HW3 solution:

Q1

Yes. If the path between the requesting host and the CDN server, chosen by the CDN, is already too congested or if the chosen CDN server is already too busy, then it might be possible that the host experiences worse performance that what it would have if it contacted the remote server directly.

Q2

(1) End-to-end delay is the time it takes a packet to travel across the network from source to destination. Delay jitter is the fluctuation of end-to-end delay from packet to the next packet.

(2) A packet that arrives after its scheduled play out time can not be played out. Therefore, from the perspective of the application, the packet has been lost.

(3) No, they are not the same thing. The client application reads data from the TCP receive buffer and puts it in the client buffer. If the client buffer becomes full, then application will stop reading from the TCP receive buffer until some room opens up in the client buffer.

Q3

This wouldn't really solve the problem. Just as Bob thinks (incorrectly) that he is authenticating Alice in the first half of Figure, so too can Trudy fool Alice into thinking (incorrectly) that she is authenticating Bob. The root of the problem that neither Bob nor Alice can tell is the public key they are getting is indeed the public key of Alice of Bob.

Q4

(a) No, without a public-private key pair or a pre-shared secret, Bob cannot verify that Alice created the message.
(b) Yes, Alice simply encrypts the message with Bob's public key and sends the encrypted message to Bob.

Q5

No, the bogus packet will fail the integrity check (which uses a shared MAC key).