DT024A

Tingting Zhang
tel: 148878, mobile: 0736962242

Examination of Network Security and Management, AV 2012

Time: 2012-08-24

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) 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 has Bob's public key Kpubb. Bob has Alice's public key Kpuba. Bob and Eva share the secret key K_{be}. Code has Eva's public key Kpuba. Eva has Code's public key Kpubc. How could Alice and Eva mutual authenticate each other and create a secure channel between them.

4. (20 p) Suppose that Alice has Bob's public key Kpubb and Bob has Alice's public key Kpuba. Alice and Bob share a secret key Kab. Describe two ways for Alice to sign a message M and send it confidentially to Bob by using a hash function MD5? Compare them.

5. (20p) What is the purpose of the X. 509 standard? What information is included in a X.509 certification?