Tingting Zhang
tel: 148878, mobile: 0736962242

DTO24A

Examination of Network Security and Management, AV 2014

Time: 2014-04-25

Total: 100

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

The use of dictionaries is permitted.

Good Luck

Tingting Zhang
tel: 148878, mobile: 0736962242

1. (20 p)
   - List out 5 security mechanisms
   - What kind of security attacks each security mechanism can protect?

2. (20 p) Give two methods to encryption for online video displaying using a symmetric 128 bit block cipher encryption. Compare these two methods. Find a better one.

3. (20 p) What are the properties a digital signature should have? Suppose Alice, Bob and Code do not share any secrete keys. They have each other's public key. How could Alice sign one message M and send it confidentially to both Bob and Code at same time by using a hash function MD5?

4. (20 p) Suppose that Alice has Code's public key Kc and Bob has Code's public key. Both Alice and Bob trust a Code. Describe a method that can create a temporary efficient secure channel between Bob and Alice.

5. (20 p) Briefly describe the methodology that using password to identifying client in Kerberos login process. How to protect client passwords?