Mittuniversitetet
MID SWEDEN UNIVERSITY

Försättsblad Prov Original

Kurskod	Provkod	Tentamensdatum
DT024A	Q102	2018-02-15

Kursnamn	Datateknik AV, Nätverkssäkerhet och nätverksdrift
Provnamn	Automaträttat (flervals) prov
Ort	Sundsvall
Termin	V18
Ämne	Datateknik

Tingting Zhang
tel: 0101428878

Examination of Network Security and Management, AV 2018

Time: 2018-02-15

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 network security? Is a system secure if we can guarantee a network security? What kind of attacks can be protected by encryption and message authentication? What kind of attacks cannot be protected by encryption and message authentication?

2. (20 p)

   Suggest two secure methods to encrypt a stream data where each data size is 32 bites. The two methods should be described in graph blocks or formula. Compare your suggested methods.

3. (20 p) Suppose that Alice and Bob share one secrete key K_{abc}. Everyone has each other'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) Suggest a method that use X.509 certification to create an efficient secure chatter room for Alice, Bob and Cod.

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

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