T-110.4206 Information security technology
Examination 2012-01-03
Lecturer: Tuomas Aura
No electronic equipment or reference material allowed in the examination.

*Answer **only 5** of the 6 problems. If you answer them all, only problems 1–5 will be marked.*

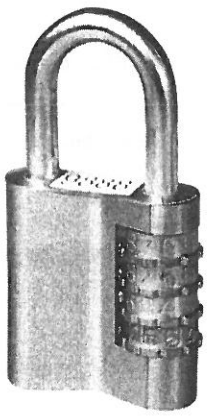
1. Access control

Give an example of each of the following types of policies and functions in the context of a university, either in computer systems or outside them (max 15 words each):

a) No write up
b) No read down
c) Separation of duty
d) Downgrading data
e) Covert channel
f) Group-based access control

2. Authentication

A mechanical combination lock has 3–6 wheels, each with digits 0–9. In order to open the lock, one needs to align the right numbers on one line.



a) What is the entropy of the secret key information for 3-wheel and 6-wheel locks?
b) If it takes one second for a brute-force attacker to try one combination, how long will it take to open the 3-wheel and 6-wheel locks?
c) The mechanical combination lock is replaced with a new electronic design, which has exactly the same physical form but an electronic mechanism inside. How could the security of the electronic lock be improved compared to the mechanical one?

It is sufficient to perform the numerical calculations approximately but please write down your calculations.

Please turn the paper for problems 3–6.

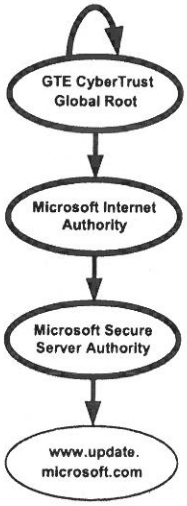
3. **Identity management**

Explain how Shibboleth authentication works.

Please choose one set to SAML bindings and tell which ones you are using in your answer. For example, you could choose the HTTP Redirect and Artifact bindings, or alternatively HTTP POST bindings.

(Terminology reminder: SP, IdP; Authentication Request, Authentication Response)

4. **PKI**



The picture on the right illustrates a certificate chain from an actual web site.

a) How many X.509 certificates are there in the chain and what types of certificates are they?
b) Explain <u>in detail</u> how the web browser checks a certificate chain of arbitrary length and how it is used in SSL to authenticate the web site.

5. **Secure storage**

Alice wants to communicate secret messages to Bob. She writes the messages into text files and uses the command line tool PGP (or its implementation GPG) to encrypt the files. She then sends the files by email.

a) What security limitations does this method have?
b) What advantages and disadvantages would there be, compared to process described above, if Alice started using an email client program with integrated encryption functionality?

6. **Threat analysis**

What security threats are there against coin locks on public toilets?