CS162 – Section 11

True/False

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

   False.

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*.

   False.

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

   True.

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

   True.

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

   False.

Short Answer

1. What are three common ways of compromising passwords?

   password guessing, dictionary attack, dumpster diving

2. What are four security requirements, explain them:

   Authentication: Ensures that a user is who is claiming to be.
   Data integrity: Ensure that data is not changed from source to destination or after being written on a storage device.
   Confidentiality: Ensures that data is read only by authorized users.
   Non-repudiation:
   a). Sender/client cannot later claim didn't send/write data;
   b). Receiver/server can't claim didn't receive/write data.

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

   DES: Data Encryption Standard
   AES: Advanced Encryption Standard
   Yes.

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.

   No. Bob can not be sure that he is talking with Alice.
   Alice: Send E(E(N_x, Pri_A), Pub_B)
   Bob: Receive msg from Alice. Send back E(E(N_x + N_y, Pri_B), Pub_A)
   Alice: Receive msg from Bob. Start to send real message E(E(N_x+N_y, Pri_A) + msg, Pub_B) N_x is a random message generated by Alice.
   N_y is a random message generated by Bob.