Mittuniversitetet
MID SWEDEN UNIVERSITY

Försättsblad Prov Original

Kurskod	Provkod	Tentamensdatum
DT024A	Q102	2018-03-19
Kursnamn	Datateknik AV, Nätverkssäkerhet och nätverksdrift	
Provnamn	Automaträttat (flervals) prov	
Ort	Sundsvall	
Termin	V18	
Ämne	Datateknik	

8982538474

0026997

Tingting Zhang
tel: 0101428878

Examination of Network Security and Management, AV 2018

Time: 2018-03-19

Total: 100

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

Good Luck

Tingting Zhang
tel: 0101428878

1. (20 p) What is security policy? List out 4 different network security mechanism. What kind of attacks can be protected by each of them?

2. (20 p) What is block cipher? How to use the DES software encrypt a large video in video conference. Use block diagram to explain your method. Is your method secure and efficient enough?

3. (20 p) Suppose that Alice, Bob and Code share one secrete key K_{abc}. Bob and Code has Alice's private key. Alice has Bob and Code's public key. Suggest two methods for Alice to sign a text M and send it confidentially in one message to Bob and Code by using a hash function MD5 at same time.

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

   Your method should guarantee that Alice and Bob mutual identify each other.

5. (20 p) How to authenticate a user for using a remote server in Kerberos system? (a server in another realm of Kerberos). Give detail information in the ticket that send from local ticket grand server to a user in the process of authenticating the user for using a remote server SQ in remote domain Q.