Tingting Zhang
tel: 148878, mobile: 0736962242

DTD24A

Examination of Network Security and Management, AV 2016

Time: 2016-04-19

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 5 security mechanisms
   - What kind of security attacks each security mechanism can protect?

2. (20 p) What kind of AES based mode of operation can be used to encrypt a stream of 56 bit data, can it guarantee confidential and authentication?

3. (20 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?

4. (20 p) Suppose that Alice has Bob's public key Kpubb. Bob has Alice's public key Kpuba. Bob and Eva share the secret key K_{be}. How could Alice and Eva mutual authenticate each other and create an efficient secure channel between them.

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

5. (20 p) What is a private key ring in PGP? What is a public key ring in PGP?