Assignment #5

This assignment is due Friday November 11th at the beginning of class.

1. In Kerberos, when Bob receives a Ticket from Alice, how does he know it is genuine (i.e. how does he know that it really contains a key that he is going to share with Alice, and that the ticket really came from Alice)?

2. In Kerberos 5, suppose that a pirate sniffs the network and sees the ticket sent by the ticket granting server (TGS) to a user $A$. What prevents the pirate from using the ticket to obtain the service in place of the legitimate client?

3. Suppose that everybody in a system knows that $A$ has public key $pk_A$ and that $A$ is the only one who knows the key $sk_A$ that can decrypt the messages encrypted with $pk_A$.

Consider the following protocol, with which $A$ identifies himself to a user $B$:

**Step 1** $A$ sends the message “I claim to be $A$” to user $B$.

**Step 2** $B$ generates a random message $r$, encrypts $c = E(pk_A, r)$ (that is, $c$ is a ciphertext that for the message $r$ encrypted with the key $pk_A$) and sends $c$ to $A$.

**Step 3** $A$ decrypts $c$ to recover $r$ and sends $r$ to $B$ to prove that he is indeed $A$.

Suppose that $A$ has initiated Step 1 of the protocol with $C$. Show how $C$ can run the protocol with $D$ while claiming to be $A$ by using the run of the protocol initiated by $A$. Show how the protocol could be modified to prevent this attack. This attack is called a *reflection* attack.

4. Suppose that every user $U$ in a system shares a key $k_U$ with a trusted server $TS$. When user $A$ wants to send a message $M$ to user $B$, he runs the following protocol:

**Step 1** $A$ generates a random key $K$ and sends his name $A$, destination $B$, and $E(k_A, K)$ to the server $TS$.

**Step 2** The server $TS$ then responds by sending $E(k_B, K)$ to $A$.

**Step 3** $A$ then sends $E(k_B, K)$ and $E(K, M)$ to $B$.

**Step 4** $B$ uses his key $k_B$ to decrypt $K$ and then uses $K$ to decrypt $M$.

Suppose that user $C$ sniffs the networks and has observed all these messages. Show how $C$ can use a replay attack in order to recover the message $M$ without breaking the encryption.
5. Suppose that an attacker hacked your wireless router in a way that when your browser requests the IP of your bank, the router instead sends the request to the IP of a cloned site hosted by a pirate, and that the router spoofs the source IP on the way back to make your browser believe that the packet really came from your bank. Explain why it will be impossible for the cloned site to establish a TLS connection.

6. Suppose that for some reason TCP does not properly do its job and gives segments to TLS out of order. Would it be possible for TLS to reorder them? If so, explain how. If not, why not?