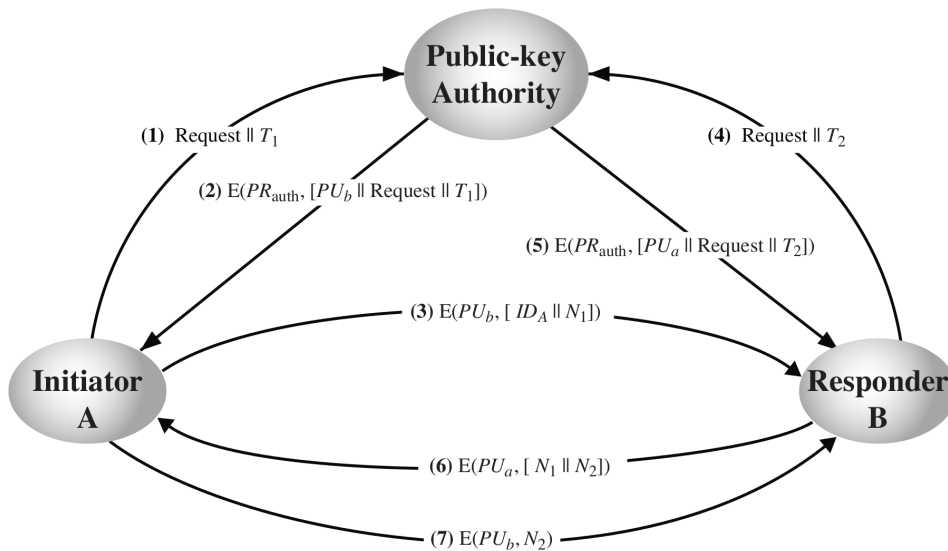


CSS322 – Quiz 11

Name: _____ ID: _____ Marks: _____ (10)

Question 1 [2 marks]

Consider the scheme in the figure below.



- (a) List all keys assumed to be known by the authority before the scheme starts (i.e. before message (1) is sent). [1 mark]

- (b) List all keys known by B after the scheme is finished (i.e. after message (7) is sent). [1 mark]

Question 2 [5 marks]

Consider the X.509 certificate in Listing 1.

Listing 1: X.509 Certificate

```
Certificate:
Data:
  Version: 3 (0x2)
  Serial Number: 3 (0x3)
  Signature Algorithm: sha1WithRSAEncryption
  Issuer: C=TH, ST=Pathumthani, O=TrustUs, OU=Crypto,
  CN=TrustUsCrypto
  Validity
    Not Before: Jan 25 02:25:10 2011 GMT
```

```

Not After : Jan 25 02:25:10 2012 GMT
Subject: C=TH, ST=Pathumthani, O=Malicious, OU=Department,
        CN=Malicious Department
Subject Public Key Info:
  Public Key Algorithm: rsaEncryption
  RSA Public Key: (1024 bit)
    Modulus (1024 bit):
      00:aa:1f:cf:01:2f:d3:2e:80:63:98:1b:0f:16:5d:
      dd:af:e2:38:de:78:88:56:b6:14:2b:61:79:92:0b:
      f3:7f:b6:89:7b:d0:fc:59:5a:1a:be:24:61:39:d5:
      4d:80:3a:40:2b:7c:89:ef:5e:50:a5:3b:44:68:a9:
      7f:97:d9:c4:9a:bf:b6:97:eb:4c:87:0d:00:96:b4:
      f9:ea:8c:6a:cb:e0:bd:f8:a8:1f:82:d3:2b:23:3c:
      b6:54:85:37:5b:13:1a:2e:be:0d:20:52:c5:98:b6:
      4c:97:67:6e:b2:43:04:3f:01:41:8e:e0:2f:38:1f:
      e1:cc:cf:0d:c2:5f:0a:04:49
    Exponent: 65537 (0x10001)
X509v3 extensions:
  X509v3 Basic Constraints:
    CA:FALSE
  Netscape Comment:
    OpenSSL Generated Certificate
  X509v3 Subject Key Identifier:
    EA:1C:DC:C5:16:F2:9D:BC:61:5E:A8:D2:67:2A:06:13:C5:64:8A:A3
  X509v3 Authority Key Identifier:
    keyid:61:52:40:EA:7F:E0:EC:77:41:F6:4F:6F:7C:49:EB:05:C1:56:6D:GA

```

```

Signature Algorithm: sha1WithRSAEncryption
a5:7a:36:91:ef:11:46:58:74:37:87:81:7a:99:ff:b6:40:4a:
80:6a:07:69:e3:3c:33:9a:fd:31:50:e9:9f:bf:ff:36:a4:34:
21:50:49:70:e0:88:b3:01:c9:51:26:8b:1e:8b:34:ca:4c:3c:
a2:ab:0a:a3:b3:39:c0:fb:88:72:98:69:c9:af:42:b2:48:1b:
4e:4a:76:e8:b4:c7:d4:f8:15:d2:5e:f8:69:fc:53:0c:ca:85:
84:ea:e5:36:17:20:65:fc:d0:3e:d1:33:17:f7:d1:40:f8:3d:
2a:87:f8:3c:66:8e:43:62:ea:02:ef:7a:d4:a7:55:e9:d9:2d:
38:1a

```

```

-----BEGIN CERTIFICATE-----
MIIC5zCCA1CgAwIBAgIBAzANBgkqhkiG9w0BAQUFADCBnzELMAkGA1UEBhMCVEGx
GDASBgNVBAGTC1BhdGh1bXRoYW5pMREwDwYDVQQHEWhCYW5na2FkaTENMAzGA1UE
ChMEU01JVDEMMAAoGA1UECxMDSUNUMR4wHAYDVQQDExVDZlJ0aWZpY2FOZSBBdXR0
b3JpdHkxKjAoBgkqhkiG9w0BCQEWG2NzcMyMi1jYUBpY3Quc21pdC50dS5hYy50
aDAeFw0xMjAxMjUwMjI1MTBhFw0xMjAxMjUwMjI1MTBhMFYxCzAJBgNVBAYTA1RI
MRQwEgYDVQIEwtQYXRodW10aGFuaTENMAzGA1UEChMEU01JVDEMMAAoGA1UECxMD
SUNUMRQwEgYDVQQDEWtEZW1vIFVzZXIgmjCBnzANBgkqhkiG9w0BAQEFAA0BjQAw
gYkCgYEAqh/PAS/TL0BjmbSPfL3dr+I43niIVrYUK2F5kgvzf7aJe9D8WVoavRh
OdVNgDpAK3yJ715QpTtEaKl/19nEmr+2l+tmhw0AlrT56oxqy+C9+KgfgtMrIzy2
VIU3WxMaLr4NIFLFmLZM12duskMEPwFBjuAvOB/hzM8Nw18KBKMAwEAAa7MHkw
CQYDVROTBAlwADAsBg1ghkgBhvCAQOEHydT3B1b1NTTCBHZW51cmF0ZWQgQ2Vy
dG1maWnhdGUwHQYDVROBBYEF0oc3MUW8p28YV6o0mcqBhPFZiQuMB8GA1UdIwQY
MBaAFGFSQOp/40x3QfZPb3xJ6wXBVm1JMA0GCSqGSIb3DQEBAUAA4GBAKV6NpHv
EUZYdDeHgXqZ/7ZASoBqB2njPD0a/TFQ6Z//zakNCFQSDXdlMByVEmix6LNMpM
PKKrCqQz0cd7iHKYacmvQrJIG05Kdui0x9T4FdJe+Gn8UwzKhYTq5TYXIGX80D7R
Mxf30UD4PSqH+DxmjkNi6gLvetSnVenZLTae
-----END CERTIFICATE-----

```

(a) Whose certificate is this? [1 mark]

(b) Whose RSA key is included in the certificate? [1 mark]

(c) The RSA algorithm is: $C = M^e \bmod n$. What are the last two hexadecimal digits

of n in the users RSA key? [1 mark]

In general, an X.509 certificate for user A can be expressed as:

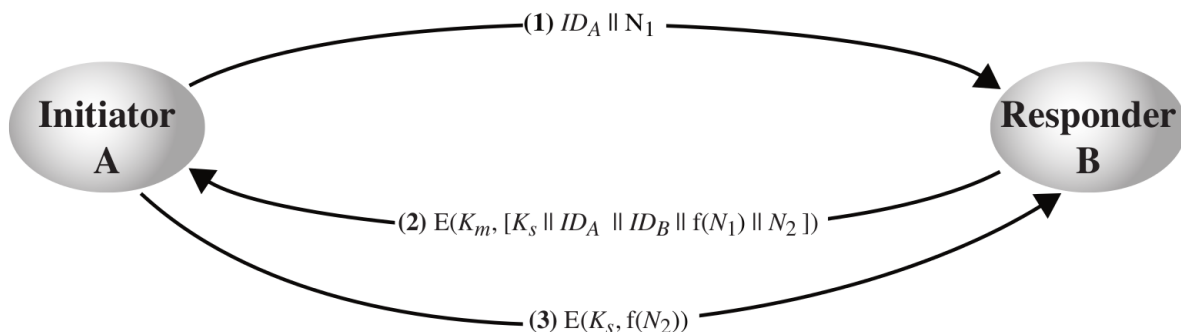
$$C_A = Data || S$$

where $Data$ is the concatenation of the fields: Version, SerialNumber, SignatureAlgorithm, Issuer, Validity, Subject, SubjectPublicKeyInfo and X509v3extensions.

- (d) Write an equation for how S is calculated in the certificate in Listing 1? You must use the names of algorithms used in the above certificate (i.e. you cannot use $E()$), as well as clearly identify which user each key belongs to. You may use the variable $Data$ in your equation to represent the concatenation of various fields. [2 marks]

Question 3 [3 marks]

Considered the scheme below (top of next page).



- (a) For this scheme to work, what keys are known by A and B before the 3 steps are taken? [1 mark]
- (b) Assume a network has 11 users, all using the above scheme. How many keys in total must be manually distributed prior the scheme being used? [2 marks]