Tingting Zhang
tel: 148878, mobile: 0736962242

Examination of Network Security and Management, AV 2015

Time: 2015-02-20

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)
   What are active security attacks? Name 5 active security attacks. What kind active attacks can be protected by authentication, encryption, and access control?

2. (20 p) Give two methods to encrypt and decrypt a very small packet (< =32 bits) by using a symmetric 128 bit block cipher encryption. Compare these two methods.

3. (20 p) Suppose Alice, Bob and Eva share a secret key K_{abe}. Suggest two methods for Alice signs a message M and sends it confidentially to Bob and Eva by using a hash function? Compare these two methods.

4. (20 p) Suppose that Alice and Bob have Code's public key Kc. Both Alice and Bob trust Code.

   1) Describe a method that can create a temporary efficient secure channel between Bob and Alice.
   2) Describe a method that Code can send his new public key to Alice and Bob.

5. (20 p) How to authenticate a user for using a remote server? (a server in another realm of Kerberos). Give detail information in the ticket that send from local ticket grand server to a user in the process of authenticating the user for using a remote server SQ in remote domain Q.