Cyber Forensics

(CS-552)

Assignment--1

1. The IPsec architecture document states that when two transport mode SAs are bundled to allow both AH and ESP protocols on the same end-to-end flow, only one ordering of security protocols seems appropriate: performing the ESP protocol before performing the AH protocol. Why is this approach recommended rather than authentication before encryption?

2. What parameters identify an SA and what parameters characterize the nature of a particular SA?

3. What is the difference between a TLS connection and a TLS session?

4. List and briefly define the parameters that define a TLS session state and a TLS session connection.

5. Two users A & B decide to use Deffie-Hellman key exchange technique a common prime $p=71$ and a primitive root $g = 7$.

(a) If user A has private key $X_A = 5$, what is A's public key Y_A?

(b) If user B has private key $X_B = 12$, what is B's public key Y_B?

(c) What is the shared secret key between A and B?

6. Briefly explain the idea behind the RSA cryptosystem.

1) What is the one-way function in this system?

2) What is the trapdoor in this system?

3) Describe the security of this system.

7. Alice uses Bob's RSA public key (e = 7, n = 143) to send the plaintext P = 8 encrypted as ciphertext C = 57. Show how Eve can use the chosen ciphertext attack if she has access to Bob's computer to find the plaintext.