# Network Security Practice Exam
DT116G

Lennart Franked*

2011-10-17

## Instructions

Carefully read the questions before you start to answering them, note the timelimit of the exam and plan your answers accordingly. Only answer the question, do not write about subjects remotely related to the question. Only write on one side of the sheet, and all answers must be written on the sheets, and not on the exam paper.
Make sure you write your answers clearly, if I can't read your answer you will not get any points, even if your answer is correct. The questions are *not* sorted by difficulty.

**Aids** Dictionary

**Time** 5 hours

**Maximum points** 60

**Questions** 12

### Bonus points
You must get an E or higher, to get the bonus points added to your final grade. The bonus-points will be added to this exam, and the first re-exam.

### Preliminary grades
$E \geq 50\%, D \geq 60\%, C \geq 70\%, B \geq 80\%, A \geq 90\%$

## Questions

1: **Symmetric Encryption** 4p
Explain the difference between a stream cipher and a block cipher.

2: **Security implementations** 6p
Give three examples where network security can be implemented in the TCP/IP protocol suite, also name a protocol for each layer.

3: **Asymmetric encryption** 6p
Describe the principle of an asymmetric cryptosystem, give two examples off when this kind of systems are used.

4: **Public key certificates** 4p
How are X.509 certificates used to insure the validity of a public key?

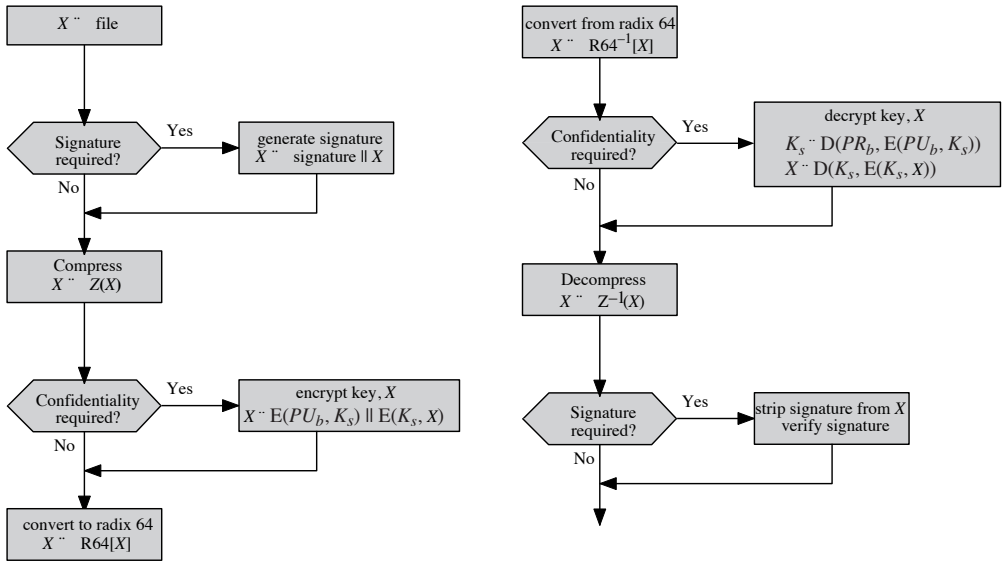
*Tel: 060-148683, email: lennart.franked@miun.com

5: **Digital Signatures** 4p

Describe the principle of digital signatures and its content, show this with an example.

6: **Email-security** 6p

Using the picture given below, explain as thoroughly as possible how PGP works.




(a) Generic Transmission Diagram (from A) (b) Generic Reception Diagram (to B)

**Figure 7.2 Transmission and Reception of PGP Messages**

7: **Threats** 6p

Explain the following terms:

(a) (2p) Integrity

(b) (2p) Confidentiality

(c) (2p) Availability

8: **Attacks** 4p

Describe the following attacks:

(a) (1p) Syn-flooding

(b) (1p) CPU hogging

(c) (1p) Ping-of-Death

(d) (1p) What kind of attacks are these?

9: **Firewalls** 4p

Describe the following types of firewalls

(a) (2p) Circuit level gateway

(b) (2p) Application level gateway

10: **AAA** 6p

Describe principle of AAA as detailed as you can.

11: **Intrusion detection** 2p

Explain the differences between a virus and a trojan horse

12: **IP-Security** 8p

With the help of the picture below, explain how IPsec processes outbound IP Packets.

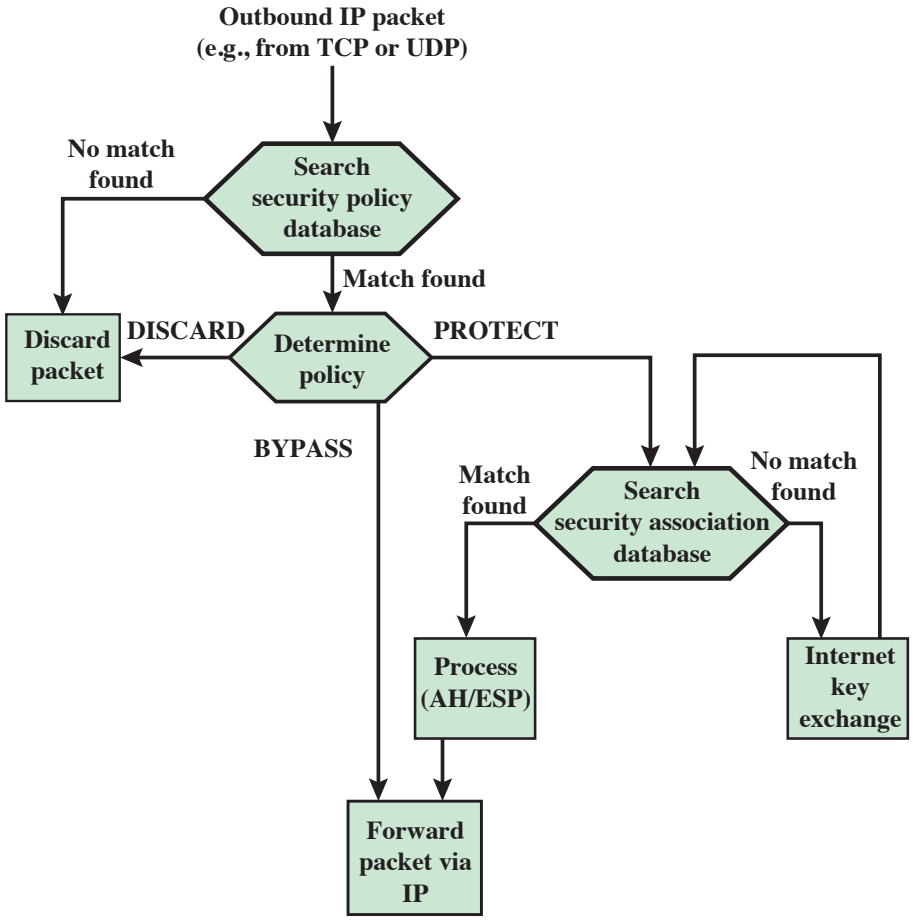



**Figure 8.3 Processing Model for Outbound Packets**