CHAPTER 30 : Cryptography

Solutions to Selected Review Questions

Review Questions

2. Only ***one key*** (the shared secret key) is needed for two-way communication. However, for more security, it is recommended that a different key be used for each direction.

3. Each person in the first group needs to have **10** keys to communicate with all people in the second group. This means we need at least 10 · 10 = **100** keys. Note that the same keys can be used for communication in the reverse direction. However, note that we are not considering the communication between the people in the same group. For this purpose, we would need more keys.

4. For two-way communication, **4** keys are needed. Alice needs a private key and a public key; Bob needs a private key and a public key.

7. Each person needs 9 keys to communicate with the other people. At first glance, it looks like we need 10 · 9 keys. However, if the same key can be used in both directions (from A to B and from B to A), then we need only (10 · 9) / 2 = **45 keys**.

8. A shared secret key can only be used between two entities. Alice needs a shared secret key to communicate with Bob and a different shared secret key to communicate with John.