



Försättsblad Prov Original

Kurskod	Provkod	Tentamensdatum
D T 0 5 5 A	Q 1 0 1	2 0 1 9 - 0 2 - 2 1
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
DT055A:T101, 3 hp
DT024A: Q102, 3.5 hp

Time: 2019-02-21

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 the attacks that can be prevented by message encryption.
 - b) List out the attacks that can be prevented by message authentication.
 - c) What kind of method(s) can prevent traffic analysis?
2. (20 p) Describe two methods of using the 128 byte AES software to encrypt a voice stream. Use block diagram to explain your methods. Compare your suggested methods.
3. (20 p) Suppose that Bob has Alice public key K_{puba} , and Alice and Code share one secrete key K_{ac} . Describe a method that
 - a) Alice confidentially send individual signed message M to Bob and Code.
 - b) Alice confidentially multicast one signed message of M to Bob and Code.
4. (20 p) Suppose that Alice and Bob both trust a KDC. The KDC share a secret key K_{ak} with Alice. The KDC has Bob's public key K_{pubb} . Bob has public key of this KDC, K_{pubk} . Suppose that Alice can communicate with the KDC. Bob can only communicate with the KDC through Alice. Describe a method that can set up a temporary efficient secure channel between Bob and Alice.
5. (20 p) In PGP system, what kind of keys are in public key ring? How to decide a trust level of a public key in PGP system?