CS162 – Section 11

True/False

1. Public key cryptography requires participants to distribute a secret keys

2. A digital certificate is an encrypted binding between the user's identity and user's public key using a certification authority's (e.g., Verisign) *public key*.

3. "Delay checking" of the password is an effective way to make it harder to crack a password, assuming the attacker doesn't have access to /etc/passwd

4. Checking the size of every argument before copying it in the buffer can avoid buffer overflow attacks.

5. Typically, the number of hosts infected by a worm increases linearly.

Short Answer

1. What are three common ways of compromising passwords?

2. What are four security requirements, explain them:

3. What do DES, and AES stand for? Are they symmetric key encryption?

4. Does the following mutual authentication work? Why? If not, please provide a working version. Alice's public key Pub_A, private key Pri_A.

   Bob's public key Pub_B, private key Pri_B.
   Alice and Bob know all each other public keys.
   Alice: Send E(E(N_x, Pri_A), Pub_B)
   Bob: Receive msg from Alice. Send back E(E(N_x, Pri_B), Pub_A)
   Alice: Receive msg from Bob. Start to send real message E(E(N_x, Pri_A) + msg, Pub_B) N_x is a random message generated by Alice.