1. Slide 9 in Module 1, introduction.

   Passive attack is more difficult to detect because it does not affect the system or the current communication.

2. a) DOIT
   b) try all 25 possible answers.
   c) One-time pad. It is provably unbreakable.

3. Specify two different network connections (e.g., Wi-Fi, Ethernet, and 4G/5G). Specify two different factors (e.g., password, token, digits calculated from function of time, fingerprint).

4. Risk aversion – people prefer certain gains instead of uncertain gains, although mathematically the expected values are the same.

   Risk taking – why facing financial losses, people prefer taking risks (i.e., a possibility of higher loss.)

5. a) Cannot change fingerprint (revocation). False positive and false negative.
   b) Advantage – more secure. All values are possible.
   Disadvantage – really difficult to remember.

6. a) Module 4, slides 23 and 24.
   b) Yes. An attacker may use Message 3 (slide 24) to generate all hash results after i and use them in future authentication.

7. a) Module 2, slides 42 and 43.
   b) Problem: cannot achieve the functionalities of digital signature.
   Alice and Bob know who generated the message and the message has not been changed, but they cannot prove to a third party.