from base64, then hexdump it:
- base64 -d -i publickey.txt | xxd -p
- This is the result:

000000077373682d727361000000030100010000018100e5eaddb684cbab
77e274b176fd44e99d33e46df1545b9893f7466c929dc97e3e7f68a6d8c1
74dcaca75f450234211d63347170cfd787be68e64f7333f5bf0317ba3929
c51f877b855d2ba6dfc15667bf6c7852bd4da37fe905be21093ce5933da3
86ee0af196b4555bc4a252649353279740081a4406c1741848418c67a693
a16db54ada98e604d95522aa18390a071d18d3e610602a3827255d11dc82
6cbc54565e32d1680707561fd1d6f72d7d517221b6be0d0480369146ade7
f6c4ee1374e12eecbf1b0e58a85a42123dfa47093e25ba268066faa60408
0b9d9c23419e32d1b319518340ebcacbb5440a4446dae87f75411e7b8c9e
09f18305c343555a752116b70ea2ef9dd923d36e314b32ad9a5066161598

bca228926b308e0ba61cfa595766f64092831771f4be5979666d846acda5
78e2cec2c3145b43dadc49c33e773c9784cc2c1cd3f02fb13012baf66f4d
4835dfc82def8e239a2a7b175ee166569286be5f03c4adacbb058bc5d8c7
a471d8d953ea8e8537f5379d0d6070973d

How I make sense of the result: https://www.thedigitalcatonline.com/blog/2018/04/25/rsa-keys/

00000007
- Length of the following item is 7 bytes

7373682d727361
- Hexadecimal and Ascii encoding of the string “ssh-rsa”[7]

00000003
- Length of the following item is 3 bytes

010001
- Hexadecimal representation of the number 65537 in decimal
- This is the public exponent

00000181
- Length of the following item is 385 bytes

The remaining bytes represent the modulus, n

Sanity check

Code in sanity_check.py

[7]https://www.rapidtables.com/convert/number/hex-to-ascii.html