Chapter 17 solutions

1. Eavesdropping, replay attack, relay attack, message modification, tag reading attack, tag rewriting attack, tag cloning, tag distraction/DoS attack, tag tracking, and wireless side-channel analysis.

[FT]See Section 17.2.

2. Identification, authentication, privacy, indistinguishability, forward security, restriction and delegation, proof of existence, and synchronization.

[FT]See Section 17.3.

3. Hash-chain-based schemes basically use hash functions. The secret key is incremented by the output of hash functions. Due to the one-way property of hash functions, the adversary cannot discover the previous secret key, which was recorded in the tag before incrementing, from the information of the current secret key.

4. The strong point is that it provides the property of forward security. The weak point is that the computational cost of the back-end system increases linearly with the number of tags.

5. e-Passports, electric car keys, credit cards using IC chips, and so on. For example, an RFID is attached to a case of medicine. The ID of the tag would be linked to any information on the medicine, so it would be easy to obtain sensitive and private information about the possessor related to the medicine from the tag's ID. Similar situations could occur with books, underwear, and so on. In such a case, the tag's ID should be identified for a dishonest reader.

6. As another example, if an RFID tag that is attached to a pair of glasses, outputs fixed data every time the glasses are worn, e.g. as an ID, the person who wears glasses with an attached RFID tag can be traced by tracking the fixed output of the tag. In such a case, the tag's output should be indistinguishable from random data.