SSH KEY FILE FORMATS

By: Sydney Nguyen

–Private Key–

Contents of id_rsa_homework:

-----BEGIN RSA PRIVATE KEY-----
MIIG5AIBAAKCAYEAuDqcbLs+WQguWieh6nankrqr5DjiDP0IB1UNW1Zd6SfniCPR
ikQcmRd2jgd78hbGsFQ8zk8viwrnt4hcCPtgmf0dKTY8hfrxFaC0nZ+c2mPe2ZNs
P5Uabz2kYHI0gguEQQa8fTHQJebCpGz1vC05ILy8pMV8LqMThG7ac9g3VbTrqdvc
fRRiGcwSqr/KapGQp9uDdPtKDr1H3JTXaqrDrQoFWznr9nA1H+a1iE5F8MGuXBFt
WtZAN5G7W4G25PYQek+epM9n9YKfTbJgOLZXYr/7LmlW8h476HRKgehI/QQ+l
Sl6tZ7EftPRIJ5CLs0hBerpQXawYRXw7fQfi6pr8u3MrDLP3w9DF8ZzyAff0x5v/LIv
c6/5CumyYsbax38k/+EdM964nFB5aaHuctvp7If3xDuZNMeswCwLZH41vOkHnfQG
XMGo5ApDv7/+AB55se03tMCzGJM6HF97OQiqACsOkhvq1dhVtgbN9CxJHREyadb7
meL7nJy1cS2U0LjfAgMBAAECggGAe+lwLPIEDX4jLyBZF4qXS2mjE+3unS3TqJrc
UQLWR2w/nqH43jbRxWaypvUBuOL44MDH5Tv9jlfXYuqkfKYXY3uLkZyZOMSAQzv
EQACLT5i82zr9JAb1sLyVQwmNp6p3WgVd4hcPGW8Mm+ttnRQNyKcpeuoZjITDK
+AjrqdPEKaPm7/1nWuIUDGinJZDX0ppMX3D/XrHZQKKwyKZgXU6B7klwSZEP4
1ZLgvPLc732+dpjyNpmh9hMf8jNXkZuwaFCoEsg6GVGDRkt4ej1tTOP6l8u6T8Fm4
+aib8xD4+aHbfsu+/0NnF9O3UpTB14yyyQQ6bPDs1TBWb8L6rlQ1UOvvAfplcFjKF
/6EUYLsInMTipvmKlmAiDJMGOSUYBQMLWOEMFmUAEBALJNFUx01wR3rccBySf
f+5r8rEQDzMDfQxZP7Q3Swlff1jfh1lvDv2oCf61Y4JLgrYBfOt8gy6qE4JzuWPmhjaL
OdKy/jmTXaYckrvYvjcCQCmwOfRMVBsBAoHBAN8F1AI2mbWMov6/RibeXGEHoL5
O9Iy/9wihfrPI0gYN2sSlzxaSrgqGwKDNEqYXFUTIfJcS8LsusqsrfYMtknuy3L4Jfcz+
nSJXn2XCJdAG1n5jFiICDn57xx5tBsOv2g0YZVFccj+aCZ3RS5wxyKZLzO5en96A
wQF/uMIDWL1WvPP10IunHvv26gEYzOzgzrcl+uKXZD8giwAtynOAvacnTaUX+na6
ZGqFXwE5MJdoD0o62k0V4lyosK1A+0TYWQKBwQDTeE3/tzu/fNVOCqNTBlGtTV
P/GZiYmeWUnkFJRgMNU3NGh0dDF3pCkNeFRRaEVCrldkL5PjMDyLfb24R2XNSV
5QK7vY/dwg7ysnQbMMPRBZN6PhXJ262EmC6oXLO2V2vdzfxrAUL80QpMEVjSkCk
k534fZ7D4mzmbYVGcbBK09MCa3IgmZvPJdKV5j13QisCWAv1vbwFSy5YBFBYoPfk
oh5Ffus9TVTkHUBw+PH6xvltiAAwl9hMTSASO7rNUc/cCgcEAlFjjGgnJmpqOvRbsC
eS03BHf2VbZkloKbyJFDj+RfFdw4odMRb6RqAzUSuG9+t611gfp3+/IUyoPzI3kMgJ
5QnDKJlpX5KikSviv3VcUIdi6il1Mlph5naal31Y0PqxVRYqpskHk+Ot0ZBaYza/LwNo
A2bn1a2KHf4C+m8bwGxl8HGaxLoOet4kZRFuDzDkJJ4hK5rg/BUKXUyoiVUwYWv

xoyF03zAvVyYknlb+906hzKzQUi1v4Mxw+UTA9MyEZAoHATLclHLJ9Y19HBpPH
YlQ1hzg5U58Wg6244qxypMFYVBpFBH4I9SbsPH/NH9TLcWATW8EGVOMioKnNQ
V4mdMYCfQpibnc7XMiMobDpe/+52fc65Crnvp4KGcMXkg5nR6v5PrL+clc31P2Ezcm
xPln8Ax5T29LDGb0+LcclUyjFtI3h3YxJfBz3Lcs6SJog/4mGiiU1iZpskXu3xFZk
H180J2be7yqXEfUlxihixpUtpQ+YmTnJLnBRxTnoJW4k8mtLAoHBAJEeHvs7fRHA
lSlt3Fpf/VZSfMMlw35qZd8P3u/oE55rQwzRkig6OwuBoVKThepmEPdkFDRTRW6W
ZuQg529BQXRx1v/v5AHxOXQH9iLCyf7IDcR+tBmJrvbh5bPe/ZwUx5VWqj2XVyU
Zv47sVMmJgB9gKyKhKNKEFJrjsLVGrz3H8mZWTn1YuFdE3xdtnxX4f0NeqAZCHP
reZ0X6aCUj2OEWlJUAvxDIRXa7HqvtdAWgbasCcVh/p8/zF9CLTatoGw==
-----END RSA PRIVATE KEY-----

Expected items in the private key:

The RSA private key should contain the following with the 10th item being optional:

1. Version version (the version number)
2. Modulus integer - - n
3. publicExponent integer - - e
4. privateExponent integer - - d
5. Prime1 integer - - p
6. Prime2 integer - - q
7. Exponent1 integer - - d mod (p - 1)
8. Exponent2 integer - - d mod (q - 1)
9. Coefficient integer - - (inverse of q) mod p
10. otherPrimeInfos otherPrimeInfos OPTIONAL

Note: The 10th otherPrimeInfos is only required for version 1

To decode the file I utilized the website https://lapo.it/asn1js/. The following text is what is the output.

The following data will be typed up as

1. Label
2. Offset
3. Length
4. Value

5. DER encoding

The decoding of the file begins by notifying that there are 9 elements in the sequence.

1. Sequence
2. 0
3. 4 + 1764
4. (9 elems)

    It should also be noted that this sequence is labeled as (constructed).

Version

Next, we are given the version, as the value is 0 this means we will not need the otherPrimeInfos:

1. INTEGER
2. 4
3. 2 + 1
4. 0
5. 02 01 00

Explanation of DER Encoding for one sequence:

The 02 in binary stands for 0000 0010 this is the type and the beginning of the object the tag class begins with 00 . Then the p/c which states that is primitive with the 0. The 01 is the length in octets of the value and lastly the 00 is the value.

Modulus

1. INTEGER
2. 7
3. 4 + 385

4. 3073 bit

```
41808500338907723059828021236522338194561748341426058849567577052998350916807214
14726415002424879027469681465741696707640914046012022271943473582877263241377598
26407387493003645126560468498860053962900740241052790138708813264303811082527439
71500327559732950635825396845693407509407822628539502577961557306053942989237362
15579137272352758722522681277664227698244935432768137549066083499107413208522698
19774425415161963867757820755358155945333810594049387405442082600969051323941641
96076216744818655459954164513813998430259373151313210809245053008727073688614718
29333741184065630108977726882325085213620102181035769273257639011019392809496128
87334264511888157515403110146585871592256532197282933231040864389659979032164689
55938583199842624539249675377283459698240835623450905520210959168631341902612338
23740598912995694290535755459435281322985603269426871290094482187072707241451219
58602211600048144029585591532881478584216598 3
```

5. 02 82 01 81

publicExponent

1. INTEGER
2. 396
3. 2+3
4. 65537
5. 02 03

privateExponent

1. INTEGER
2. 401
3. 4+384
4. 3071 bit

```
28120278544014105504939487253092217642191157161451709325860793086289688396064238
51582165392173713589741116606037719011746211928349023326476163320463703918090918
58767377827663772787567106389211455798780301658995788475430436069556311587619353
07745768631964057921894250468562268688141001594000660293216739338859847215551259
95738718143419894174112330297685874497438649219165044221780566102211800574205113
69999491467420531414174660709159520790855766528612798828629430444148390672520570
27917086918453288128933103972374364671539741295789217723314503407914496428723883
67431852046347952839598128372157168611861092856402880178993951691730031537216022
68024480519085885838489433862490637380400726251820571465498658122810418998188004
97492356043652996602636421999405934347049471467350065400177764161143134521031731
69423637893594690018605679206109005930526471737815406807199133500683970556556610
92197936153872593810165419277513186131182259 3
```

5. 02 82 01 80

Prime1

1. INTEGER
2. 789

3. 3+193
4. 1536 bit

```
209982244127780411037638602119585667279837814612243262809709959792678303337209268252770338065446450347452650111944372105299398230686902786445677354472953905217418022597204614337871869199009324109390347478763576711777870877484943022123096309481964384140390625815467493172162307122902506096045786828273822657248113569115017917835672479625822408827815289799751052482371302827366420068612373265323574663672988325390277915751453531082807204497345596791904571859434504 9
```

5. 02 81 C1

Prime 2

1. INTEGER
2. 985
3. 3+193
4. 1536 bit

```
199104931526810491032333609481351988929075691905774503371581588121965156403865896624769828845819343211190779634215314725453010677719170037587130290674848441584114610850522672556144332570498495724617862300460911861674655110330181000215603684730866501654835604532449069762541969497592616874822676011080719703458483345460515277362136949207042713605586371577301074232017356749037954459549684647948984218274769931317612554188106572039102369193383118988019064631331736 7
```

5. 02 81 C1

Exponent1

1. INTEGER
2. 1181
3. 3+193
4. 1536 bit

```
139673100206941597240700361356166714889756471190190587846005863515910482282969370446358810248973970581450224702534309064899471551495096711316148327105901698126903945238261451589649333872353227427264803357519273076224617012713446162677756476837095594524016746444554134283545394877502624203873229657283786425594246733666627415385274029071894695825404264498000767637214429124522689480906844645810853458885298391555668581313321296442134132726976608778170499270385945
```

5. 02 81 C1

Exponent2

1. INTEGER
2. 1377
3. 3+192

4. 1535 bit

```
72229728963027288772658674724493698777618361766022076348617609252784253070813612
03982334682407426163611487840156658235191792924398085459578000248196888050564814
26503039683925114413462145597408464346808092140039902851049826525482289412999924
39024536930950707199886730146397230950535796057172423549497903641450256214631791
97581953409474644003411771695354151598394595743864852491519715265807871869477988
74323682359009181961675656534424649827224873573729841404078923
```

5. 02 81 C0

Coefficient

1. INTEGER
2. 1572
3. 3+193
4. 1536 bit

```
13663238274923863988252022510420555980608290099789952748314762850270365188946111
90868765268967784300330295050542738800694031068434146642710617848235168971009684
56920028439910983285353405351661522132846437689285535057017736114172653687789603
94727564726562730917491056522505402487263780084211135950815392448407760515999724
15501094321306867702397592240731809622652973611830036865000669121588223569549161
49641061212685731019606641398916469444766448012742561498001615 5
```

5. 02 81 C1

–Public Key–

Contents of id_rsa_homework.pub:

ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQC4Opxsuz5ZCC5aJ6HqdqeSuqvkOOIM/Q
gHVQ1bVl3pJ+eII9GKRByZF3aOB3vyFsawVDzOTy+LCue3iFwI+2CZ/R0pNjyF+
vEVoLSdn5zaY97Zk2w/lRpvPaRgcjSCC4RBBrx9MdAl5sKkbPW8LTkgvLykxXwuoxO
Ebtpz2DdVtOup29x9FGIZzBKqv8pqkZCn24N0+0oOvUfclNdqqsOtCgVbOev2cDUf5r
WITkXwwa5cEW1a1kA3kbtbgbbk9hB6T56kz2f1gp9NsmA4tldiv/suaVbyHjvodEqB6E
j9BD6VKXq1nsR+09EgnkIuzSEF6ulBdrBhFfDt9B+Lqmvy7cysMs/fD0MXxnPIB9/T
Hm/8si9zr/kK6bJixtrHfyT/4R0z3ricUHlpoe5y2+nsh/fEO5k0x6zALAtkfjW86Qed9AZ
cwajkCkO/v/4AHnmx7Te0wLMYkzocX3s5CKoAKw6SG+rV2FW2Bs30LEkdETJp1v
uZ4vucnLVxLZTQuN8= kali@kali

According to the RFC 8017, we are supposed to find the following in the public key:

n the RSA modulus, a positive integer

e the RSA public exponent, a positive integer

When I attempt to put the contents into the decode we receive the error “Length over 48 bits not supported at position 1” to fix this we must in the kali terminal type out ssh-keygen -f id_rsa_homework.pub -e -m pem

To then get a file that is able to decoded:

-----BEGIN RSA PUBLIC KEY-----
MIIBigKCAYEAuDqcbLs+WQguWieh6nankrqr5DjiDP0IB1UNW1Zd6SfniCPRikQc
mRd2jgd78hbGsFQ8zk8viwrnt4hcCPtgmf0dKTY8hfrxFaC0nZ+c2mPe2ZNsP5Ua
bz2kYHI0gguEQQa8fTHQJebCpGz1vC05ILy8pMV8LqMThG7ac9g3VbTrqdvcfRRi
GcwSqr/KapGQp9uDdPtKDr1H3JTXaqrDrQoFWznr9nA1H+a1iE5F8MGuXBFtWtZ
AN5G7W4G25PYQek+epM9n9YKfTbJgOLZXYr/7LmlW8h476HRKgehI/QQ+lSl6tZ
7EftPRIJ5CLs0hBerpQXawYRXw7fQfi6pr8u3MrDLP3w9DF8ZzyAff0x5v/LIvc6/5
CumyYsbax38k/+EdM964nFB5aaHuctvp7If3xDuZNMeswCwLZH41vOkHnfQGXMGo
5ApDv7/+AB55se03tMCzGJM6HF97OQiqACsOkhvq1dhVtgbN9CxJHREyadb7meL7
nJy1cS2U0LjfAgMBAAE=
-----END RSA PUBLIC KEY-----

Again inputting into https://lapo.it/asn1js/ I get the following information:

1. Type
2. Offset
3. Length
4. Value
5. DER encoding

Sequence

1. SEQUENCE
2. 0
3. 4+394 (constructed)

4. (2 elem)
5. 30 82 01 8A

Modulus

1. INTEGER
2. 4
3. 4+385
4. 3072 bit

```
418085003389077230598280212365223381945617483414260588495675770529983509168072141
147264150024248790274696814657416967076409140460120222719434735828772632413775982
640738749300364512656046849886005396290074024105279013870881326430381108252743971
500327559732950635825396845693407509407822628539502577961557306053942989237362155
791372723527587225226812776642276982449354327681375490660834991074132085226981977
442541516196386775782075535815594533381059404938740544208260096905132394164196076
216744818655459954164513813998430259373151313210809245053008727073688614718293337
411840656301089777268823250852136201021810357692732576390110193928094961288733426
451188815751540311014658587159225653219728293323104086438965997903216468955938583
199842624539249675377283459698240835623450905520210959168631341902612338237405989
129956942905357554594352813229856032694268712900944821870727072414512195860221160
004814402958559153288147858421659830
```

5. 02 82 01 81

Public Exponent

1. INTEGER
2. 393
3. 2+3
4. 65537
5. 02 03

I want to note that the modulus and the publicExponenet are the same for the public and private key which is to be expected to be able to perform the RSA calculations.

–Sanity Check–

We must use RSA formulas to do a sanity check. It is important to acknowledge that the private and public keys match the n and e. I used the formula $\lambda(n) = \text{lcm}(p - 1, q - 1)$, where lambda is $e * d \bmod \lambda(n) = 1$ and lastly $\gcd(e,\text{lambda}(n))=1$. I also verified that n

= p * q. In the SSH file you will also be able to find the python code used to check such integer value

Cite

https://www.thedigitalcatonline.com/blog/2018/04/25/rsa-keys/
https://datatracker.ietf.org/doc/html/rfc8017#section-3.1
https://datatracker.ietf.org/doc/html/rfc4716#section-3.4
https://lapo.it/asn1js/
https://en.wikipedia.org/wiki/X.690