1. **Questions and Short Answers**
2. **(5 pts)** When A receives a message from B, A needs to be sure that the message he has received is correct. This security service is called integrity. Explain the difference between *data integrity* and *origin integrity*.
3. The following is a partial listing of an X.509 certificate.

|  |
| --- |
|  |

1. **(1 pts)** Who is the certification authority of this certificate?

Answer:

1. **(1 pts)** Who is the owner of this certificate?

Answer:

1. **(5 pts)** Show how the signature on this certificate was generated? Hint: Show how the public key packet (pkp) is signed by the CA.
2. **(5 pts)** (Continued from above) Explain how can this signature be verified? Clearly state the prerequisite of the verification.
3. When browsing a web site, we see the following message.

There is a problem with this website’s security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.

1. **(5 pts)** What does it mean that the certificate is not issued by a trusted CA?
2. **(5 pts)** What is considered as a trusted CA?