DT024A.

Tingting Zhang
tel: 148878, mobile: 0736962242

Examination of Network Security and Management, AV 2011

Time: 2011-08-26

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)
   List out categories of passive and active security attacks.

2. (20 p) What is 2DES? Is 2DES more secure than DES? Describe block structure of 3DES and compare with 2DES.

3. (20 p) Suppose that Alice has Bob's public key Kpubb and Bob has Alice's public key Kpuba. How could Alice sign a message M and send it confidentially to Bob by using a hash function MD5?

4. (20 p) Suppose Alice and Code trust each other, they have each other's public key. Code and Bob share a secrete key. Describe a process that create a secure channel and between Alice and Code.

5. (20 p) What is a private key ring in PGP? What is a public key ring in PGP?