Ryan Son

CS 338: Computer Security

Jeff Ondich

October 2, 2024

What's in a key file?

Private Key

According to RFC 8017, the structure of an ASN.1 RSA Private Key should be a sequence of several integers: version, modulus, publicExponent, privateExponent, prime1, prime2, exponent1, exponent2, and coefficient (Moriarty, Kathleen, et al). These integers can be set to varying arbitrary lengths.

Decoding the RSA Private Key was done using https://lapo.it/asn1js/, an ASN.1 JavaScript decoder. The RSA Private Key contained in **id_rsa_homework** was input into the text box and then I pressed decode.

The integers within the RSA Private Key are detailed below (Moriarty, Kathleen, et al):

Version

- This is expressed as either 0 or 1. If the version is 0, the RSA Private Key is constrained by the normal two prime numbers (p & q) that we have demonstrated in class. The version value of 1 will be an RSA Private Key that includes more than two prime numbers.
- **Value:** 0

Modulus

- This provides what modulus (n) the RSA Private Key is in, where p * q = n.

- **Value:** 0x 00 CF 09 FE E7 EA 34 CB EB 64 03 24 F2 D1 FB 43 2B 1A C3 7A 7F 4D B1 E0 8B BF 1A 35 AA 1C 21 17 AC 2C B6 5C 5C 6E 29 2E E8 CF B7 34 03 58 96 73 F3 AE 49 09 63 52 CE 5D 69 22 56 86 29 CB 4C 84 5C 5E E4 06 C2 FA A8 4D FA BF D8 20 1B C5 5E 4C DA E0 10 70 5D D2 A9 1B F1 C9 AA D9 DE FE 73 76 00 78 4A 9D 95 97 7E 9A 7C 0E ED 56 7B A7 F6 59 D4 5B 7A EB 98 BF C8 C5 91 7F 98 AF 1D D2 DF 80 63 0B EE BE 5E E2 83 85 5B F9 2B C9 F5 3E 83 7D F8 51 4B DD D2 D1 7C 6A 49 25 B2 4D CB 07 BB 41 B1 49 D4 31 1C BF 61 72 7E 51 A9 80 6F 1B BE BF AF 85 2A 32 3D 1F E8 3C 81 4D 1D 6C E9 5F 29 BE A5 1E 77 80 C0 D7 CA E4 99 F4 2B CE 15 8E 26 1A EF 16 F8 10 33 4B 27 B8 99 92 31 78 31 3C 43 CB CC 15 0D 5D EF 03 8F C6 24 C2 72 B8 FF 75 87 D5 E5 1B DB 42 51 12 32 68 2E 0E D3 8B 82 4E C5 AB C4 1A CE D4 DE 02 5E 0C 5A 7D 02 02 3D A6 C2 61 25 5B 56 6F 39 6A 5C 1A 19 CB F7 5A 2C 16 D5 93 52 5B 78 60 D4 B5 4A 37 55 1E 51 26 1D 1D D6 CD 92 65 B4 9E 61 12 C8 4C 8F CA 53 F0 8C E8 42 43 95 0D E1 E0 18 C5 E5 70 29 2A 7C D2 AC AF 15 AB 54 4D F1 2B 12 B4 53 EC 9E 41 41 30 54 56 FC FE 37 79 5D FA 02 D1 BC 84 AF B1 86 2A FF 36 FF 07 FE B8 AB 1E 7D A0 9C F3 BE 68 25 E2 AF 1D ED 36 55

publicExponent

- This is the RSA public exponent e.
- **Value:** 0x 01 00 01

privateExponent

- This is the RSA private exponent d.
- **Value:** 0x 56 A6 C3 56 03 12 E7 C9 F4 08 D0 DD 03 FF 5A 64 5F 06 33 6D B6 71 DD 1D FF F4 93 43 48 14 9D 98 C4 F9 E9 FC 11 6B 11 24 05 53 92 E4 57 9E 58 97 43 79 74 01 6A F5 CD E8 A3 A3 7C F1 5F 11 FE 4F BE B3 47 15 31 DD 61 0D B2 5F 5D 48

E2 39 0E 87 88 C1 B8 95 BC 06 65 18 B4 23 DA 9D D6 F7 32 0B 0E 4D 84 58 C8 98 07 46 26 E5 34 8D FA 85 43 A1 7A 4C 1E F0 C6 4B DC 4C 82 0F C0 33 06 3F DE B7 15 96 6D 7C BE E6 F6 D8 C0 97 90 26 21 6C DD 3B 21 A3 54 0A D8 FC 6E 6B 80 E8 78 60 A2 32 C0 52 D8 28 84 09 99 1B CA D4 8D 8F 18 9E E8 08 D4 A7 3C 5F A5 B9 29 72 84 68 45 83 2C 43 1C 3E 17 78 B9 64 9B C1 F2 E1 8A F7 28 7E CD 5F B4 C7 C9 59 15 A0 72 70 99 81 57 59 81 48 1D 83 79 4D B0 72 1F F9 4C CF 3C 64 B8 34 1B FB 40 2C 02 9D 9D 8A E9 23 FF 4C 8E 06 97 B0 0C 3F 76 50 CB 82 A6 22 04 E1 89 28 1C B4 6B 4F E7 59 18 43 F7 E6 FA A8 F3 A9 95 59 F6 7A 98 23 14 C8 E5 EA D4 5F E2 64 33 8B FF CF 3F D0 41 6F 13 FD A6 C7 01 54 99 5C 9F AC 2A 5A 55 78 A9 89 72 26 6F 63 92 E5 BF 91 82 C3 D5 1F 0D B9 38 2A B5 37 7C 7E 95 58 FD F5 7B AE E5 6D 3F A2 60 58 F9 30 E9 32 59 BA 16 41 67 D8 A5 96 C3 F5 CC F4 4C 50 9B 7D 82 50 29 CE 80 66 26 A9 5B 8F CA 9A CB AE 91 50 96 52 A2 7D

prime1

- This is the prime factor p of n.
- **Value:** 0x 00 E9 DA 7F 2D AA DE 2F A6 A8 0D 93 2A 39 CF E4 BC E5 84 60 E7 62 07 DF 22 90 21 FA 87 E2 0E 10 BF 45 A5 1D 62 07 4B 61 0F AE 49 CE 7B 11 7C 62 01 A5 22 79 98 83 0A AE C0 3B D1 20 72 2B 7D 3A 5E 6E A7 94 0D CF 6A 2D 27 D4 D6 7C A1 E8 25 63 6A 85 C1 D5 7B 8A 81 07 1E 9A DB F6 6C 6B E5 59 81 15 D8 65 BC C6 36 68 6D E0 28 D0 EE 10 A3 8E 39 8D 58 80 82 0F A4 24 14 62 70 A6 82 72 1C 9F B9 F0 1A EF FB DB CC 50 65 9B 84 54 DD BD 8A 91 D8 D5 1C 70 77 9A 6D 2D C5 20 BD 4A 2A EE 44 6C C4 EF D0 17 FF 47 ED E3 01 3C 54 3A EE E5 A6 8F E1 77 C8 FD DB 0B 6C F3 D8 C7 19 F0 02 F4 DE DB 17

prime2

- This is the prime factor q of n.
- **Value:** 0x 00 E2 A5 69 F8 82 5F ED 2D 21 7C 05 44 70 F7 65 07 FD 1D A1 D4 0B 86 EF 96 01 CB 1B C7 65 CA 75 14 B3 BF C0 B7 E8 27 91 82 89 61 9D 1F B9 9B 06 0C F8 AD 8F BC 96 8E 15 85 DD FD 66 AA 2A 40 2F B8 FD 5D 94 D0 B4 4E 3E B5 F0 D1 CE 3A B4 B3 AF 27 84 29 7E 25 CF 76 23 A9 A3 A0 19 DC 43 0B 44 2A CB E6 4D 96 53 D3 0D 60 64 98 19 8E A8 E4 0A 20 8C 0B 58 D7 C7 DB 5B F4 1D 66 9A 25 C4 8A F4 F0 B3 6C 16 FA 37 10 FE F2 F7 AD 8A 0F EC 33 0C 21 A4 B6 4A D9 53 31 23 F8 50 41 6C AB 51 83 BB AF 50 68 19 1A 91 47 1A EB 2D 4F CE 46 C9 BF 2B A4 29 AA 63 9D 58 42 51 B0 04 3E E8 3C 8E B8 6D 73

exponent1

- Is d mod (p - 1).
- **Value:** 0x 46 4D 4F 6A 75 31 B2 75 91 93 F3 28 00 95 45 18 9C 8F 3D 6A 92 07 F7 C6 B6 39 E0 CD 34 E2 31 9A AE DF 42 84 13 D9 4F 66 9D 68 C6 D0 2C A3 8D FB 1C 9F CE 9A 50 DA C7 4A 37 31 59 65 B9 39 3E 70 E1 27 33 D5 2B 03 AA 6B 8D 0A A6 11 2E 6E FF 02 29 0F EA 93 E7 41 7E D8 6E 89 AD FD 4E 3A 76 BB DD CB 5E 5A 6F E4 2F 64 C8 BC BC 82 B5 31 D6 31 EB 12 2E 1F EB 7F D6 F0 E1 DF 27 CF 93 6A 93 82 1C 72 9C AE C4 97 19 9C 52 32 68 28 F9 30 4D 44 38 5D 02 5A 92 6C 3C 14 45 11 62 D8 A1 24 A4 E6 57 89 E1 8C F7 1C C6 DF BA 39 40 36 4D 87 D3 3D 5E FB 67 85 90 5B C2 BA EA B0 1B 7D 68 0C 0F 25

exponent2

- Is d mod (q - 1).
- **Value:** 0x 00 BA 17 3B 25 52 56 D4 F4 83 53 C3 37 68 D1 98 60 B0 D1 0D B8 7F 26 71 BD 67 07 8F 6D 6F 04 86 91 52 ED 14 9D 6B BE 61 59 1E D7 C9 1C ED 56 7D E7 54

9F 9D 2F 29 26 CC 41 37 FE 01 B7 A2 2D 45 81 CC 76 73 E3 D0 C7 95 F1 E9 23 3B 03 34 AF 7C 17 24 0A B5 8A F2 06 7C 4D A3 0D A7 6E 14 96 41 88 2A 16 94 89 E3 95 9C 9C 12 BC 57 EF AC 78 60 60 4C DC 5C 3B FF DA FA 6B 3B 60 AD 1C 69 7D F6 93 53 9E 62 57 5B B3 56 C1 C3 DE F7 47 0F 96 F2 55 05 5A AF A6 35 0A 5A 10 5E 44 F9 A6 C8 AD 33 03 45 2F D3 BC DE 9F D5 58 57 C1 F9 0A 62 47 D6 DB 59 62 8F 9B F7 85 AC 70 AB 6B C3 5F 45 87 E4 45

coefficient

- Is the inverse of q mod p.
- **Value:** 0x 5B CB 7B 87 C6 92 8B 00 24 22 D3 38 1D 1C 95 7F 9C C8 24 3A FD 8F 29 BA A2 31 CF AB DC CF 8B E7 4B 4B 34 F8 98 31 67 DA 06 B4 4A 49 10 15 F6 05 3E 30 C7 9A 9A 2B F6 C4 60 AE 63 C7 E6 D8 95 C3 6F 82 6E D7 14 92 A6 67 7F B8 E4 0E 9C 71 13 02 18 95 B1 86 E8 A2 D0 A2 B7 75 6A C5 C2 A1 C8 05 25 36 F9 7A 5B 70 96 DA C0 C9 B9 95 44 F7 9C 73 8D 2A A5 0B 6E 54 71 D3 38 68 BE 09 32 94 8C 6D 7D 4C A1 9D 3D AC 0C FC 07 8C D0 9F F9 28 73 7F 71 E1 13 93 31 49 77 E8 E1 08 AA AB AE B4 A2 EF D0 06 E1 4F A6 33 53 B5 47 B4 87 34 E6 6F 34 05 46 BB 23 77 E7 E7 4F BB C6 77 82 A8 41 0D 81 5C

Public Key

According to RFC 8017, the structure of an ASN.1 RSA Public Key should be a sequence of two integers: modulus (n) and publicExponent (e) (Moriarty, Kathleen, et al). These integers can be set to varying arbitrary lengths and should be the same values found in the RSA Private Key.

The RSA Public Key contained in **id_rsa_homework.pub** after decoding it further using the command: *ssh-keygen -f id_rsa_homework.pub -e -m pem* was input into the text box and then I pressed decode using https://lapo.it/asn1js/, an ASN.1 JavaScript decoder.

The integers within the RSA Public Key are detailed below (Moriarty, Kathleen, et al):

Modulus

- This provides what modulus (n) the RSA Public and Private Key are in, where p * q = n.
- **Value:** 0x 00 CF 09 FE E7 EA 34 CB EB 64 03 24 F2 D1 FB 43 2B 1A C3 7A 7F 4D B1 E0 8B BF 1A 35 AA 1C 21 17 AC 2C B6 5C 5C 6E 29 2E E8 CF B7 34 03 58 96 73 F3 AE 49 09 63 52 CE 5D 69 22 56 86 29 CB 4C 84 5C 5E E4 06 C2 FA A8 4D FA BF D8 20 1B C5 5E 4C DA E0 10 70 5D D2 A9 1B F1 C9 AA D9 DE FE 73 76 00 78 4A 9D 95 97 7E 9A 7C 0E ED 56 7B A7 F6 59 D4 5B 7A EB 98 BF C8 C5 91 7F 98 AF 1D D2 DF 80 63 0B EE BE 5E E2 83 85 5B F9 2B C9 F5 3E 83 7D F8 51 4B DD D2 D1 7C 6A 49 25 B2 4D CB 07 BB 41 B1 49 D4 31 1C BF 61 72 7E 51 A9 80 6F 1B BE BF AF 85 2A 32 3D 1F E8 3C 81 4D 1D 6C E9 5F 29 BE A5 1E 77 80 C0 D7 CA E4 99 F4 2B CE 15 8E 26 1A EF 16 F8 10 33 4B 27 B8 99 92 31 78 31 3C 43 CB CC 15 0D 5D EF 03 8F C6 24 C2 72 B8 FF 75 87 D5 E5 1B DB 42 51 12 32 68 2E 0E D3 8B 82 4E C5 AB C4 1A CE D4 DE 02 5E 0C 5A 7D 02 02 3D A6 C2 61 25 5B 56 6F 39 6A 5C 1A 19 CB F7 5A 2C 16 D5 93 52 5B 78 60 D4 B5 4A 37 55 1E 51 26 1D 1D D6 CD 92 65 B4 9E 61 12 C8 4C 8F CA 53 F0 8C E8 42 43 95 0D E1 E0 18 C5 E5 70 29 2A 7C D2 AC AF 15

AB 54 4D F1 2B 12 B4 53 EC 9E 41 41 30 54 56 FC FE 37 79 5D FA 02 D1 BC 84 AF

B1 86 2A FF 36 FF 07 FE B8 AB 1E 7D A0 9C F3 BE 68 25 E2 AF 1D ED 36 55

publicExponent

- This is the RSA public exponent e.
- **Value:** 0x 01 00 01

Sanity Check

Running the below code in Python confirms that the values work:

```
from math import lcm, gcd

p =
220179689286137632070003645911696407087048780199297518855438713377811133306546817205108630033471418161951436955044766211296085653553568694506662825998389021693084924422490845819597430691053821586238819641178618296347733258440110302878935723047682784950406426021308605375565241482077937835540361973728555345912796273202459000926806248987929881740425372353267325769612791469805870089839406908346383327119201128001890415659469481718729153483467605362333345799935464 7
q =
213393760783199008380196192076823685491925261783615840323834183947699978558083283539670710747570214263275102092029285216885902502648923084616941698193133217987683280427037999768131627555061956207923638429247268855168929024628278613418745625184160752393840671898273086759722083175344408920154608017519733747101371529544236149181747522548061634448219858572418479125303943515521863523113003826317526798796853333124388760452395786564755433340678959054025877369916145 9
n =
469849719448451394992773622427491076235603953439360720640382486034436387675519037298020216682546370514340576363182512461551256578197953913222957744648845085134696490528690008795526682582879127123289512964822741178415027152519315107692878001324910565410759818316150519849898253667880847508876225526548713185938765359504831882570165340268862052915606042275856796910030603970971063590423519649055711377320115448737929352277484697138006006721949022055070254745849802986555430770408119919675673633221572373693095888342888120076853584569769682725672770652908150670523535066762897616219346228131590273798141120295410416671442824610477289768239359979926714504374692288813781879136706815738299303655373010959342531754256177995495451038842774853469041398066555436677328609319575772142380646759750083506973287882104157011524403517900484217512951251988159147323520019481650860092616002948007633503196801776091974995516331841214705494997 3
e_Private_d =
196644764861857779771760637435899221823760751772010498870111724588942990608635072409081362190146695277148430514935553093350232186916044049283993465976955283299447646171084769100279441623173410114089453455623993741359198584990508276074271129032603246815040520102185423342975601546653610375965636200574431844166561643935 1
```

```
867963161367041876523565958402327821652017097562348474549190871914674846192391120303716440228671137859724671251913817196911250054964397857567838359617847398705479909444582294760042860291025790052259513422518927811656457487289771710757864337479975902925059922065129755204316862020237739344672886487774894257733438098069455527520666845940947415674824070650246880931457523419810471187429470758665930519852740189793387948447911973417134008713484712002550572172508996249313689963487575883756327447188311116697314388877774900251686192933441442195031341108915745532111337117569202462265258763602376910059708504 29

e_Public_e = 65537

lambda_n = lcm(p - 1, q - 1)

gcd_e_lambda = gcd(e_Public_e, lambda_n)

test_d = (e_Public_e * e_Private_d) % lambda_n

print("Test p * q = n:", hex(p * q))
print("Value of n:", hex(n))
print("Test (e*d*mod(lambda(n))) = 1?", test_d)
print("Test gcd( e, lambda) = 1?", gcd_e_lambda)
```

Where the calculated hexadecimal value of n by multiplying p and q together matches the hexadecimal value after both being printed. The last two print statements also equal one, where e*d*mod(lambda(n)) should equal 1 and gcd(e, lambda) should also equal one. Therefore, confirming the validity of the values.

id_rsa_homework

-----BEGIN RSA PRIVATE KEY-----

MIIG4wIBAAKCAYEAzwn+5+o0y+tkAyTy0ftDKxrDen9NseCLvxo1qhwhF6wstlxc

biku6M+3NANYlnPzrkkJY1LOXWkiVoYpy0yEXF7kBsL6qE36v9ggG8VeTNrgEHBd

0qkb8cmq2d7+c3YAeEqdlZd+mnwO7VZ7p/ZZ1Ft665i/yMWRf5ivHdLfgGML7r5e

4oOFW/kryfU+g334UUvd0tF8akklsk3LB7tBsUnUMRy/YXJ+UamAbxu+v6+FKjI9

H+g8gU0dbOlfKb6lHneAwNfK5Jn0K84VjiYa7xb4EDNLJ7iZkjF4MTxDy8wVDV3v

A4/GJMJyuP91h9XlG9tCURIyaC4O04uCTsWrxBrO1N4CXgxafQICPabCYSVbVm85

alwaGcv3WiwW1ZNSW3hg1LVKN1UeUSYdHdbNkmW0nmESyEyPylPwjOhCQ5UN4eAY

xeVwKSp80qyvFatUTfErErRT7J5BQTBUVvz+N3ld+gLRvISvsYYq/zb/B/64qx59

oJzzvmgl4q8d7TZVAgMBAAECggGAVqbDVgMS58n0CNDdA/9aZF8GM222cd0d//ST

Q0gUnZjE+en8EWsRJAVTkuRXnliXQ3l0AWr1zeijo3zxXxH+T76zRxUx3WENsl9d

SOI5DoeIwbiVvAZlGLQj2p3W9zILDk2EWMiYB0Ym5TSN+oVDoXpMHvDGS9xMgg/A

MwY/3rcVlm18vub22MCXkCYhbN07IaNUCtj8bmuA6HhgojLAUtgohAmZG8rUjY8Y

nugI1Kc8X6W5KXKEaEWDLEMcPhd4uWSbwfLhivcofs1ftMfJWRWgcnCZgVdZgUgd

g3lNsHIf+UzPPGS4NBv7QCwCnZ2K6SP/TI4Gl7AMP3ZQy4KmIgThiSgctGtP51kY

Q/fm+qjzqZVZ9nqYIxTI5erUX+JkM4v/zz/QQW8T/abHAVSZXJ+sKlpVeKmJciZv

Y5Llv5GCw9UfDbk4KrU3fH6VWP31e67lbT+iYFj5MOkyWboWQWfYpZbD9cz0TFCb

fYJQKc6AZiapW4/KmsuukVCWUqJ9AoHBAOnafy2q3i+mqA2TKjnP5LzlhGDnYgff

IpAh+ofiDhC/RaUdYgdLYQ+uSc57EXxiAaUieZiDCq7AO9Egcit9Ol5up5QNz2ot

J9TWfKHoJWNqhcHVe4qBBx6a2/Zsa+VZgRXYZbzGNmht4CjQ7hCjjjmNWICCD6Qk

FGJwpoJyHJ+58Brv+9vMUGWbhFTdvYqR2NUccHeabS3FIL1KKu5EbMTv0Bf/R+3j

ATxUOu7lpo/hd8j92wts89jHGfAC9N7bFwKBwQDipWn4gl/tLSF8BURw92UH/R2h

1AuG75YByxvHZcp1FLO/wLfoJ5GCiWGdH7mbBgz4rY+8lo4Vhd39ZqoqQC+4/V2U

0LROPrXw0c46tLOvJ4QpfiXPdiOpo6AZ3EMLRCrL5k2WU9MNYGSYGY6o5AogjAtY

18fbW/QdZpolxIr08LNsFvo3EP7y962KD+wzDCGktkrZUzEj+FBBbKtRg7uvUGgZ

GpFHGustT85Gyb8rpCmqY51YQlGwBD7oPI64bXMCgcBGTU9qdTGydZGT8ygAlUUY

nI89apIH98a2OeDNNOIxmq7fQoQT2U9mnWjG0Cyjjfscn86aUNrHSjcxWWW5OT5w

4Scz1SsDqmuNCqYRLm7/AikP6pPnQX7Ybomt/U46drvdy15ab+QvZMi8vIK1MdYx

6xIuH+t/1vDh3yfPk2qTghxynK7ElxmcUjJoKPkwTUQ4XQJakmw8FEURYtihJKTm

V4nhjPccxt+6OUA2TYfTPV77Z4WQW8K66rAbfWgMDyUCgcEAuhc7JVJW1PSDU8M3

aNGYYLDRDbh/JnG9ZwePbW8EhpFS7RSda75hWR7XyRztVn3nVJ+dLykmzEE3/gG3

oi1Fgcx2c+PQx5Xx6SM7AzSvfBckCrWK8gZ8TaMNp24UlkGIKhaUieOVnJwSvFfv

rHhgYEzcXDv/2vprO2CtHGl99pNTnmJXW7NWwcPe90cPlvJVBVqvpjUKWhBeRPmm

yK0zA0Uv07zen9VYV8H5CmJH1ttZYo+b94WscKtrw19Fh+RFAoHAW8t7h8aSiwAk

ItM4HRyVf5zIJDr9jym6ojHPq9zPi+dLSzT4mDFn2ga0SkkQFfYFPjDHmpor9sRg

rmPH5tiVw2+CbtcUkqZnf7jkDpxxEwIYlbGG6KLQord1asXCocgFJTb5eltwltrA

ybmVRPecc40qpQtuVHHTOGi+CTKUjG19TKGdPawM/AeM0J/5KHN/ceETkzFJd+jh

CKqrrrSi79AG4U+mM1O1R7SHNOZvNAVGuyN35+dPu8Z3gqhBDYFc

-----END RSA PRIVATE KEY-----

id_rsa_homework.pub

ssh-rsa

AAAAB3NzaC1yc2EAAAADAQABAAABgQDPCf7n6jTL62QDJPLR+0MrGsN6f02x4Iu/Gj

WqHCEXrCy2XFxuKS7oz7c0A1iWc/OuSQljUs5daSJWhinLTIRcXuQGwvqoTfq/2CAbxV5M

2uAQcF3SqRvxyarZ3v5zdgB4Sp2Vl36afA7tVnun9lnUW3rrmL/IxZF/mK8d0t+AYwvuvl7ig4V

b+SvJ9T6DffhRS93S0XxqSSWyTcsHu0GxSdQxHL9hcn5RqYBvG76/r4UqMj0f6DyBTR1s6V

8pvqUed4DA18rkmfQrzhWOJhrvFvgQM0snuJmSMXgxPEPLzBUNXe8Dj8YkwnK4/3WH1e
Ub20JREjJoLg7Ti4JOxavEGs7U3gJeDFp9AgI9psJhJVtWbzlqXBoZy/daLBbVk1JbeGDUtUo3
VR5RJh0d1s2SZbSeYRLITI/KU/CM6EJDlQ3h4BjF5XApKnzSrK8Vq1RN8SsStFPsnkFBMF
RW/P43eV36AtG8hK+xhir/Nv8H/rirHn2gnPO+aCXirx3tNlU= ryanson@Ryans-MacBook-Air-7.local

RSA Public Key (ssh-keygen -f id_rsa_homework.pub -e -m pem)

-----BEGIN RSA PUBLIC KEY-----
MIIBigKCAYEAzwn+5+o0y+tkAyTy0ftDKxrDen9NseCLvxo1qhwhF6wstlxcbiku
6M+3NANYlnPzrkkJY1LOXWkiVoYpy0yEXF7kBsL6qE36v9ggG8VeTNrgEHBd0qkb
8cmq2d7+c3YAeEqdlZd+mnwO7VZ7p/ZZ1Ft665i/yMWRf5ivHdLfgGML7r5e4oOF
W/kryfU+g334UUvd0tF8akklsk3LB7tBsUnUMRy/YXJ+UamAbxu+v6+FKjI9H+g8
gU0dbOlfKb6lHneAwNfK5Jn0K84VjiYa7xb4EDNLJ7iZkjF4MTxDy8wVDV3vA4/G
JMJyuP91h9XlG9tCURIyaC4O04uCTsWrxBrO1N4CXgxafQICPabCYSVbVm85alwa
Gcv3WiwW1ZNSW3hg1LVKN1UeUSYdHdbNkmW0nmESyEyPylPwjOhCQ5UN4eAYxeVw
KSp80qyvFatUTfErErRT7J5BQTBUVvz+N3ld+gLRvISvsYYq/zb/B/64qx59oJzz
vmgl4q8d7TZVAgMBAAE=
-----END RSA PUBLIC KEY-----

Works Cited

Moriarty, Kathleen, et al. “RFC 8017: PKCS #1: RSA Cryptography Specifications Version 2.2.” IETF Datatracker, Internet Engineering Task Force (IETF), Nov. 2016, datatracker.ietf.org/doc/html/rfc8017#appendix-A.1.