Student ID: _____

1. Given the following protocol: **[12]**

$$A \to B : \{A, K_A, T_A\}_{K_A^{-1}}$$
$$B \to C : \{A, K_A, T_B\}_{K_B^{-1}}$$
$$C \to B : \left\{h\left(\{A, K_A, T_B\}_{K_B^{-1}}\right)\right\}_{K_C^{-1}}$$
$$B \to A : \left\{h\left(\{A, K_A, T_B\}_{K_B^{-1}}\right)\right\}_{K_C^{-1}}, \{A, K_A, T_B\}_{K_B^{-1}}$$

(a) Explain the meaning of the notation in each step in the protocol.

i. $A \to B : \{A, K_A, T_A\}_{K_A^{-1}}$ 2

. . . . . .

. . . . . .

ii. $B \to C : \{A, K_A, T_B\}_{K_B^{-1}}$ 2

. . . . . .

. . . . . .

iii. $C \to B : \left\{h\left(\{A, K_A, T_B\}_{K_B^{-1}}\right)\right\}_{K_C^{-1}}$ 2

. . . . . .

. . . . . .

iv. $B \to A : \left\{h\left(\{A, K_A, T_B\}_{K_B^{-1}}\right)\right\}_{K_C^{-1}}, \{A, K_A, T_B\}_{K_B^{-1}}$ 2

. . . . . .

. . . . . .

(b) After the conclusion of the protocol, what are two facts that Alice knows about the message $\{A, K_A, T_B\}$?

i. _____ 1

ii. _____ 1

(c) What is the significance of the token that Bob sends to Alice? 2

. . . . . .

. . . . . .

2. Explain one security vulnerability in the WEP standard for IEEE 802.11 networking. How was this vulnerability addressed in later Wi-Fi protocols? [4]

3. Explain a security threat posed by one of the types of middleboxes that we discussed in class. How can this threat be mitigated? [4]

Student ID: _____

4. What is the same origin policy? Why is it important? What is one of its limitations? [6]

5. What is cross-site request forgery? How can websites prevent it? [4]