Tingting Zhang
tel: 148878, mobile: 0736962242

DJD24A

Examination of Network Security and Management, AV 2016

Time: 2016-02-18

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. What is network security? Is a system secure if we can guarantee a network security?

2. (20 p) If we use the following AES based mode of operation to encrypt a 3 Mbyte file, can it guarantee confidential? Can it guarantee confidential and authentication? What is the disadvantage of this mode of operation? Suggest a mode of operation that is better than this and use formula or graph to explain your suggestion.

3. (20 p) Suppose that Bob has Alice's public key K_{puba}, and Alice and Code share one secrete key K_{ac}. Describe one way for Alice to sign a message M and multicast it confidentially to Bob and Code by using a hash function MD5.

4. (20 p) Suppose that Alice trust Bob. Bob and Cod trust Eva. Suppose that Alice and Bob share a secret key K_{ab}, Eva has Bob's public key K_{pubb}. Eva and Cod share one secrete key K_{ec}. Describe a method that can create a temporary efficient secure channel between Cod and Alice.

   Does your method can guarantee that Alice and Cod mutual identify each other?

5. (20 p) What is DAC, MAC and Role Based Access Control method? Compare them.