DT024A

Tingting Zhang
tel: 148878, mobile: 0736962242

Examination of Network Security and Management, AV 2013

Time: 2013-05-29

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 main security threats?
   - List out categories of passive and active security attacks.

2. (20 p) How to use a given symmetric 128 bit block cipher encryption and decryption program to encrypt and decrypt a stream of very small packets (packets size less than 60 bits). Use block cipher flow graph to describe it.

3. (20 p) The Diffie-Hellman key exchange can be used to create a session key between two users. Explain why this key exchange method is vulnerable to man in middle attack. Suggest a method that can protect the main middle attack to Diffie-Hellman key exchange on an unsecure channel.

4. (20 p) Suppose that Alice and Bob both trust a KDC. The KDC share a secret key Kak with Alice and has Bob's public key Kpubb. Bob has public key of this KDC, Kpubk. Suppose that Alice can communicate with the KDC, Bob can only communicate with the KDC through Alice. Describe a method that can create a temporary efficient secure channel between Bob and Alice.

5. (20 p) What is a private key ring in PGP? What is a public key ring in PGP? How to decide the trust level of a public key in PGP?