DT024A

Tingting Zhang
tel: 148878, mobile: 0736962242

Examination of Network Security and Management, AV 2013

Time: 2013-04-19

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 five main security mechanisms.
   - List 3 main security attacks.
   - What kind security mechanism can protect each of your listed security attacks

2. (20 p) Briefly describe a stream cipher method. Why is it not desirable to reuse a stream cipher key?

3. (20 p) Suggest a method that uses X.509 certifications to create an efficient temporary secure chatter room for Alice, Bob and Cod. The method should be described by detailed messages contents and messages passed between Alice, Bob and Cod.

4. (20 p) Suppose that Alice has Bob's public key K_{pubb} and Bob has Alice's public key K_{puba}. Alice and Bob share a secret key K_{ab}. Describe two different methods for Alice to sign a message M and send it confidentially to Bob by using a hash function MD5? Compare your two methods.

5. (20p) Given an AES software program, how to use block cipher modes of operation to encrypt and decrypt a big file? Use a block flow graph to describe it.