OTOZYA

Tingting Zhang
tel: 0101428878

Examination of Network Security and Management, AV 2016

Time: 2016-08-23

Total: 100

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

Good Luck

Tingting Zhang
tel: 0101428878

1. (20 p)
   - What are main security threats?
   - What is a typical phases of operation of a virus?

2. (20 p) Compare ECB, CBC, CTR, CFB mode of operation.

3. (20 p) Suppose that Alice, Bob and code share one secrete key K_{abc}. How could Alice sign a text M and send it confidentially to Bob and code by using a hash function MD5 in one message.

4. (20 p) Suppose that Alice has Eva's public key K_{pubeva}. Eva does not know Alice and has no information about Alice. Bob has Alice's public key, $K_{pubalice}$. Bob and Eva share the secret key K_{be}. How could Alice start to create a mutual authenticate with Eva and create an efficient secure channel between them?

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

5. (20 p) Suggest a method of password change in Kerberos system.