CS5285: **Information Security for eCommerce** Autumn, 2024
Tutorial 7, Week 9 (November 5)

Questions:

1. **Key Establishment 1** The following protocol establishes a new key K_{AB} between A and B using a trusted third party S. What type of key establishment is this and what is S called?

$$\begin{array}{ccccl} A & \rightarrow & S & : & E_{KAS}(K_{AB}, B) \\ B & \leftarrow & S & : & E_{KBS}(K_{AB}, A) \end{array}$$

2. **Key Establishment 2** Consider the following protocol, where E is a symmetric key encryption scheme and K is a long-term symmetric key shared between A and B.

$$\begin{array}{ccccl} A & \rightarrow & B & : & \text{“Alice”},\ R_1 \\ A & \leftarrow & B & : & R_2,\ E_K(R_1) \\ A & \rightarrow & B & : & E_K(R_2) \end{array}$$

Does the scheme support session key establishment? If not, modify the protocol so that it does.

3. **Asymmetric Key Exchange** Consider the following protocol, where E is a symmetric key encryption scheme, and K is computed as $K = g^{ab}\ mod\ p$. $[message]_{name}$ means *message* signed by *name*.

$$\begin{array}{ccccl} A & \rightarrow & B & : & \text{“I'm Alice”},\ g^a\ mod\ p \\ A & \leftarrow & B & : & \text{“Bob”},\ g^b\ mod\ p,\ E_K([g^a\ mod\ p, g^b\ mod\ p]_{\text{Bob}}) \\ A & \rightarrow & B & : & \text{“Alice”},\ E_K([g^a\ mod\ p, g^b\ mod\ p]_{\text{Alice}}) \end{array}$$

What is the long-term secret of this scheme?

4. **Trusted Third Party Key Exchange**

i) Design a protocol that will use a key distribution centre to set up a shared key K between Alice and Bob. You should use timestamps for freshness and assume that Bob cannot talk directly to the KDC. Alice and Bob does not need to be authenticated to each other and there is no need for explicit key authentication. State all your assumptions.

ii) What is the key hierarchy in this protocol?

iii) If K_{AT} and K_{BT} are 56-bit DES keys and K is a 256-bit AES key what is the effective security of key K?