DT024A

Tingting Zhang
tel: 148878, mobile: 0736962242

Examination of Network Security and Management, AV 2015

Time: 2015-04-23

Total: 100

A: 90
B: 80
C: 70
D: 60
E: 50
Fail < 50

Good Luck

Tingting Zhang
tel: 148878, mobile: 0736962242

1. (20 p)
   What is a typical phases of operation of a virus?

2. (20 p) What is stream cipher? What is basic method of stream cipher encryption? How to use the AES software to create a streaming cipher encryption software. Use block diagram to explain your method.

3. (20 p) Suppose that Alice and Bob share one secret key K_{ab}, and Alice and Code share one secrete key K_{ac}. Describe two ways for Alice to sign a message M and send it confidentially to Bob and Code by using a hash function MD5 in one packet? Compare them.

4. (20 p) Suppose that Alice has Bob's X.509 certification. Bob has Alice's X 509 certification. Bob and Code share the secret key K_{bc}. How could Alice and Code mutual authenticate each other and create an efficient secure channel between them.

5. (10p) How is an X.509 certificate revoke?

6. (10p) What are the implications of SSL being implemented at TCP, contrasted with IPsec's being implemented at IP layer?