## 10.3 Question 3

### 10.3.A Which of the following features are provided by both TLS and DTLS,and which only by DTLS? For those provided only by DTLS, explain why they are needed in DTLS and not in TLS.

**Confidentiality, integrity**

Both

**Message fragmentation and reassembly in the Handshake Protocol**

**Alert messages (*unknown_ca*, *certificate_expired*, ...)**

**Key exchange**

**Cookie exchange**

**Retransmission of lost handshake messages**