

Tingting Zhang
tel: 148878, mobile: 0736962242

Examination of Network Security and Management, AV 2017

Time: 2017-08-24

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 categories of passive and active security attacks. What kind of security mechanism can protect these attacks?
2. (20 p) Give two methods to encrypt a very large packet by using a symmetric 128 bit block cipher encryption. Compare these two methods.
3. (20 p) Suppose Alice and Bob share a secret key K_{ab} . Suggest two methods for Alice who signs a message M and sends it confidentially to Bob by using a hash function? Compare these two methods.
4. (20 p) Suppose that Alice has Code's public key K_c and Code has Bob's public key K_b . 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) What is X.509 protocol? What information is included in a X.509 certification? Suppose that Bob is certificated by X.509 certification authority XB , Alice is certificated by X.509 certification authority XA . How can Alice get Bob's certification?