★ Team Members:
Kritik Agarwal (CS23MTECH11009), Rohit Sutrave (CS23MTECH14010)

Part A: Secure file transfer between Alice (student A) and Bob (student B)

1. **Alice and Bob create RSA (2048) key pairs and exchange their public keys over email. They also password protect their respective private keys.**

Alice	Bob

Creating Encrypted Private Key
 	
$ openssl genpkey -out alice09_private.pem -algorithm RSA -pkeyopt rsa_keygen_bits:2048 -aes-256-cbc
... †. . . . .†.+ ...
++++++++++++++++++++++++++++++++++++++★.
++++++++++++★.
++++++
, . . + ... ++++++++++++++++++++++++++++
// Enter PEM pass phrase: 11009
// Verifying Enter PEM pass phrase: 11009
	Creating Encrypted Private Key
	
	$ openssl genpkey -out BOB10enc.pem -algorithm RSA -pkeyopt rsa_keygen_bits:2048 -aes-256-cbc
	+++++++★ ... +.+ .. + ..
	++++++++++++++++++★++++++++++++++★.
	+++++++★+++++.
	++++★++
	, . . ★ ... +++++++++★+++++++++
	// Enter PEM pass phrase: 14010
	// Verifying Enter PEM pass phrase: 14010

Creating Public Key from Private Key
 	
$ openssl rsa -in alice09_private.pem -pubout -out alice09_public.pem
// Enter pass phrase for alice09_private.pem: 11009
writing RSA key
	Creating Public Key from Private Key
	
	$ openssl rsa -in BOB10enc.pem -pubout -out BOB10pub.pem
	// Enter pass phrase for BOB10enc.pem: 14010
	writing RSA key

Displaying the contents of Encrypted Private Key
 	
$ openssl pkey -in alice09_private.pem -text -noout
// Enter pass phrase for alice09_private.pem: 11009
Private-Key: (2048 bit, 2 primes)
modulus:
00:8d:9e:96:63:92:0c:15:46:f1:d3:36:75:48:ef:
67:8c:8a:34:f2:80:12:7b:8a:3b:ce:eb:6d:f2:89:
92:25:ce:46:bc:1c:2d:28:ea:55:9e:7a:d0:9d:20:
28:2c:86:35:d7:02:c3:e8:1b:b7:f5:da:a1:76:93:
2f:44:ff:c3:d9:a9:6c:31:f8:db:72:fd:2d:0c:c5:
dd:1c:39:92:01:01:f1:66:85:99:e0:33:c6:3b:86:
32:90:9b:2b:f2:df:fe:31:7c:3c:5b:dc:82:3c:df:
4a:af:f1:e5:54:99:1a:46:3b:f9:e0:f6:d4:22:ad:
6d:3f:ef:34:98:69:bd:4a:ea:83:b1:0c:ee:77:ce:
74:ed:f5:c4:73:af:21:9a:37:a0:80:3c:e2:be:92:
43:aa:5d:74:1a:b3:a6:1a:c6:2d:5a:20:80:a1:ed:
29:9e:05:db:61:de:78:8e:36:08:f3:72:af:ec:38:
7d:17:c2:0a:cb:62:6d:ae:4f:d8:da:3c:0f:4b:26:
44:50:31:8c:23:7f:e4:a4:4b:79:10:e6:53:22:48:
98:a5:1c:8f:3e:1e:1c:2e:c1:05:00:68:81:a4:c4:
58:08:61:90:3c:3d:9c:b3:ec:07:f9:fd:23:a7:d5:
a1:72:90:c3:44:ed:64:4f:d7:3a:41:87:3f:28:c6:
23:37
publicExponent: 65537 (0x10001)
privateExponent:
34:6c:bb:06:44:07:c6:0e:9b:b1:90:ec:cc:e1:96:
e6:ff:38:87:76:a2:a0:e9:f4:a6:ee:1f:26:d4:07:
	Displaying the contents of Encrypted Private Key
	
	$ openssl pkey -in BOB10enc.pem -text -noout
	// Enter pass phrase for BOB10enc.pem: 14010
	Private-Key: (2048 bit, 2 primes)
	modulus:
	00:dc:d9:45:02:8c:36:8f:08:7f:ff:73:14:cc:4a:
	c6:64:02:4c:81:5c:2e:fa:3f:a9:1e:6f:b2:06:51:
	f2:ac:19:59:be:33:4a:57:46:31:e2:1a:95:0c:f7:
	34:56:a3:79:a8:fd:3a:ed:a6:78:d8:8b:d5:66:f2:
	4f:8b:7c:c2:7e:b8:60:2c:65:88:14:f8:f2:20:d9:
	0a:b7:50:4f:10:f4:6b:43:b5:a2:83:ff:4a:ef:5c:
	32:d3:3d:ec:aa:ee:7d:22:8b:1c:ea:40:4f:7a:59:
	1d:2d:0f:49:0f:45:56:38:c0:cd:51:0f:40:b6:b2:
	5e:5b:7f:3e:ff:5c:c4:f6:08:7c:62:8f:a7:7e:27:
	49:6c:0a:1f:17:e3:1f:e6:6b:ab:a5:b6:61:7a:d5:
	7e:1b:e8:9d:43:e6:46:b2:90:31:26:e2:32:ee:a7:
	93:5d:34:9a:89:8a:d7:ed:15:4c:2a:28:1a:09:a6:
	c4:6d:0a:54:4b:56:32:05:75:da:ca:a4:69:db:63:
	1b:b8:6c:80:b8:38:e0:0f:ac:a1:2c:f3:a2:c1:80:
	a7:b0:57:31:1a:7b:e0:b4:bd:62:29:40:2e:4c:e8:
	95:3a:82:57:3c:05:62:e3:d2:2d:bb:38:06:22:fb:
	74:dc:15:4c:f9:b5:0e:d8:cd:0c:0e:9a:09:9d:8b:
	dd:4b
	publicExponent: 65537 (0x10001)
	privateExponent:
	42:3e:f0:1a:e8:09:33:95:76:a3:9f:17:15:82:b6:
	88:e8:41:9f:aa:11:b3:62:26:2e:29:8e:0a:a4:49:

```
    6e:88:54:46:09:76:2c:39:c7:15:22:28:bc:a9:ad:
    45:82:2f:47:17:46:77:53:5f:7f:9a:fd:ff:7b:8f:
    d9:8e:86:ad:3a:1b:0b:ca:b0:4d:fa:6b:e5:59:0f:
    b7:85:96:47:5a:35:47:3a:f8:d1:f6:c8:90:bb:66:
    57:82:a1:bb:c8:70:7c:58:1d:ad:f1:cc:a2:85:14:
    4c:5a:93:07:04:a0:25:d4:c8:f5:1e:da:3b:b6:10:
    85:c4:e2:a6:f3:29:b8:23:d8:25:32:44:0a:29:23:
    05:f8:3e:b2:67:94:0e:de:c6:1d:1d:44:c5:cc:c8:
    08:04:81:ec:42:9f:50:ef:d7:1b:65:68:1e:37:62:
    61:8c:fe:f8:37:d2:ae:9d:1e:ed:ec:ad:27:9c:93:
    1d:76:cb:e7:b0:42:99:ff:a4:55:fd:0d:8d:9c:6e:
    65:82:d3:41:ee:e1:c3:87:78:db:e1:e8:20:00:92:
    c0:4a:41:44:a4:62:df:32:8b:c4:62:df:6b:21:b9:
    bb:3e:9d:94:03:01:bd:26:cb:0f:b9:f2:11:81:9c:
    fd:33:a7:f2:b0:b6:ea:af:6c:18:fd:04:94:39:da:
    dd
prime1:
    00:c5:f7:1a:43:8b:50:ad:a4:c1:70:37:aa:64:3a:
    31:09:14:f0:e7:cf:c1:e3:8e:e7:2f:84:63:c3:fd:
    0b:7e:9c:49:74:d2:a7:17:ce:fe:a7:a0:60:f3:75:
    f9:c4:61:27:05:92:3c:a6:94:21:ea:01:d4:8d:f3:
    ea:c0:0b:fd:c7:bc:19:b5:01:d8:52:69:2d:73:8d:
    86:ff:2b:9b:ac:7e:80:84:dc:9f:89:51:48:2e:c1:
    e5:2b:39:c9:34:e8:e8:66:8f:d7:27:8b:8b:2d:22:
    de:51:e3:2e:22:2e:63:3f:d4:0f:b3:28:a9:74:63:
    a3:7a:06:ca:c7:96:55:52:c3
prime2:
    00:b7:22:d8:fc:8f:a6:dc:7a:91:d9:cf:f3:83:87:
    63:10:b4:de:14:b8:b7:c7:b9:de:c4:2c:e9:5e:55:
    cf:e9:bb:13:41:a6:8e:eb:a3:15:c7:9c:2b:6b:8b:
    18:f3:0c:ed:11:ec:43:f9:a7:00:a0:f2:ca:49:7f:
    fc:7d:76:07:54:30:1d:f1:c0:b5:cf:f6:08:fb:23:
    5d:3e:ee:90:6a:91:44:07:ce:d4:83:fa:0a:3e:a8:
    f1:89:23:1e:eb:56:6c:de:1f:b4:31:25:d1:cb:4a:
    13:05:a4:33:ab:84:69:f0:8e:15:60:78:c7:8c:2b:
    4c:e2:12:31:95:a0:90:be:7d
exponent1:
    40:85:79:19:ea:9e:30:fa:31:d1:d1:52:c7:b7:ef:
    a3:76:1f:ce:6d:f8:53:a2:8f:d6:fc:df:47:51:82:
    1d:91:f2:9f:10:c9:45:09:42:16:80:3f:19:1a:aa:
    7d:46:ec:e0:f3:f8:b0:92:37:3b:7d:bd:39:46:f6:
    8c:01:5c:85:6c:d9:34:15:95:db:c6:4b:fa:0d:76:
    a2:54:24:38:e4:42:1f:0b:89:33:c8:3a:2e:83:23:
    9e:23:07:61:27:48:17:a5:6a:0a:89:80:a3:05:6a:
    50:66:2a:f3:19:0b:60:12:4d:cb:a6:c5:14:1a:25:
    7d:f0:18:c7:54:48:1a:e1
exponent2:
    00:ad:28:47:de:55:bd:41:ce:aa:c5:35:b8:5b:ee:
    d1:1e:64:c5:6e:f6:50:de:89:c2:35:de:f9:30:f7:
    16:45:3b:5b:33:c1:d6:74:ba:98:c7:49:c4:4c:45:
    12:ec:0c:96:c3:51:8f:dc:27:a9:92:84:bd:fb:cd:
    05:e1:62:8d:ff:6e:17:82:13:e2:54:a5:9f:4c:45:
    dd:ce:b9:26:d7:7c:4e:c4:cb:2d:69:34:2c:27:9e:
    f9:f1:de:c1:47:67:4a:3c:a3:e1:6e:6f:01:f4:a3:
    2f:65:30:22:a2:d3:ea:8f:46:e8:b3:74:bf:c8:aa:
    d0:61:19:2e:c4:f9:32:a2:c9
coefficient:
    74:a6:ca:4b:a4:f6:b5:19:8e:01:d6:e7:39:9d:9f:
    1d:50:b9:bb:24:db:42:80:38:2a:2d:76:b0:0c:be:
    0f:e0:35:88:52:53:f9:34:da:e7:b3:56:1a:e2:56:
    a5:26:77:d4:61:99:ec:ab:6b:f4:73:e8:7f:75:88:
    52:56:da:12:2f:fa:7e:5b:7f:ad:e4:ec:3f:ef:59:
    29:de:bd:3c:80:89:ae:93:fe:2f:c5:ab:59:06:2b:
```

```
    39:43:6f:6e:84:bf:1f:77:c0:5d:d4:e0:71:df:b3:
    34:eb:db:82:0b:d7:c1:d2:a6:3c:3a:91:bc:4c:21:
    fd:32:e2:ba:95:3e:d0:02:72:b3:eb:ca:e1:7c:89:
    60:dc:77:a3:1b:d6:13:1c:e8:4f:54:e4:5a:f1:5a:
    93:8f:e7:2e:8c:d4:3f:68:e0:37:0a:2c:6d:04:4f:
    22:a5:8b:a2:47:87:aa:05:77:71:01:b4:c5:38:b2:
    e2:1a:44:c0:df:c8:7b:0e:18:ba:a9:20:f7:ba:f0:
    24:a7:0c:4e:5c:03:d1:1b:5c:e6:85:6e:4a:04:37:
    21:5c:d4:88:85:77:84:9c:14:ad:76:02:81:7b:12:
    55:d1:49:82:4f:65:04:3f:f0:f0:59:7d:05:b8:db:
    de:9a:74:56:94:43:0f:8b:c8:ed:9b:85:00:03:9f:
    53:0d:03:3f:52:5b:c9:71:b2:92:ee:89:dc:07:eb:
    72:14:eb:e5:a1:88:13:e9:be:82:c1:cf:a7:8f:5e:
    71:c2:cf:b7:4c:13:28:35:40:bb:c9:32:ab:71:60:
    1c:6d:82:f6:05:89:b7:01:d9:29:27:b8:7b:17:68:
    6d
prime1:
    00:fa:e9:d1:10:e5:b1:15:9a:2f:0b:48:77:87:6b:
    dc:77:70:50:a7:ee:c2:64:f3:6f:6e:cc:41:27:a0:
    10:2f:36:b6:97:64:d7:b2:f4:84:ef:fc:9f:22:32:
    60:15:2c:0e:d1:d3:67:bd:40:fe:a8:bc:b9:c2:51:
    30:92:66:50:18:50:2d:30:ef:a9:53:a1:89:2d:b3:
    81:fc:43:71:5e:30:ea:15:fc:f2:4c:d7:d4:48:ef:
    3c:16:58:58:ab:8b:af:65:09:b8:a6:6f:4c:12:7f:
    90:bc:c5:7e:2e:14:0e:a6:e9:df:f9:f1:6f:48:76:
    b2:ac:60:4b:1d:73:97:36:2f
prime2:
    00:e1:53:6c:9c:61:1a:db:d6:eb:42:19:72:be:1a:
    f2:68:7d:04:19:41:73:2e:8b:da:9f:66:30:43:c6:
    58:10:73:77:3f:94:c1:9c:ed:b3:93:3e:e6:07:22:
    ff:7a:96:7c:c1:48:d6:50:65:b2:a6:6b:58:61:33:
    24:98:d5:18:de:bc:fe:55:53:0a:dc:3d:d1:2e:aa:
    e1:62:fd:c5:2a:98:e9:8d:ee:46:c3:c3:2c:58:b7:
    cd:25:57:6a:21:f6:16:5c:22:01:0f:de:35:88:ee:
    56:e0:76:9a:43:ed:5a:50:b6:72:75:91:32:36:57:
    a3:84:3a:64:2e:03:8d:df:a5
exponent1:
    36:cf:54:a8:08:44:c2:9f:47:9f:83:58:f8:f0:0a:
    dc:dc:60:02:0f:19:cf:cb:8d:8f:fa:76:51:1d:99:
    eb:76:5c:34:7e:06:d0:44:b1:b5:6a:cd:a8:3e:b0:
    d6:6f:25:5d:98:7c:94:ce:d9:d2:2a:47:b9:b6:da:
    91:60:60:26:af:7c:ef:af:aa:a1:66:2b:fd:1b:b5:
    4d:51:be:36:01:21:61:64:3b:d9:a5:5b:ee:02:b4:
    71:7d:23:01:76:25:fe:40:3d:61:bd:f6:34:24:41:
    8d:ba:e6:71:52:58:51:05:cd:b3:5f:96:1b:92:32:
    3d:8d:5b:5b:37:a0:d4:69
exponent2:
    5a:c1:bc:64:7c:64:52:1a:0d:e6:30:d3:db:a8:84:
    ec:fb:35:d4:6a:5d:57:69:33:64:b2:c7:4b:f5:2e:
    f1:69:60:a5:b6:68:09:aa:60:83:35:79:77:74:6c:
    4c:d7:22:66:c3:cc:b6:d3:4f:92:e2:77:d5:a6:c0:
    dd:e2:2f:43:40:02:7d:21:96:a5:41:2c:e9:4c:20:
    be:3b:92:d7:e6:81:64:0e:8e:68:39:4b:ba:6c:45:
    ef:fd:76:9d:39:3e:a6:5b:77:ec:09:47:ac:e0:bb:
    13:6c:12:14:bc:1c:7d:98:0f:20:35:9c:70:f0:f9:
    c6:bf:b2:2c:2a:78:51:95
coefficient:
    48:3c:2c:02:39:3b:7a:c9:e3:4e:d3:e4:38:06:ae:
    c5:3e:c0:d6:1c:b8:46:ba:9d:78:a1:8b:4b:0a:45:
    0f:01:79:f3:a3:2e:bb:f4:f1:46:a0:0c:7c:1a:49:
    99:5c:e7:2f:fb:f1:b7:19:76:e2:77:86:34:db:0e:
    d2:77:e4:f1:9d:83:28:59:36:6a:da:7c:fe:48:ac:
    27:3f:02:d7:37:6f:68:96:04:ba:6f:5a:d4:b6:02:
```

<table>
<tr>
<td>

```
    82:a9:96:f7:da:13:68:40:f6:53:fe:ea:36:0b:a5:
    f5:78:81:19:e2:a9:2b:8d:5a:fe:78:25:1b:f9:b3:
    ed:09:d8:f1:ac:2d:89:39
```

</td>
<td>

```
    de:a2:88:7d:01:79:a7:6e:dc:14:c4:e5:1d:50:38:
    b2:be:e4:0a:ea:fb:dd:23:0a:fc:57:b2:3e:33:56:
    4b:12:79:b8:62:92:6c:7f
```

</td>
</tr>
<tr>
<td>

Displaying the contents of Public Key

```
$ openssl pkey -in alice09_public.pem -text -pubin
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAjZ6WY5I
MFUbx0zZ1SO9n
jIo08oASe4o7zutt8omSJc5GvBwtKOpVnnrQnSAoLIY11wLD6Bu
39dqhdpMvRP/D
2alsMfjbcv0tDMXdHDmSAQHxZoWZ4DPGO4YykJsr8t/+MXw8W9y
CPN9Kr/HlVJka
Rjv54PbUIq1tP+80mGm9SuqDsQzud8507fXEc68hmjeggDzivpJ
Dql10GrOmGsYt
WiCAoe0pngXbYd54jjYI83Kv7Dh9F8IKy2Jtrk/Y2jwPSyZEUDG
MI3/kpEt5EOZT
IkiYpRyPPh4cLsEFAGiBpMRYCGGQPD2cs+wH+f0jp9WhcpDDRO1
kT9c6QYc/KMYj
NwIDAQAB
-----END PUBLIC KEY-----
Public-Key: (2048 bit)
Modulus:
    00:8d:9e:96:63:92:0c:15:46:f1:d3:36:75:48:ef:
    67:8c:8a:34:f2:80:12:7b:8a:3b:ce:eb:6d:f2:89:
    92:25:ce:46:bc:1c:2d:28:ea:55:9e:7a:d0:9d:20:
    28:2c:86:35:d7:02:c3:e8:1b:b7:f5:da:a1:76:93:
    2f:44:ff:c3:d9:a9:6c:31:f8:db:72:fd:2d:0c:c5:
    dd:1c:39:92:01:01:f1:66:85:99:e0:33:c6:3b:86:
    32:90:9b:2b:f2:df:fe:31:7c:3c:5b:dc:82:3c:df:
    4a:af:f1:e5:54:99:1a:46:3b:f9:e0:f6:d4:22:ad:
    6d:3f:ef:34:98:69:bd:4a:ea:83:b1:0c:ee:77:ce:
    74:ed:f5:c4:73:af:21:9a:37:a0:80:3c:e2:be:92:
    43:aa:5d:74:1a:b3:a6:1a:c6:2d:5a:20:80:a1:ed:
    29:9e:05:db:61:de:78:8e:36:08:f3:72:af:ec:38:
    7d:17:c2:0a:cb:62:6d:ae:4f:d8:da:3c:0f:4b:26:
    44:50:31:8c:23:7f:e4:a4:4b:79:10:e6:53:22:48:
    98:a5:1c:8f:3e:1e:1c:2e:c1:05:00:68:81:a4:c4:
    58:08:61:90:3c:3d:9c:b3:ec:07:f9:fd:23:a7:d5:
    a1:72:90:c3:44:ed:64:4f:d7:3a:41:87:3f:28:c6:
    23:37
Exponent: 65537 (0x10001)
```

</td>
<td>

Displaying the contents of Public Key

```
$ openssl pkey -in BOB10pub.pem -text -pubin
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAiT2WwN9P
B80YwbtkzIK/
qyySb8IeQLltbArqbs0PmqJalW7ubN4fpW1CyDDUJTnWG3XnH5iG
fpMmGtzFNYGm
cFBRncYhUw4u07Wh+o/AJFO0n+z4DCxt0e4jc2CoKXm6xUSySdHP
xSJ7TRCDQGzH
ZPhb7iWr+5qq9568ydLGvcrJXfpT+5XPKnS5yspsmxG3518c2Jdq
wRIytix1MrYS
sWK6flUc5ZOaH1xpGq9nUgRks36vZU1vWJer8YuNrseOCypLDKff
LAGfazdV/V0e
EOWtPad8aWDv2WdVsf16GGHWUGOWjhuGCSNlLAd0Du63DvRVhupy
WOXRSyosJoMm
WwIDAQAB
-----END PUBLIC KEY-----
Public-Key: (2048 bit)
Modulus:
    00:89:3d:96:c0:df:4f:07:cd:18:c1:bb:64:cc:82:
    bf:ab:2c:92:6f:c2:1e:40:b9:6d:6c:0a:ea:6e:cd:
    0f:9a:a2:5a:95:6e:ee:6c:de:1f:a5:6d:42:c8:30:
    d4:25:39:d6:1b:75:e7:1f:98:86:7e:93:26:1a:dc:
    c5:35:81:a6:70:50:51:9d:c6:21:53:0e:2e:d3:b5:
    a1:fa:8f:c0:24:53:b4:9f:ec:f8:0c:2c:6d:d1:ee:
    23:73:60:a8:29:79:ba:c5:44:b2:49:d1:cf:c5:22:
    7b:4d:10:83:40:6c:c7:64:f8:5b:ee:25:ab:fb:9a:
    aa:f7:9e:bc:c9:d2:c6:bd:ca:c9:5d:fa:53:fb:95:
    cf:2a:74:b9:ca:ca:6c:9b:11:b7:e7:5f:1c:d8:97:
    6a:c1:12:32:b6:2c:75:32:b6:12:b1:62:ba:7e:55:
    1c:e5:93:9a:1f:5c:69:1a:af:67:52:04:64:b3:7e:
    af:65:4d:6f:58:97:ab:f1:8b:8d:ae:c7:8e:0b:2a:
    4b:0c:a7:df:2c:01:9f:6b:37:55:fd:5d:1e:10:e5:
    ad:3d:a7:7c:69:60:ef:d9:67:55:b1:fd:7a:18:61:
    d6:50:63:96:8e:1b:86:09:23:65:2c:07:74:0e:ee:
    b7:0e:f4:55:86:ea:72:58:e5:d1:4b:2a:2c:26:83:
    26:5b
Exponent: 65537 (0x10001)
```

</td>
</tr>
<tr>
<td>

Sends alice09_public.pem to Bob over email

</td>
<td>

Sends BOB10pub.pem to Alice over email

</td>
</tr>
</table>

2. **Alice creates a text file named SA09.key with this info <symmetric encryption algo, its parameters and passphrase>. Bob also does the same thing (SB10.key). These serve like keys for decrypting files exchanged in each way.**

<table>
<tr><th>Alice</th><th>Bob</th></tr>
<tr>
<td>

Creating SA09.key

```
$ echo -e "rc4-40,iter999,kritik@9" > SA09.key
```

</td>
<td>

Creating SB10.key

```
$ echo -e "aes-256-cbc,iter1000,bob@10" > SB10.key
```

</td>
</tr>
<tr>
<td>

Displaying SA09.key

```
$ cat SA09.key
rc4-40,iter999,kritik@9
```

</td>
<td>

Displaying SB10.key

```
$ cat SB10.key
aes-256-cbc,iter1000,bob@10
```

</td>
</tr>
</table>

3. **Alice securely sends SA09.key to Bob. Bob verifies it indeed came from Alice without any tampering and sees the message. Similarly, Bob securely sends his SB10.key to Alice and Alice checks its authenticity and integrity. For that, we generate a digital signature of the SA and SB files.**

Alice	Bob

Signing SA09.key
Since SA09.key file size is very small we can directly compute the signature without generating digest hash for it
 	
$ openssl pkeyutl -sign -in SA09.key -out alice09_signature.key -inkey alice09_private.pem
// Enter pass phrase for alice09_private.pem: 11009
	Signing SB10.key
	Since SB10.key file size is very small we can directly compute the signature without generating digest hash for it
	
	$ openssl pkeyutl -sign -in SB10.key -out BOB10-signature.key -inkey BOB10enc.pem
	// Enter pass phrase for BOB10enc.pem: 14010

Sends SA09.key and alice09_signature.key to Bob	**Sends SB10.key and BOB10-signature.key to Alice**
Verifying the file received from BOB $ openssl pkeyutl -verify -sigfile BOB10-signature.key -in SB10.key -inkey BOB10pub.pem -pubin Signature Verified Successfully	**Verifying the file received from Alice** $ openssl pkeyutl -verify -sigfile alice09_signature.key -in SA09.key -inkey alice09_public.pem -pubin Signature Verified Successfully
Displaying SB10.key $ cat SB10.key aes-256-cbc,iter1000,bob@10	**Displaying SA09.key** $ cat SA09.key rc4-40,iter999,kritik@9

4. **Alice encrypts a large file (alice09-original.png) with SA09.key and sends it along with a signature to Bob so that he could decrypt it with the same SA09.key and verify it indeed came from Alice without tampering. Similarly, Bob sends a large file (BOB10-original.jpg) securely to Alice without any tampering.**

Alice	Bob
Encrypting alice09-original.png using SA09.key $ openssl enc -rc4-40 -e -iter 999 -salt -in alice09-original.png -out alice09-enc.png -pass file:SA09.key	**Encrypting BOB10-original.jpg using SB10.key** $ openssl enc -aes-256-cbc -e -iter 1000 -salt -in BOB10-original.jpg -out BOB10-encrypted.jpg -pass file:SB10.key

Signing the encrypted image file
 	
$ openssl dgst -sha256 -sign alice09_private.pem -out alice09_signature.sign alice09-enc.png
// Enter pass phrase for alice09_private.pem:
	Signing the encrypted image file
	
	$ openssl dgst -sha256 -sign BOB10enc.pem -out BOB10_signature.sign BOB10-encrypted.jpg
	// Enter pass phrase for BOB10enc.pem: 14010

Sends alice09-enc.png and alice09_signature.sign to Bob	**Sends BOB10-encrypted.jpg and BOB10_signature.sign to Alice**
Verifying the file received from BOB $ openssl dgst -sha256 -verify BOB10pub.pem -signature BOB10_signature.sign BOB10-encrypted.jpg Verified OK	**Verifying the file received from Alice** $ openssl dgst -sha256 -verify alice09_public.pem -signature alice09_signature.sign alice09-enc.png Verified OK

Decrypting the encrypted file using SB10.key $ openssl enc -aes-256-cbc -d -iter 1000 -in BOB10-encrypted.jpg -out BOB10-dec.jpg -pass file:SB10.key	**Decrypting the encrypted file using SA09.key** $ openssl enc -rc4-40 -d -iter 999 -in alice09-enc.png -out alice09-dec.png -pass file:SA09.key

Part B: Alice (Browser), Bob (web server) and Charlie (Root CA)

1. Charlie generates a self-signed certificate named charlie-ca.crt as he plays the role of the root CA.
2. Bob generates a CSR named BOB10-domain.csr for getting X.509 V3 certificate and emails it to Charlie for getting the end-user cert named BOB10-domain.crt issued by the root CA (Charlie). Bob verifies BOB10-domain.crt is valid and indeed signed by the root CA, Charlie.

Charlie	Bob

Generating a self-signed X.509 certificate (charlie-ca.crt) along with the corresponding private key (charlie_private.pem) using RSA with a key size of 2048 bits.
 	
$ openssl req -newkey rsa:2048 -nodes -keyout charlie_private.pem -x509 -days 90 -out charlie-ca.crt
.++
++++++++++++++*.....+..+....+.....+.....++++
+++++++*.....+.....+.+..+.....+.
..+.....+.+.....+.....+.+.....+..
+.+..+....+...+...+.....+...+.....+...+....+
.....+.....+.....+...+.....
+.....++++++++++++*.....
..+...+.....+.+.....+...+.....+...+...
.....+.....+.....+++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++++++
----- 	
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
----- 	
Country Name (2 letter code) [AU]:IN
State or Province Name (full name) [Some-State]:Telangana
Locality Name (eg, city) []:Hyderabad
Organization Name (eg, company) [Internet Widgits Pty Ltd]:IIT Hyderabad
Organizational Unit Name (eg, section) []:Dept. of CSE
Common Name (e.g. server FQDN or YOUR name) []:Charlie
Email Address []:cs23mtech11010@iith.ac.in
	Generating a new certificate signing request (CSR) using an existing encrypted private key.
	
	$ openssl req -new -key BOB10enc.pem -out BOB10-domain.csr
	// Enter pass phrase for BOB10enc.pem: 14010
	You are about to be asked to enter information that will be incorporated
	into your certificate request.
	What you are about to enter is what is called a Distinguished Name or a DN.
	There are quite a few fields but you can leave some blank
	For some fields there will be a default value,
	If you enter '.', the field will be left blank.
	----- 	
	Country Name (2 letter code) [AU]:IN
	State or Province Name (full name) [Some-State]:Telangana
	Locality Name (eg, city) []:Kandi
	Organization Name (eg, company) [Internet Widgits Pty Ltd]:IITH
	Organizational Unit Name (eg, section) []:CSE
	Common Name (e.g. server FQDN or YOUR name) []:BOB10
	Email Address []:cs23mtech14010@iith.ac.in
	
	Please enter the following 'extra' attributes
	to be sent with your certificate request
	A challenge password []:
	An optional company name []:

Viewing the charlie-ca.crt	**Viewing the BOB10-domain.csr**

```
$ openssl x509 -in charlie-ca.crt -text
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:

65:b6:15:00:eb:10:02:78:0a:91:57:19:3e:3f:05:8e:de:
dd:45:df
        Signature Algorithm:
sha256WithRSAEncryption
        Issuer: C = IN, ST = Telangana, L =
Hyderabad, O = IIT Hyderabad, OU = Dept. of CSE, CN
= Charlie, emailAddress = cs23mtech11010@iith.ac.in
        Validity
            Not Before: Jan 28 13:58:47 2024 GMT
            Not After : Apr 27 13:58:47 2024 GMT
        Subject: C = IN, ST = Telangana, L =
Hyderabad, O = IIT Hyderabad, OU = Dept. of CSE, CN
= Charlie, emailAddress = cs23mtech11010@iith.ac.in
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:

00:de:96:13:21:28:29:de:d7:b6:4f:fd:96:a8:22:

bf:10:e8:7c:08:f7:a7:e7:4a:3d:70:25:5a:36:a2:

c9:78:ad:4d:2a:b1:cb:86:21:7f:f0:2a:81:45:7c:

ff:57:0f:6f:1e:6c:1a:65:01:75:97:74:1b:d0:be:

a8:0b:10:c4:44:b3:77:35:1f:d8:4b:82:fb:d2:20:

91:a5:72:6c:c6:76:ec:12:84:0e:df:73:f2:3c:80:

5d:46:7b:42:f8:05:b9:88:46:40:d2:78:aa:6b:f2:

b6:bb:87:eb:8f:16:08:03:87:18:b1:e7:5d:25:50:

e8:5c:38:ef:48:b3:ca:9b:96:c8:b9:ad:d6:f6:26:

2d:28:dd:ea:86:11:dd:39:e1:b4:8e:91:45:b0:a8:

dd:ff:a3:a7:1b:ba:5d:e7:2c:36:0c:c7:65:01:94:

71:34:bf:f4:c1:00:46:22:41:f8:a1:24:c2:0d:9f:

f6:51:39:fc:c6:a2:5a:e3:b2:26:07:0f:ac:cb:57:

f5:a4:18:16:4b:7f:74:93:34:9b:4e:13:a6:15:08:

38:97:21:57:87:db:26:80:c0:cd:4c:68:46:bd:29:

e7:c7:11:02:46:27:c2:ed:cb:b2:fe:b3:fa:e6:b6:

b3:4f:cd:2f:4e:6a:92:29:04:40:09:5c:42:70:45:
                    38:25
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
```

```
$ openssl req -text -in BOB10-domain.csr --noout
Certificate Request:
    Data:
        Version: 1 (0x0)
        Subject: C = IN, ST = Telangana, L = Kandi,
O = IITH, OU = CSE, CN = BOB10, emailAddress =
cs23mtech14010@iith.ac.in
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:

00:dc:d9:45:02:8c:36:8f:08:7f:ff:73:14:cc:4a:

c6:64:02:4c:81:5c:2e:fa:3f:a9:1e:6f:b2:06:51:

f2:ac:19:59:be:33:4a:57:46:31:e2:1a:95:0c:f7:

34:56:a3:79:a8:fd:3a:ed:a6:78:d8:8b:d5:66:f2:

4f:8b:7c:c2:7e:b8:60:2c:65:88:14:f8:f2:20:d9:

0a:b7:50:4f:10:f4:6b:43:b5:a2:83:ff:4a:ef:5c:

32:d3:3d:ec:aa:ee:7d:22:8b:1c:ea:40:4f:7a:59:

1d:2d:0f:49:0f:45:56:38:c0:cd:51:0f:40:b6:b2:

5e:5b:7f:3e:ff:5c:c4:f6:08:7c:62:8f:a7:7e:27:

49:6c:0a:1f:17:e3:1f:e6:6b:ab:a5:b6:61:7a:d5:

7e:1b:e8:9d:43:e6:46:b2:90:31:26:e2:32:ee:a7:

93:5d:34:9a:89:8a:d7:ed:15:4c:2a:28:1a:09:a6:

c4:6d:0a:54:4b:56:32:05:75:da:ca:a4:69:db:63:

1b:b8:6c:80:b8:38:e0:0f:ac:a1:2c:f3:a2:c1:80:

a7:b0:57:31:1a:7b:e0:b4:bd:62:29:40:2e:4c:e8:

95:3a:82:57:3c:05:62:e3:d2:2d:bb:38:06:22:fb:

74:dc:15:4c:f9:b5:0e:d8:cd:0c:0e:9a:09:9d:8b:
                    dd:4b
                Exponent: 65537 (0x10001)
        Attributes:
            challengePassword        :14010
            Requested Extensions:
    Signature Algorithm: sha256WithRSAEncryption
    Signature Value:

d1:d8:18:a4:f0:3d:4a:11:12:89:fe:f3:29:b4:d9:47:f3:7
c:

fb:88:eb:74:87:79:2e:1d:24:a6:01:4c:83:f6:f1:c9:e1:e
2:

d1:dd:aa:bd:5e:3f:68:12:09:ad:c2:ae:5a:5b:eb:24:8a:3
7:
```

```
7F:2E:9F:51:91:73:99:8A:F6:BB:A3:49:64:82:DF:B8:3F:
51:0B:63
            X509v3 Authority Key Identifier:

7F:2E:9F:51:91:73:99:8A:F6:BB:A3:49:64:82:DF:B8:3F:
51:0B:63
            X509v3 Basic Constraints: critical
                CA:TRUE
    Signature Algorithm: sha256WithRSAEncryption
    Signature Value:

de:3e:b9:3d:b9:50:bb:e7:1a:fc:c5:72:19:1d:06:e1:66:
0c:

be:1d:4b:30:1b:b2:0e:ed:72:9f:fb:30:7b:c3:35:15:0c:
e7:

41:f4:f6:c5:99:49:96:52:e9:17:9b:fa:43:bf:c8:b0:aa:
f2:

f5:b0:9c:7b:ff:26:31:4d:a9:68:fe:a7:29:0e:77:24:55:
12:

f1:44:a3:c2:65:19:69:09:93:a9:9a:8d:09:fd:b4:c5:c7:
22:

52:51:7a:9d:71:20:79:09:8e:07:8d:e5:a2:66:9e:d6:d4:
c5:

e2:29:f9:83:49:39:66:ff:5d:08:b8:1e:1b:33:6c:8e:a7:
3a:

cf:d9:3a:e6:9e:82:3d:99:9a:c2:18:87:b8:a2:c4:29:93:
17:

36:33:bb:04:1b:1d:cd:cf:c2:9e:5f:3b:f4:1f:37:d5:5f:
bb:

d2:87:7a:49:53:58:d2:e7:51:29:f9:44:0b:a1:8d:a0:e5:
e4:

48:11:4a:05:6e:3b:6a:77:82:1d:f3:ae:a1:13:5a:84:5a:
e7:

d8:0b:1e:20:02:22:73:71:91:7d:7e:84:94:1b:a4:17:f4:
f1:

89:c2:64:27:92:de:48:0f:9e:c2:c5:1c:11:71:ba:d6:7e:
3a:

df:68:27:e7:7a:d9:17:02:fa:ae:37:e6:ae:ef:dd:f4:8c:
f9:
        74:97:a5:75
-----BEGIN CERTIFICATE-----
MIIEIzCCAwugAwIBAgIUZbYVAOsQAngKkVcZPj8Fjt7dRd8wDQY
JKoZIhvcNAQEL
BQAwgaAxCzAJBgNVBAYTAklOMRIwEAYDVQQIDAlUZWxhbmdhbmE
xEjAQBgNVBAcM
CUh5ZGVyYWJhZDEWMBQGA1UECgwNSUlUIEh5ZGVyYWJhZDEVMBM
GA1UECwwMRGVw
dC4gb2YgQ1NFMRAwDgYDVQQDDAdDaGFybGllMSgwJgYJKoZIhvc
NAQkBFhljczIz
bXRlY2gxMTAxMEBpaXRoLmFjLmluMB4XDTI0MDEyODEzNTg0N1o
eb:2b:49:11:3e:a2:b0:f2:30:15:dc:1c:06:69:43:6d:50:7
a:

28:55:18:64:41:ac:45:6a:d1:68:9b:36:ec:30:d1:18:b6:f
1:

b7:d3:f8:e2:52:6d:f9:55:d5:35:c0:2b:50:fa:62:05:63:c
2:

a0:d0:66:f1:57:de:52:ef:20:8a:eb:1c:5e:f5:0e:94:eb:9
9:

cd:58:c0:d9:75:d3:ec:cb:a5:bd:e1:12:bc:5b:d9:6c:28:5
0:

71:03:a1:f0:81:b9:d9:5c:13:a4:3d:b4:01:45:81:d3:4f:9
1:

a3:3d:9c:e6:93:7a:e5:cc:56:97:2e:02:fb:8e:8e:af:76:8
e:

c4:3d:10:b0:17:4d:14:cf:16:5e:10:80:79:58:ae:2b:dc:2
5:

6e:84:a2:8a:fc:87:d4:fd:0b:aa:62:67:f6:4a:65:4b:98:2
0:

58:e0:a4:9c:1d:e2:15:aa:93:c9:b8:28:be:87:f9:21:b0:a
7:

29:b0:bf:9b:aa:8e:09:59:8c:c9:92:e7:16:25:25:fe:2a:3
2:
        7b:7d:50:cf
```

XDTI0MDQyNzEz NTg0N1owgaAxCzAJBgNVBAYTAklOMRIwEAYDVQQIDAlUZWxhbmd hbmExEjAQBgNV BAcMCUh5ZGVyYWJhZDEWMBQGA1UECgwNSUlUIEh5ZGVyYWJhZDE VMBMGA1UECwwM RGVwdC4gb2YgQ1NFMRAwDgYDVQQDDAdDaGFybGllMSgwJgYJKoZ IhvcNAQkBFhlj czIzbXRlY2gxMTAxMEBpaXRoLmFjLmluMIIBIjANBgkqhkiG9w0 BAQEFAAOCAQ8A MIIBCgKCAQEA3pYTISgp3te2T/2WqCK/EOh8CPen50o9cCVaNqL JeK1NKrHLhiF/ 8CqBRXz/Vw9vHmwaZQF1l3Qb0L6oCxDERLN3NR/YS4L70iCRpXJ sxnbsEoQO33Py PIBdRntC+AW5iEZA0niqa/K2u4frjxYIA4cYseddJVDoXDjvSLP Km5bIua3W9iYt KN3qhhHdOeG0jpFFsKjd/6OnG7pd5yw2DMdlAZRxNL/0wQBGIkH 4oSTCDZ/2UTn8 xqJa47ImBw+sy1f1pBgWS390kzSbThOmFQg4lyFXh9smgMDNTGh GvSnnxxECRifC 7cuy/rP65razT80vTmqSKQRACVxCcEU4JQIDAQABo1MwUTAdBgN VHQ4EFgQUfy6f UZFzmYr2u6NJZILfuD9RC2MwHwYDVR0jBBgwFoAUfy6fUZFzmYr 2u6NJZILfuD9R C2MwDwYDVR0TAQH/BAUwAwEB/zANBgkqhkiG9w0BAQsFAAOCAQE A3j65PblQu+ca /MVyGR0G4WYMvh1LMBuyDu1yn/swe8M1FQznQfT2xZlJllLpF5v 6Q7/IsKry9bCc e/8mMU2paP6nKQ53JFUS8USjwmUZaQmTqZqNCf20xcciUlF6nXE geQmOB43lomae 1tTF4in5g0k5Zv9dCLgeGzNsjqc6z9k65p6CPZmawhiHuKLEKZM XNjO7BBsdzc/C nl879B831V+70od6SVNY0udRKflEC6GNoOXkSBFKBW47aneCHfO uoRNahFrn2Ase IAIic3GRfX6ElBukF/TxicJkJ5LeSA+ewsUcEXG61n4632gn53r ZFwL6rjfmru/d 9Iz5dJeldQ== -----END CERTIFICATE-----	
Receives BOB10-domain.csr from BOB	**Sends BOB10-domain.csr to root CA (Charlie)**
Generates BOB10-domain.crt X509 V3 certificate for BOB $ openssl x509 -req -sha256 -days 90 -in BOB10-domain.csr -CAkey charlie_private.pem -CA charlie-ca.crt -out BOB10-domain.crt -CAcreateserial -ext "subjectAltName=DNS:example.com" -extfile <(echo -e "basicConstraints=CA:FALSE\nkeyUsage=digitalSignature, keyCertSign\nextendedKeyUsage=serverAuth") Certificate request self-signature ok subject=C = IN, ST = Telangana, L = Kandi, O = IITH, OU = CSE, CN = BOB10, emailAddress = cs23mtech14010@iith.ac.in	

Viewing BOB10-domain.crt
 	
$ openssl x509 -text -in BOB10-domain.crt
Certificate:
  Data:
  Version: 3 (0x2)
  Serial Number:	

```
7e:8d:31:f0:76:ab:fa:83:61:f9:43:97:c0:50:79:a8:0b:
3f:9e:cf
        Signature Algorithm:
sha256WithRSAEncryption
        Issuer: C = IN, ST = Telangana, L =
Hyderabad, O = IIT Hyderabad, OU = Dept. of CSE, CN
= Charlie, emailAddress = cs23mtech11010@iith.ac.in
        Validity
            Not Before: Jan 28 14:03:49 2024 GMT
            Not After : Apr 27 14:03:49 2024 GMT
        Subject: C = IN, ST = Telangana, L = Kandi,
O = IITH, OU = CSE, CN = BOB10, emailAddress =
cs23mtech14010@iith.ac.in
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:

00:dc:d9:45:02:8c:36:8f:08:7f:ff:73:14:cc:4a:

c6:64:02:4c:81:5c:2e:fa:3f:a9:1e:6f:b2:06:51:

f2:ac:19:59:be:33:4a:57:46:31:e2:1a:95:0c:f7:

34:56:a3:79:a8:fd:3a:ed:a6:78:d8:8b:d5:66:f2:

4f:8b:7c:c2:7e:b8:60:2c:65:88:14:f8:f2:20:d9:

0a:b7:50:4f:10:f4:6b:43:b5:a2:83:ff:4a:ef:5c:

32:d3:3d:ec:aa:ee:7d:22:8b:1c:ea:40:4f:7a:59:

1d:2d:0f:49:0f:45:56:38:c0:cd:51:0f:40:b6:b2:

5e:5b:7f:3e:ff:5c:c4:f6:08:7c:62:8f:a7:7e:27:

49:6c:0a:1f:17:e3:1f:e6:6b:ab:a5:b6:61:7a:d5:

7e:1b:e8:9d:43:e6:46:b2:90:31:26:e2:32:ee:a7:

93:5d:34:9a:89:8a:d7:ed:15:4c:2a:28:1a:09:a6:

c4:6d:0a:54:4b:56:32:05:75:da:ca:a4:69:db:63:

1b:b8:6c:80:b8:38:e0:0f:ac:a1:2c:f3:a2:c1:80:

a7:b0:57:31:1a:7b:e0:b4:bd:62:29:40:2e:4c:e8:

95:3a:82:57:3c:05:62:e3:d2:2d:bb:38:06:22:fb:

74:dc:15:4c:f9:b5:0e:d8:cd:0c:0e:9a:09:9d:8b:
                    dd:4b
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Key Usage:
                Digital Signature, Certificate Sign
            X509v3 Extended Key Usage:
                TLS Web Server Authentication
            X509v3 Subject Key Identifier:
```

```
39:B5:4B:B8:F9:E2:FF:9C:91:3A:15:7F:DE:0E:9B:44:EF:
65:70:1A
            X509v3 Authority Key Identifier:

7F:2E:9F:51:91:73:99:8A:F6:BB:A3:49:64:82:DF:B8:3F:
51:0B:63
    Signature Algorithm: sha256WithRSAEncryption
    Signature Value:

48:04:7b:00:9b:c0:a0:60:54:76:9f:5e:ac:40:31:17:2e:
d7:

0c:7d:21:9e:48:ce:12:c1:17:1f:51:bb:6d:00:70:e5:bf:
f7:

f2:42:3c:5f:17:55:4e:a0:3a:26:e6:b6:f7:f7:a4:57:95:
78:

32:9a:2f:38:13:35:2f:65:a3:fe:a5:45:d8:4c:d7:00:ce:
eb:

94:d8:aa:a8:fd:27:c3:0a:fd:fb:d1:48:09:50:b0:db:14:
48:

43:79:7c:fc:fb:8b:d6:a5:f9:81:4a:19:6a:16:7b:5a:dc:
98:

c0:6e:de:00:88:32:1e:f9:5b:15:6f:1a:92:26:36:af:b1:
50:

72:da:fe:84:3c:ef:69:8c:c0:c3:22:70:db:66:9e:f6:9f:
ab:

0a:8d:73:4c:a9:69:22:87:e6:2b:5f:2d:ff:11:51:5c:b3:
58:

83:9b:a7:b6:be:99:93:ff:4e:9a:3f:cb:3b:8a:a9:f1:d8:
f9:

71:a4:da:32:ee:8f:ec:b4:e9:d9:55:57:fc:fd:14:85:89:
cf:

73:af:6a:29:20:12:3b:2e:2c:5e:84:de:be:c5:26:1a:b1:
c8:

66:cf:9e:fd:37:0c:6a:a2:8f:0b:72:b4:02:36:d5:cc:f8:
61:

7e:db:cd:b3:84:07:4d:e6:97:b8:98:d9:39:82:08:f7:5f:
33:
        81:bd:2c:bf
```


```
-----BEGIN CERTIFICATE-----
MIIEJzCCAw+gAwIBAgIUfo0x8Har+oNh+UOXwFB5qAs/ns8wDQY
JKoZIhvcNAQEL
BQAwgaAxCzAJBgNVBAYTAklOMRIwEAYDVQQIDAlUZWxhbmdhbmE
xEjAQBgNVBAcM
CUh5ZGVyYWJhZDEWMBQGA1UECgwNSUlUIEh5ZGVyYWJhZDEVMBM
GA1UECwwMRGVw
dC4gb2YgQ1NFMRAwDgYDVQQDDAdDaGFybGllMSgwJgYJKoZIhvc
NAQkBFhljczIz
bXRlY2gxMTAxMEBpaXRoLmFjLmluMB4XDTI0MDEyODE0MDM0OVo
XDTI0MDQyNzE0
MDM0OVowgYgxCzAJBgNVBAYTAklOMRIwEAYDVQQIDAlUZWxhbmd
```

hbmExDjAMBgNV BAcMBUthbmRpMQ0wCwYDVQQKDARJSVRIMQwwCgYDVQQLDANDU0U xDjAMBgNVBAMM BUJPQjEwMSgwJgYJKoZIhvcNAQkBFhljczIzbXRlY2gxNDAxMEB paXRoLmFjLmlu MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA3NlFAow 2jwh//3MUzErG ZAJMgVwu+j+pHm+yBlHyrBlZvjNKV0Yx4hqVDPc0VqN5qP067aZ 42IvVZvJPi3zC frhgLGWIFPjyINkKt1BPEPRrQ7Wig/9K71wy0z3squ59Iosc6kB PelkdLQ9JD0VW OMDNUQ9AtrJeW38+/1zE9gh8Yo+nfidJbAofF+Mf5murpbZhetV +G+idQ+ZGspAx JuIy7qeTXTSaiYrX7RVMKigaCabEbQpUS1YyBXXayqRp22MbuGy AuDjgD6yhLPOi wYCnsFcxGnvgtL1iKUAuTOiVOoJXPAVi49ItuzgGIvt03BVM+bU O2M0MDpoJnYvd SwIDAQABo28wbTAJBgNVHRMEAjAAMAsGA1UdDwQEAwIChDATBgN VHSUEDDAKBggr BgEFBQcDATAdBgNVHQ4EFgQUObVLuPni/5yROhV/3g6bRO9lcBo wHwYDVR0jBBgw FoAUfy6fUZFzmYr2u6NJZILfuD9RC2MwDQYJKoZIhvcNAQELBQA DggEBAEgEewCb wKBgVHafXqxAMRcu1wx9IZ5IzhLBFx9Ru20AcOW/9/JCPF8XVU6 gOibmtvf3pFeV eDKaLzgTNS9lo/6lRdhM1wDO65TYqqj9J8MK/fvRSAlQsNsUSEN 5fPz7i9al+YFK GWoWe1rcmMBu3gCIMh75WxVvGpImNq+xUHLa/oQ872mMwMMicNt mnvafqwqNc0yp aSKH5itfLf8RUVyzWIObp7a+mZP/Tpo/yzuKqfHY+XGk2jLuj+y 06dlVV/z9FIWJ z3OvaikgEjsuLF6E3r7FJhqxyGbPnv03DGqijwtytAI21cz4YX7 bzbOEB03ml7iY 2TmCCPdfM4G9LL8= -----END CERTIFICATE-----	
Sends BOB10-domain.crt and charlie-ca.crt to BOB	**Verifies BOB10-domain.crt is indeed signed by root CA, Charlie** $ openssl verify -verbose -CAfile charlie-ca.crt BOB10-domain.crt BOB10-domain.crt: OK
Sends charlie-ca.crt to Alice.	**Sends BOB10-domain.crt to Alice.**

3. Alice (Student A) gets charlie-ca.crt over email from Charlie and BOB10-domain.crt over email from Bob and verifies that these certificates are valid and signed by the root CA, Charlie.

Alice
Verifies BOB10-domain.crt is valid and signed by root CA, Charlie $ openssl verify -verbose -CAfile charlie-ca.crt BOB10-domain.crt BOB10-domain.crt: OK

Comment on whether Bob's cert is of type X.509 V3, what is the serial no assigned, and what are the key usages/constraints associated with the cert.

1. Bob's certificate is indeed of type X.509 V3.
2. The serial number assigned to Bob's certificate is: 7E:8D:31:F0:76:AB:FA:83:61:F9:43:97:C0:50:79:A8:0B:3F:9E:CF (which corresponds to the decimal representation: 722481592524317182470690699152957466529765498575).
3. The key usages associated with the certificate are:
   digitalSignature: This indicates that the certificate can be used for digital signatures.
   keyCertSign: This indicates that the certificate can be used to sign other certificates.

   The basic constraints associated with the certificate are:
   CA:FALSE: This means that the certificate is not a Certificate Authority (CA) certificate, indicating that it cannot be used to issue other certificates.

   Additionally, the certificate has an extended key usage of serverAuth, indicating that it can be used for server authentication purposes.

Certificate Summary

Subject

RDN	Value
emailAddress	cs23mtech14010@iith.ac.in
Common Name (CN)	BOB10
Organizational Unit (OU)	CSE
Organization (O)	IITH
Locality (L)	Kandi
State (ST)	Telangana
Country (C)	IN

Properties

Property	Value
Issuer	emailAddress = cs23mtech11010@iith.ac.in,CN = Charlie,OU = Dept. of CSE,O = IIT Hyderabad,L = Hyderabad,ST = Telangana,C = IN
Subject	emailAddress = cs23mtech14010@iith.ac.in,CN = BOB10,OU = CSE,O = IITH,L = Kandi,ST = Telangana,C = IN
Valid From	28 Jan 2024, 2:03 p.m.
Valid To	27 Apr 2024, 2:03 p.m.
Serial Number	7E:8D:31:F0:76:AB:FA:83:61:F9:43:97:C0:50:79:A8:0B:3F:9E:CF (722481592524317182470690699152957466529765498575)
CA Cert	No
Key Size	2048 bits
Fingerprint (SHA-1)	CE:6F:2F:8C:48:E5:D8:71:41:D4:83:BE:0B:9D:72:61:78:5E:4F:99
Fingerprint (MD5)	01:7E:13:FD:19:23:F3:66:38:BC:2F:E6:AF:A1:AC:EF
SANS	

References:

[1] A 6 Part Introductory OpenSSL Tutorial - KeyCDN
[2] LX-Openssl.pdf
[3] Other materials provided in Classroom by Course Instructor Dr. Bheemarjuna Reddy Tamma Sir
[4] CSR Decoder and Certificate Decoder | CSR Checker | Certificate Checker (certlogik.com)