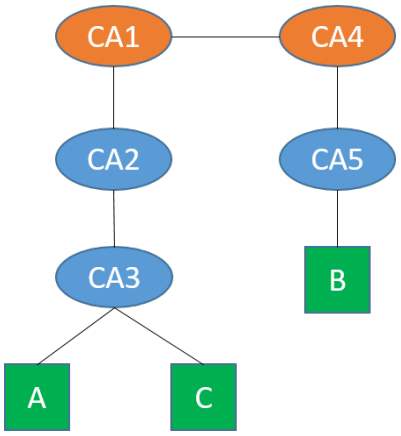
There are certificate authorities (CA) and end entities that follow the X.509 hierarchy as follows.



- CA1 and CA4 are the root certificate authorities.
- End-entity A is a subscriber of CA3 and it trusts CA1.
- End-entity B is a subscriber of CA5 and it trusts CA4.
- End-entity C is a subscriber of CA3 and it trusts CA1.
- Suppose that the certificate authorities and the end-entities have created their 2048-bit RSA public and private key files as follows.

Entity	Public Key File	Private Key File
CA1	pk1.pem	sk1.pem
CA2	pk2.pem	sk2.pem
CA3	pk3.pem	sk3.pem
CA4	pk3.pem	sk4.pem
CA5	pk5.pem	sk5.pem
A	pka.pem	ska.pem
B	pkb.pem	skb.pem
C	pkc.pem	skc.pem

Your tasks [36 marks].

Use OpenSSL commands to complete the questions as follows. Note that you DO NOT need to demonstrate the information of a Certificate Signing Request (CSR) file.

1. **[6 marks]** Create certificates for the root certificate authorities, CA1 and CA4, respectively.
2. **[12 marks]** Create certificates for B and C, respectively.
3. **[6 marks]** Demonstrate how to verify C's certificate by B.
4. **[5 marks]** Create certificate(s) that are needed to verify B's certificate by A.
5. **[7 marks]** Demonstrate how to verify B's certificate by A.

** You may choose a reasonable expiry time for each certificate.