Mittuniversitetet
MID SWEDEN UNIVERSITY

Försättsblad Prov Original

Kurskod	Provkod	Tentamensdatum
DT055A	Q101	2019-03-26

Kursnamn	Datateknik AV, Nätverkssäkerhet och nätverksdrift
Provnamn	Automaträttat (flervals) prov
Ort	Sundsvall
Termin	
Ämne	

Tingting Zhang
tel: 148878, mobile: 0736962242

Examination of Network Security and Management, AV 2019

Time: 2019-03-26

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)
   a) List out 3 type of active security attacks.
   b) What kind of method(s) can prevent the attack that you listed out?

2. (20 p) Describe two methods of using the 128 byte AES software to encrypt data stream. The size of each packet is 32 bytes. Use block diagram to explain your methods. Compare your suggested methods.

3. (20 p) Suppose that Bob, Alice and Code share a security key, k_{abc}. Alice need to confidentially send one signed message M to Bob and Code. Describe a method that use X.509 Authentication Service to do this task.

4. (20 p) Suppose that Alice has Bob's public key Kpubb. Bob and Alice share one security key K_{ab}. 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) How to use Kerberos system to authenticate a use for using a remote server? (a server in another realm of Kerberos). Describe the ticket for using the remote server.