

LAB: Certificates PKI and Apache

John Gavigan

jsg5514@psu.edu

SRA 221

Professor Stout

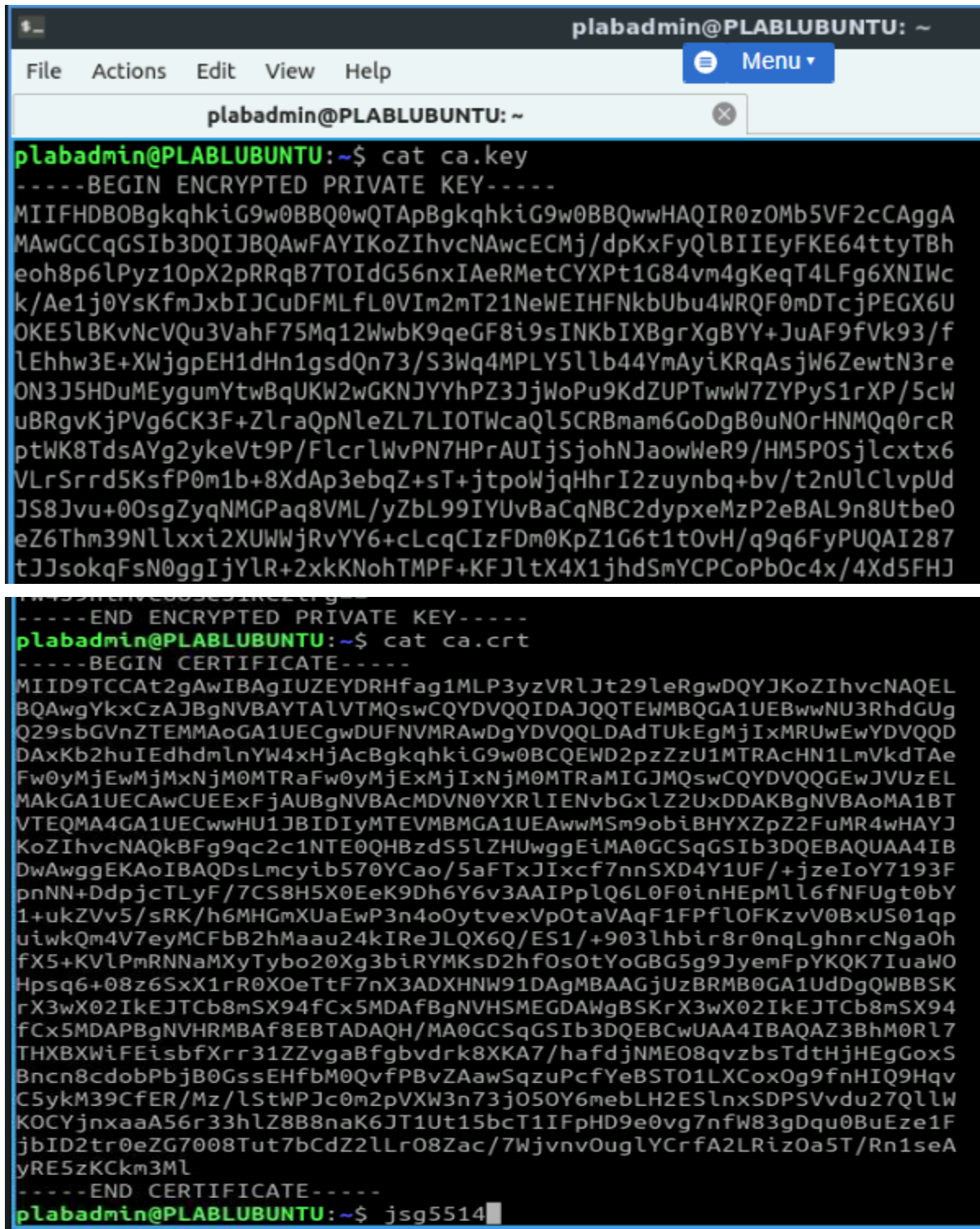
10/21/2022

By submitting this report I certify that this is my work and was not copied from other sources.

Any use of public material is cited

Task 1

1.1 This is a screenshot of the CA's private key and the CA's public key

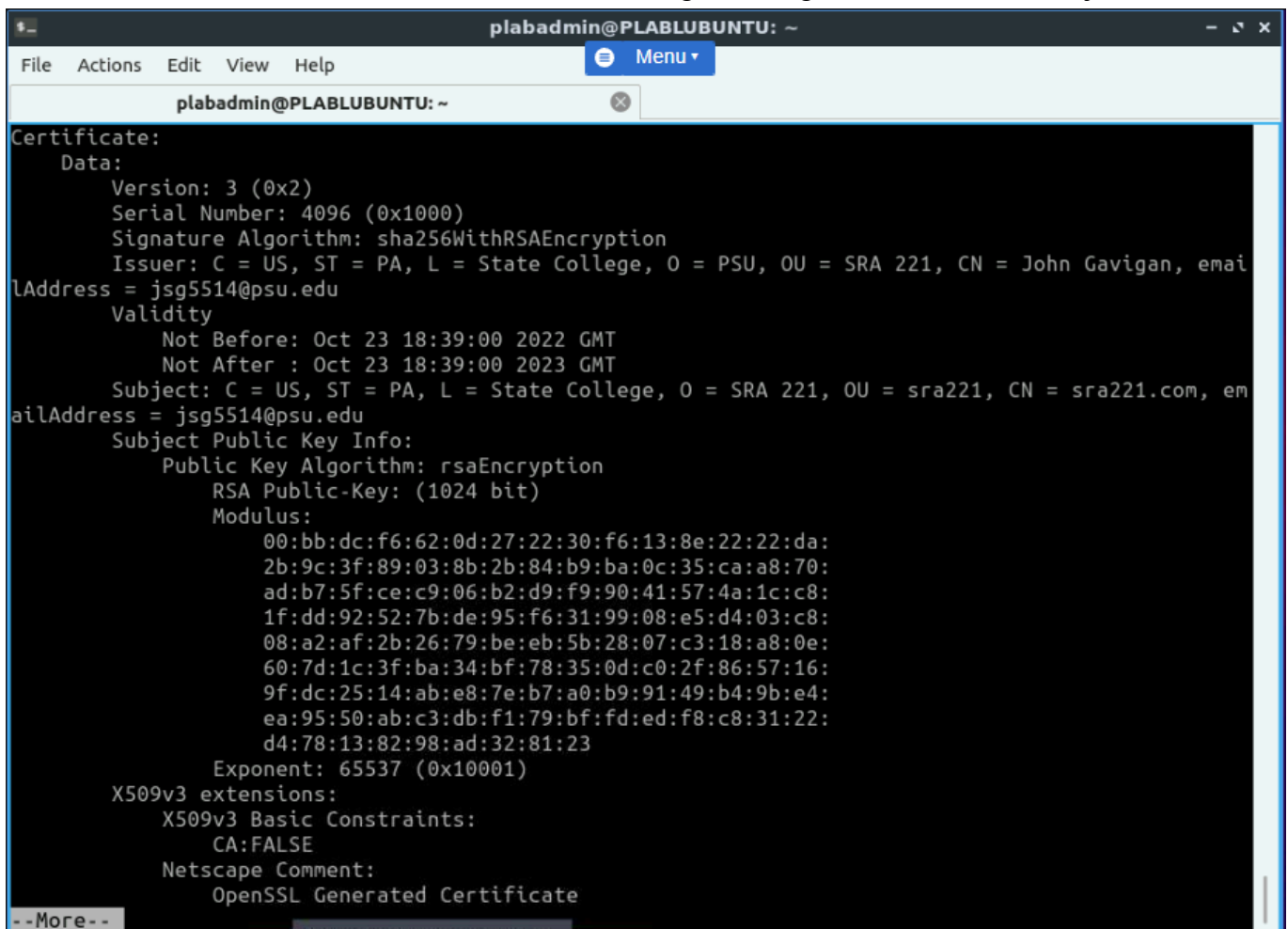


```
plabadmin@PLABLUBUNTU: ~  
File Actions Edit View Help Menu  
plabadmin@PLABLUBUNTU: ~  
plabadmin@PLABLUBUNTU:~$ cat ca.key  
-----BEGIN ENCRYPTED PRIVATE KEY-----  
MIIFHDBOBBgkqhkiG9w0BBQ0wQTApBgkqhkiG9w0BBQwwHAQIR0zOMb5VF2cCAggA  
MAwGCCqGSIb3DQIJBQAwFAYIKoZIhvcNAwcECMj/dpKxFyQlBIIEyFKE64ttyTBh  
eoh8p6lPyz10pX2pRRqB7TOIdG56nxIAeRMetCYXPt1G84vm4gKeqT4LFg6XNIWc  
k/Ae1j0YsKfmJxbIJCuDfMLfL0VIm2mT21NeWEIHFNkbUbu4WRQF0mDTcjPEGX6U  
OKE5lBKvNcVQu3VahF75Mq12WwbK9qeGF8i9sINKbIXBgrXgBYy+JuAF9fVkd93/f  
lEhhw3E+XWjgpEH1dHn1gsdQn73/S3Wq4MPLY5llb44YmAyiKRqAsjW6ZewtN3re  
ON3J5HDuMEygmYtwBqUKW2wGKNJYYhPZ3JjWoPu9KdZUPTwwW7ZYPyS1rXP/5cW  
uBRgvKjPVg6CK3F+ZlraQpNleZL7LIOTWcaQl5CRBmam6GoDgB0uNORHNMqQ0rcR  
ptWK8TdsAYg2ykeVt9P/FicrlWvPN7HPrAUIjSjohNJaowWeR9/HM5POSjlcctx6  
VLrSrrd5KsfP0m1b+8XdAp3ebqZ+sT+jtpoWjqHhrI2zuynbq+bv/t2nUlClvpUd  
JS8Jvu+00sgZyqNMGPaq8VML/yZbL99IYUvBaCqNBC2dypxeMzP2eBAL9n8Utbe0  
eZ6Thm39Nllxxi2XUWWjRvYY6+cLcqCIzFDm0KpZ1G6t1t0vH/q9q6FyPUQAI287  
tJJsokqFsN0ggIjYlR+2xkKNohTMPF+KFJlTx4X1jhdSmYCPCoPb0c4x/4Xd5FHJ  
-----END ENCRYPTED PRIVATE KEY-----  
plabadmin@PLABLUBUNTU:~$ cat ca.crt  
-----BEGIN CERTIFICATE-----  
MIID9TCCAt2gAwIBAgIUZEYDRHfag1MLP3yzVRLJt29leRgwDQYJKoZIhvcNAQEL  
BQAwYkxkCzAJBgNVBAYTA1VMTQswCQYDVQQLIDAJQQTETWMBQGA1UEBwwNU3RhZGUg  
Q29sbGVnZTEMAAoGA1UECgwDUFNVMRAwDgYDVQQQLDAdTUkEgMjIxMRUwEwYDVQQD  
DAxKb2huIEthdmlnYW4xHjAcBgkqhkiG9w0BCQEWDPzZzU1MTRAcHN1LmVkdTAe  
Fw0yMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEw  
MAkGA1UECAwCUExEExFAUjAUBGNVBAcMDVN0YXRlIENvbGx1Z2UxDDAKBgNVBAoMA1BT  
VTEQMA4GA1UECwwHU1JBIDImTEVMBMGA1UEAwwMSm9obiBHXYXpZ2FuMR4wHAYJ  
KoZIhvcNAQkBFg9qc2c1NTE0QHBzdS5lZHUwggEiMA0GCSqGSIb3DQEBQUAA4IB  
DwAwggEKAoIBAQDsLmcyib570YCAo/5aFTxJlxcF7nnSXD4Y1UF/+jzeIoY7193F  
pnNN+DdpjcTLyF/7CS8H5X0EeK9Dh6Y6v3AAIPpLQ6L0F0inHEpMll6fNFUgt0bY  
1+ukZVv5/sRK/h6MHGmXUaEwP3n4o0ytvexVpOtaVAqF1FPfLOFKzvV0BxUS01qp  
uiwkQm4V7eyMCFbB2hMaau24kIREJLQX6Q/ES1/+903lhbir8r0nqLghnrcNga0h  
fX5+KVlPmRNNaMXyTybo20Xg3biRYMKsD2hfOsOtYoGBG5g9JyemFpYKQK7IuaW0  
Hpsq6+08z6SxX1rR0X0eTtF7nX3ADHXHNW91DAgMBAAGjUzBRMB0GA1UdDgQWBBSK  
rX3wX02IkeJTCb8mSX94fCx5MDAfbGnVHSMEGDAWgBSKrX3wX02IkeJTCb8mSX94  
fCx5MDAPBgNVHRMBAf8EBTADAQH/MA0GCSqGSIb3DQEBQwUAA4IBAQA3BhM0RL7  
THXBXWiFEisbfXrr31ZZvgaBfgbvdRk8XKA7/hafdjNME08qvzbsTdtHjHEGoxS  
Bncn8cdobPbjB0GssEHfbM0QvFPBvZAawSqzuPcfYeBSTO1LXCoxOg9fnHIQ9Hqv  
C5ykM39CFER/Mz/lStWPJc0m2pVXW3n73j05OY6mebLH2ESlnxSDPSVvdu27QllW  
KOCYjnxaaaA56r33hLZ8B8naK6JT1Ut15bcT1IFpHD9e0vg7nfW83gDqu0BuEze1F  
jbID2tr0eZG7008Tut7bCdZ2LLr08Zac/7Wjvnnv0ugLYCrfa2LRizOa5T/Rn1seA  
yRE5zKCKm3Ml  
-----END CERTIFICATE-----  
plabadmin@PLABLUBUNTU:~$ jsg5514
```

1.2 The ca.key and ca.crt files are both important because they contain the private and public keys generated by the root CA in the self-signed certificate. This is used by the CA to verify the ID and authenticity of other entities.

Task 2

2.1 This screenshot shows the new certificate with the signature algorithm, issuer, and subject

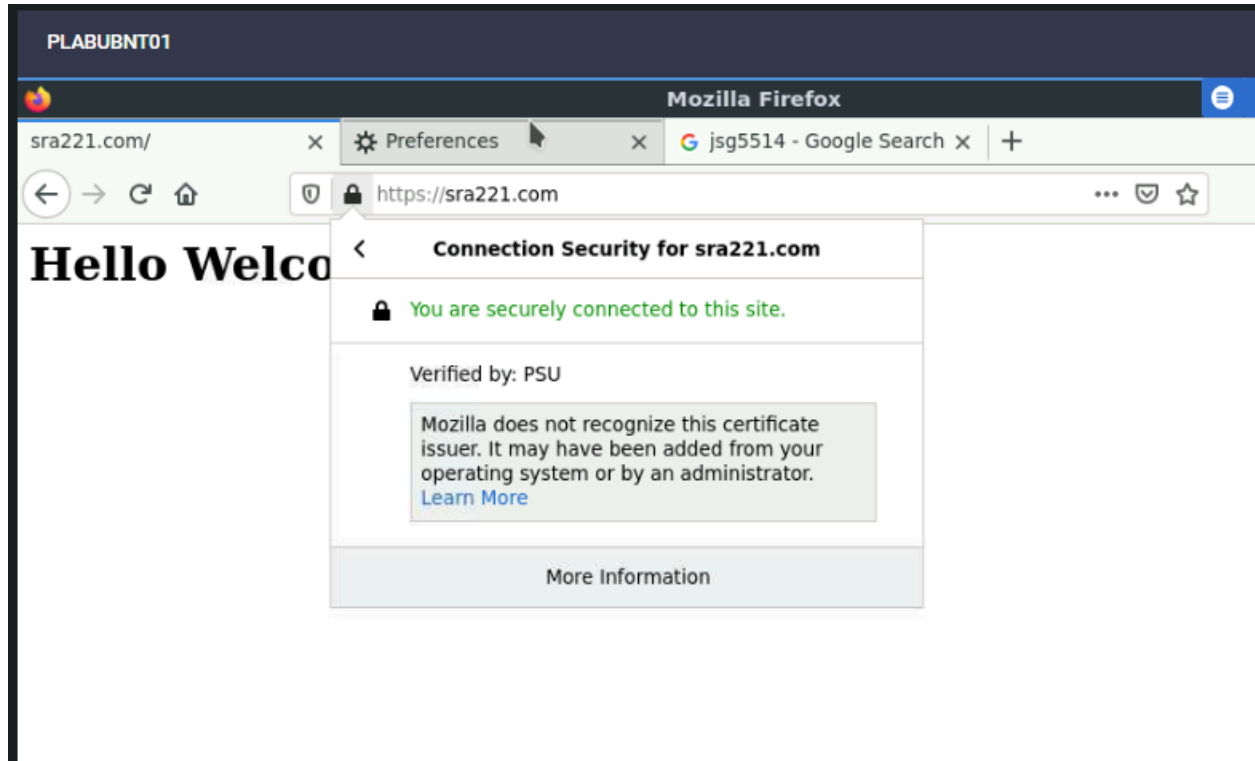
A screenshot of a terminal window titled 'plabadmin@PLABLUBUNTU: ~'. The window has a menu bar with 'File', 'Actions', 'Edit', 'View', 'Help', and a 'Menu' button. The terminal output displays the details of a new certificate. The 'Certificate:' section includes 'Data:' (Version: 3 (0x2), Serial Number: 4096 (0x1000), Signature Algorithm: sha256WithRSAEncryption, Issuer: C = US, ST = PA, L = State College, O = PSU, OU = SRA 221, CN = John Gavigan, emailAddress = jsg5514@psu.edu), 'Validity' (Not Before: Oct 23 18:39:00 2022 GMT, Not After: Oct 23 18:39:00 2023 GMT), 'Subject: C = US, ST = PA, L = State College, O = SRA 221, OU = sra221, CN = sra221.com, emailAddress = jsg5514@psu.edu', 'Subject Public Key Info:' (Public Key Algorithm: rsaEncryption, RSA Public-Key: (1024 bit), Modulus: a long hexadecimal string, Exponent: 65537 (0x10001)), 'X509v3 extensions:' (X509v3 Basic Constraints: CA:FALSE, Netscape Comment: OpenSSL Generated Certificate), and a '--More--' prompt at the bottom.

```
plabadmin@PLABLUBUNTU: ~
File Actions Edit View Help Menu
plabadmin@PLABLUBUNTU: ~
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 4096 (0x1000)
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: C = US, ST = PA, L = State College, O = PSU, OU = SRA 221, CN = John Gavigan, email
Address = jsg5514@psu.edu
    Validity
      Not Before: Oct 23 18:39:00 2022 GMT
      Not After : Oct 23 18:39:00 2023 GMT
    Subject: C = US, ST = PA, L = State College, O = SRA 221, OU = sra221, CN = sra221.com, em
ailAddress = jsg5514@psu.edu
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public-Key: (1024 bit)
      Modulus:
        00:bb:dc:f6:62:0d:27:22:30:f6:13:8e:22:22:da:
        2b:9c:3f:89:03:8b:2b:84:b9:ba:0c:35:ca:a8:70:
        ad:b7:5f:ce:c9:06:b2:d9:f9:90:41:57:4a:1c:c8:
        1f:dd:92:52:7b:de:95:f6:31:99:08:e5:d4:03:c8:
        08:a2:af:2b:26:79:be:eb:5b:28:07:c3:18:a8:0e:
        60:7d:1c:3f:ba:34:bf:78:35:0d:c0:2f:86:57:16:
        9f:dc:25:14:ab:e8:7e:b7:a0:b9:91:49:b4:9b:e4:
        ea:95:50:ab:c3:db:f1:79:bf:fd:ed:f8:c8:31:22:
        d4:78:13:82:98:ad:32:81:23
      Exponent: 65537 (0x10001)
    X509v3 extensions:
      X509v3 Basic Constraints:
        CA:FALSE
      Netscape Comment:
        OpenSSL Generated Certificate
--More--
```

Task 3

Challenge and Analysis Deliverables

1. This is a screenshot showing that the sra221 site is trusted



2. I was able to get the browser to trust sra221.com because I imported the proper certificate to firefox. The ca.crt file contains the public key created earlier by the root CA, the browser was able to verify the public key of sra221.com by looking at the signature that was created earlier by the CA.