Mittuniversitetet
MID SWEDEN UNIVERSITY

Försättsblad Prov Original

Kurskod	Provkod	Tentamensdatum
DT024A	Q102	2018-08-23

Kursnamn	Datateknik AV, Nätverkssäkerhet och nätverksdrift
Provnamn	Automaträttat (flervals) prov
Ort	Sundsvall
Termin	H18
Ämne	Datateknik

Tingting Zhang
tel: 148878, mobile: 0736962242

Examination of Network Security and Management, AV 2018

Time: 2018-08-23

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)
   What is passive attack? What is active attack? List out the methods that can prevent passive attack.

2. (20 p) What is block cipher? What is stream cipher? How to use the 128 byte AES software to encrypt a voice stream. Use block diagram to explain your method.

3. (20 p) Suppose that Bob has Alice's public key K_{puba}, and Alice and Code share one secrete key K_{ac}. Describe one way for Alice to sign a message M and multicast it confidentially to Bob and Code by using a hash function MD5.

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

5. (20 p) What is a private key ring in PGP? What is a public key ring in PGP? How to decide the trust level of a public key in PGP?