Solutions

2.1

- Integrity – alteration is detected (with key possession assumed) ✓.

2.2

- Certificates: the server proves possession of the private key matching the certified public one ✓.

2.3

- Fresh randoms – a replayed handshake derives different keys and fails the Finished check ✓.

3.1

- Order: ClientHello (suites + random); ServerHello (suite + random
  – certificate); key exchange (premaster encrypted under the public key); derive session keys; Finished both ways ✓.
- The three values: client random, server random, premaster ✓.
- Finished proves the whole handshake was not tampered with (it is checked under the derived keys) ✓.
- The first data byte uses the symmetric session keys ✓.

3.2

- Sniffing: encryption (confidentiality) acts on the data stream ✓.
- Handshake modification: the Finished check acts after key derivation – tampering changes the keys, so Finished fails ✓.
- Impostor: the certificate chain to a trusted root ✓.
- Full-handshake replay: the fresh randoms make the derived keys differ, so Finished fails ✓.
- Encrypting without authenticating: a private channel to the wrong machine ✓.
- HTTPS makes the channel private and the server identified – the content can still lie ✓.