Tingting Zhang
tel: 148878

Examination of Network Security and Management, AV 2010

Time: 2010-03-26 (2 hours)

Total: 100

A: 90
B: 80
C: 70
D: 60
E: 50
Fail < 50

Good Luck!

Tingting Zhang
tel: 148878

1. (15 p) What is a typical phases of operation of a virus?

2. (15 p) Suppose that Alice has Bob's public key Kpubb and Bob has Alice's public key Kpuba. How could Alice sign a message M and send it confidentially to Bob by using a hash function MD5?

3. (20 p) One method of encrypt a large amount of data using AES is as the following:

   - Divide the data into block $B_1, B_2, \ldots, B_n$. Each block has size of 128 bits.
   - Encrypt each block Bi as: $E_k(B_i)$, I = 1, …, n.

   What advantage of this method? What disadvantage of this method? How to improve it? Describe the improvement as a block structure.

4. (20 p) Suppose that Alice and Jimmy trust each other and they share a secret key. Bob trust Jimmy. Bob has Jimmy's public key. Jimmy does not have Bob's public key. Describe a simple method that Alice and Bob mutual authenticated and securely exchange their public key.

5. (10 p) Describe a ticket send from KDC send to user A in Kerberos system.

6. (20 p) What is the purpose of the X. 509 standard? What information is included in a X.509 certification? What is a chain of certification in X.509?